The Common Law Duty of Confidence and the Use of Information in Healthcare in Wales

Andrew George Fletcher
LL.M, LL.B (Hons), PGDip (LPC); MBCS, FedIPPra

Supervised by:

Dr Professor Nicola Whitehead
Dr Professor John Rees

Submitted in partial fulfilment for the award of the degree of Ph.D. by research
University of Wales Trinity Saint David.
2025

DECLARATION

This work has not previously been accepted in substance for any degree and is not being concurrently submitted in candidature for any degree.

Signed (candidate)

Date: 17th December 2025

STATEMENT 1

This thesis is the result of my own investigations, except where otherwise stated. Where correction services have been used the extent and nature of the correction is clearly marked in a footnote(s). Other sources are acknowledged by footnotes giving explicit references. A bibliography is appended.

Signed (candidate)

Date 17th December 2025

STATEMENT 2

I hereby give consent for my thesis, if accepted, to be available for deposit in the University's digital repository.

Signed (candidate)

Date: 17th December 2025

Abstract

This thesis describes how information that is subject to the common law duty of confidence can be shared lawfully in the National Health Service in Wales. The complexities of modern healthcare and the exploitation of data to improve service provision necessitate a clearer understanding of the duty of confidence to ensure that information is shared lawfully.

Guidance produced by the health service and professional bodies assists healthcare professionals and health service staff in making decisions around using information to ensure compliance with legal and ethical frameworks when everyday tasks are being performed. However, they lack a comprehensive legal perspective, potentially inhibiting lawful information sharing. The Law Commission highlighted that this issue extends beyond the NHS to the wider public service[1].

There is an absence of detailed legal guidance that focuses on the common law duty of confidence, specifically in relation to the National Health Service in Wales. There are no texts that examine the provisions under section 251 of the National Health Service Act 2006 to create regulation. There are no studies that explain how statutory functions can confer powers to enable bodies to lawfully collect and use information that is subject to the duty of confidence.

Employing doctrinal and empirical legal research methodologies, this thesis reviews primary legal resources and interprets them following established legal research methods to ensure an accurate representation of the law without social biases. The research aims to clarify misunderstandings and confusions around the duty of confidence and will be utilised in other work to create a comprehensive legal framework for healthcare professionals and organisations in Wales.

[1] See: The Law Commission, Data Sharing between Public Bodies: A Scoping Report (Law Com No 351, 2014),

The author

The author is an experienced national lead in information governance with twenty-two years' experience working in the National Health Service in Wales at the time of writing. The author has lectured extensively in areas such as data protection, information security and the common law duty of confidence in the NHS in Wales and to both undergraduate and postgraduate students as part of formal degree programmes. He has also assisted in writing the syllabus for governance modules for degree programmes. He was recently engaged in writing exam questions for the British Computer Society's Professional Certificate in Data Protection, often seen as a staple qualification for experienced Data Protection Officers and senior information governance staff.

Table of Contents

Tables and Figures

List of Tables

List of Figures

Acknowledgements

I would like to take this opportunity to express my sincere gratitude to Associate Professor Nicola Whitehead and Professor John Rees as my supervisors throughout this research. Their encouragement and insightful discussions at every stage of the research project have been invaluable. I thank them for their unwavering support and belief in me.

This Ph.D. thesis has been supported and part funded by my employers at Digital Health and Care Wales in the recognition of a void in knowledge of an area of law fundamental to information sharing in the modern NHS. I am extremely grateful for the opportunity to explore this area of work with the aim of improving the understanding of the Common Law duty of confidence as it applies to organisation in Wales.

I am indebted to my late parents in everything I have achieved. If it was not for the support that they provided, and the sacrifices they made to ensure that the little they had could improve my prospects, the academic journey I have undertaken would not have happened. My late father was so proud when I enrolled on the Ph.D. but sadly passed away before its completion.

Finally, I would like to thank all my family and friends, particularly those who have now become experts in the common law duty of confidence regardless of their wish to do so as a result of my consistent discussions on the subject.

Table of statutes

- **Children's Act 1989**
  Section 105(1).

- **Cities and Local Government Devolution Act 2016**

- **Data Protection Act 1998,**
  Schedule 1, Paragraphs 3, 7

- **Data Protection Act 2018, 2018**
  Sections 3(2), 3(3), 3(5). 3(10), 205(4)

- **Family Law Reform Act 1969**
  Sections 8(1), 8(3).

- **Freedom of Information Act 2000**
  Sections 1(1)(a), 1(1)(b), 1(6), 2(1), 2(1)(a), 2(2)(b), 2(3), 3, 41(1), 41(1)(a), 41(1)(b), 41(2), Schedule 1, Section 8.

- **Health and Social Care Act 2012**
  Section 251(1)(a), 254, 254(1), 254(2)-(7), 255(1), 255(2), 55(7), 255(8)(a), 255(8)(b)(i), 256(1), 256(1)(a), 256(1)(b), 256(2)(b), 256(2)(c), 257(4), 259, 259(2)(a), 259(2)(b), 259(1)(a), 259(1)(b), 259(3)-(11), 260(1), 260 (2)(a), 260(2)(b), 260(2)(c), 261(1A)(a), 261(1A)(b), 261(2), 261(4), 261(7), 262(4)(a), 262(4)(b), 262(5), 263, 265

- **Human Rights Act 1998**
  Section 6(1), 6(2), 6(3)(b), 6(5), 6(6), 21(1).

- **Interpretation Act 1978**
  Sections 6, 12(1), 12(2)

- **Mental Capacity Act 2005**
  Sections 1(1), 1(3), 1(4), 2(1), 2(2), 2(3)(a), 2(3)(b), S2(4), 2(5), 3(1)(a), 3(1)(b), 3(1)(d), 3(3), S3(2), 3(3)(1)(c), 3(4)(a), 3(4)(b).

- **National Health Service (Consequential Provisions) Act 2006**
  Section 4, 6; Schedule 2, Part 1; Schedule 4.

- **National Health Service (Wales) Act 2006**
  Sections 1, 1(2), 2(1)(a), 2(1)(b), 11, 12, 12(1), 12(3). 13(1), 13(2)(a), 13(2)(b), 13(2)(c), 13(3)(b), 13(3)(c), 13(3)(aa), 13(3)(ab), 18, 18(1), 19, 19(1), 19(1)(a), 19(1)(b), 19(1)(c), 22, 22(1), 23, 23(1), 23(3), 24, 24(1), 31(2), 140(6), 204(1), 204(3)(a), 204(3)(b)(i), 204(3)(b)(ii)

- **National Health Service Act 1977**
  Section 16BA

- **National Health Service Act 2006**
  Sections 251(1), 251(1)(a), 251(1)(b), 251(2), 251(2)(a), 251(2)(a)(i), 251(2)(a)(ii), 251(2)(b), 251(2)(c), 251(2)(d), 251(4), 251(5), 251(5)(a), 251(5)(b), 251(6), 251(7), 251(8), 251(9), 251(10), 251(10)(a), 251(10)(b), 251(11), 251(12), 251(12)(a), 251(12)(b)

- **National Health Service and Community Care Act 1990**
  Section 3(1)(d)(vi), 3(2), 3(3), 3(3)(b), 3(3)(c), 3(4), 4, 5(1), 8(1), 8(2), 8(3), Schedule

- **United Kingdom General Data Protection Regulation**
  Articles 4(1), 4(2), 4(5), 4(11), 5(1)(a), 5(1)(c), 5(1)(f), 6(1), 6(1)(a), 6(1)(c), 6(1)(e), 7(1), 7(2), 7(3), 7(4), 9(1), 9(2), 9(2)(a), 9(2)(h), 9(2)(i), 13, 14, 28, 77
  Recitals 32, 42, 43.

Table of secondary legislation

Statutory instruments

- **Health Protection (Notification) (Wales) Regulations 2010**
  Regulation 2(1).

- **Local Health Boards (Establishment and Dissolution) (Wales) Order 2009**
  Article 7.

- **Local Health Boards (Establishment) (Wales) Order 2003**
  Article 3, Schedule.

- **Public Health Wales National Health Service Trust (Establishment) Order 2009 (SI 2009/2058)**
  Article 2, 3(2)(a), 3(2)(b), 3(2)(c), 3(2)(d)

- **The Abortion Regulations 1991 [SI 1991/499]**
  Regulation 5.

- **The Digital Health and Care Wales (Establishment and Membership) Order 2020, SI 2020/1451 (W. 313)**
  Article 1(2), Article 2, 3(a), 3(b), 3(c), 3(d), 3(e)

- **The Digital Health and Care Wales (Transfer of Staff, Property, Rights and Liabilities) Order 2021, SI 2021/233] (W. 59)**
  Article 1(2)

- **The Freedom of Information Act 2000 (Commencement No. 5) Order 2004, SI 2004/3122**
  Article 2

- **The Health Authorities (Transfer of Functions, Staff, Property, Rights and Liabilities and Abolition) (Wales) Order 2003, S.I. 2003/813 (W.98)**
  Article 3, 7.

- **The Health Education and Improvement Wales (Establishment and Constitution) Order 2017, SI 2017/913 (W. 224)**
  Article 2, 3(1)(a).

- **The Health Service (Control of Patient Information) Regulations 2002, SI 2002/1438**
  Regulation 2, 2(1), 2(1)(a), 2(1)(b), 2(1)(c), 2(1)(d), 2(1)(e), 2(1)(e)(i), 2(1)(e)(ii) 2(2), 2(2)(a), 2(2)(b), 2(2)(c), 2(2)(d), 2(3)(a), 2(3)(b), 2(4), 2(5), 3, 3(1), 3(1)(a), 3(1)(b), 3(1)(c), 3(1)(d), 3(1)(d)(i), 3(1)(d)(ii), 3(1)(d)(iii), 3(1)(d)(iv), 3(1)(d)(v), 5, 5(1), 5(1)(a), 5(1)(b), 5(2), 5(3), 7, 7(1), 7(1)(a)-(e), 7(2), Schedule

- **The Local Health Boards (Establishment and Dissolution) (Wales) Order 2009, SI 2009/778 (W. 66)**
  Article 1(2), 3, Schedule 1

- **The National Health Service (General Medical Services Contracts) (Wales) Regulations 2023, SI 2023/953 (W. 155)**
  Schedule 3, Paragraphs 79, 85, 85(1), 85(1)(a), 85(1)(b), 85, 85(3)(a), 85(3)(b).

- **The National Health Service (General Medical Services Contracts) Regulations 2015, SI 2015/1862**
  Regulation 74.

- **The Welsh Ministers (Transfer of Functions) Order 2018, S.I. 2018/644**
  Article 1(1), 1(5), 43(1).

- **Velindre National Health Service Trust (Establishment) Order 1993, SI 1993/2838**
  Article 2, Article 3(2)(a), Article 3(2)(b), Article 3(2)(c), Article 3(2)(d), Article 3(2)(f).

- **Welsh Ambulance Services National Health Service Trust (Establishment) Order 1998, SI 1998/678**
  Article 2, 3(2)(a), 3(2)(b)

Directions

- **The Digital Health and Care Wales Directions 2020 (WG20-72)**
  Paragraphs 2, 3, 3(1). 3(1)(a), 3(1)(b). 3(2), 3(3).

- **The Digital Health and Care Wales (No.2) Directions 2021 (WG21-30)].**
  - *Paragraph 2, 3, 3(1), 3(1)(a), 3(1)(b), 3(2), 3(3).*

Table of cases

- Derry City Council v. Information Commissioner [2006] UKIT EA 2006 0014
- Donoghue v. Stevenson (1932) AC 562
- Dory v. Sheffield Health Authority 11 BMLR 93.
- Dubai Aluminium v. Salaam [2003] 2 AC 366.
- Francome and another v. Mirror Group Newspapers Ltd and others [1984] 2 All ER 408.
- Fraser v. Evans and Others [1969] 1 Q.B. 349.
- Fraser v. Thames Television Ltd [I984] Q.B. 44.
- Freeman v. the Home Office (No 2) [1984] 1 Q.B. 524
- Gartside v. Outram (1857) 26 L.J.Ch. 113.
- Gillick v. West Norfolk and Wisbech Area Health Authority [1986] 1 A.C. 112.
- H (a Healthworker) v. Associated Newspapers Ltd. [2002] EWCA civ 195.
- Hewer v. Bryant [1970] 1 Q.B. 357
- Hunter v. Mann [1974] 1 QB 767.
- Initial Services Ltd v. Putterill [1968] 1 QB 396.
- Jockey Club v. Buffham [2002] EWHC 1866 (QB).
- Kennedy v. The Charity Commission [2014] 2 All ER 847.
- Lewis v. The Secretary of State for Health [2008] EWHC 2196 (QB).
- Lion Laboratories Ltd. v. Evans and Others [1985] 1 Q.B. 526.
- MacFisheries (Wholesale and Retail) Ltd v. Coventry Corpn [1957] 3 All ER 299.
- Malone v. Metropolitan Police Commissioner [1979] Ch. 344
- Marcel v. Commissioner of Police for the Metropolis [1991] 2 WLR 1118.
- Marland v. Director of Public Prosecutions [2023] EWHC 1046 (Admin).
- Montgomery v. Lanarkshire Health Board [2015] UKSC 11.
- Morison v. Moat (1861) 68 E.R. 492.
- Morris v. Murray [1991] 2 QB 6.

- Mosley v. News Group Newspapers Ltd [2008] EWHC 1777 (QB).
- Murray v. Express Newspapers plc, [2008] EWCA Civ 446.
- Nettleship v. Weston [1971] 3 All ER 581, 587.
- O. Mustad and Son v. Dosen [1964] 1 W.L.R. 109.
- Peter Pan Manufacturing Corporation v. Corsets Silhouette Ltd [l964] 1 WLR. 96.
- Powell v. Powell [1900] 1 Ch. 243.
- Printers and Finishers Ltd v. Holloway and Others [1964] 3 All ER 731
- R (Brown (formerly Bajinya) v. Governor of Belmarsh Prison [2007] EWHC 498 (Admin)
- R (on the application of Stevens) v. Plymouth City Council [2002] EWCA Civ 388.
- R (on the application of the Confederation of Passenger Transport UK) v. Humber Bridge Board 4 All ER 533.
- R (W and others) v. Secretary of State for Health (British Medical Association intervening) [2015] EWCA Civ 1034.
- R v. Chief Constable of North Wales Police, ex p Thorpe [1999] QB 396
- R v. D [1984] A.C. 778
- R v. Department of Health Ex p. Source Informatics Ltd (No.1) [1999] EWHC 510 (Admin).
- R v. Department of Health ex parte Source Informatics (CA) [2001] Q.B. 424.
- R v. Tabassum [2000] All ER (D) 649.
- Re a Company's Application [1989] 2 All ER 248.
- Re Caughey ex p. Ford (1876) 1 Ch.D 521.
- Re F (mental patient: sterilisation) [1989] 2 All ER 545.
- Re L (Vulnerable Adults: Court's Jurisdiction) (No 2) (CA) [2012] 3 WLR 1439.
- Re T (adult: refusal of medical treatment) [1992] 4 All ER 649.
- Rex (Piffs Elm Ltd) v. Commission for Local Administration in England [2024] KB 107

- Richmond Waterworks Co and Southwark and Vauxhall Waterworks Co v. Richmond (Surrey) Vestry (1876) 3 ChD 82
- Royal Bank of Scotland plc v. Etridge (No 2) [2002] 2 AC 773
- Saltman Engineering Co. Ltd. v. Campbell Engineering Co. Ltd. (1948) 65 R.P.C. 203.
- Schering Chemicals Ltd. v. Falkman Ltd. [1982] 1 Q.B. 1.
- Seager v. Copydex Ltd. [1967] 1 W.L.R. 923.
- Smith and Others v. Talktalk Telecom Group Plc [2022] EWHC 1311 (QB).
- Smith Kline & French Laboratories Ltd v. Licensing Authority (Generics (UK) Ltd and another intervening) [1989] 1 All ER 578.
- Smith v. Austin Lifts Ltd [1959] 1 All ER 81.
- South West Water Authority v. Rumble's [1985] AC 609
- Sports Direct International plc v. Rangers International Football Club plc [2016] EWHC 85 (Ch)
- St George's Healthcare NHS Trust v. S; R v. Collins and others ex parte S, [1998] 3 All ER 673.
- Stephens v. Avery [1988] Ch. 449.
- Sunderland v. Barclays Bank Ltd (1938) 5 LDAB 163.
- Taranto v. Cornelius [2001] All ER 227.
- Taylor v. Shropshire Health Authority [1998] Lloyd's Rep Med 395.
- Tchenguiz v. Director of the Serious Fraud Office [2013] EWHC 2128 (QB).
- Tweddle v. Atkinson [1861] EWHC QB J57.
- Utah Construction and Engineering Pty Ltd v. Pataky [1965] 3 All ER 650
- Various Claimants v. Wm Morrison Supermarkets plc [2020] AC 989.
- Venables v. MGN and Thompson v. MGN [2001] Fam. 430.
- W v. Egdell [1990] 1 Ch 359.
- Warren v. DSG Retail Ltd [2022] 1 All ER (Comm) 1191
- Winterbotham v. Shahrak [2024] EWHC 2633 (KB).

- Woolgar v. Chief Constable of the Sussex Police and another [1999] 3 All ER 604.
- X v. Y and others [1988] 2 All ER 648.
- YL v. Birmingham City Council and others [2007] 3 All ER 957.

Glossary of terms

Term	Meaning
Article (as a provision in legislation)	Used to describe a provision in legislation. Often only used where legislation refers to the provisions contained therein as articles.
Battery (tort of)	Intentionally and directly applying force to another person's body without any lawful justification.
Causation (law)	The need to prove that certain actions caused civil or criminal liability.
Chief Medical Officer	Senior government official (including in devolved administrations, who leads on matters of policy and operational health and social care.
Civil debt	A financial sum that a civil court has ruled is owed by a defendant in a case.
Claimants (Civil litigation)	A person applying for any relief from someone in a civil court. Prior to 1999 the claimant was called the Plaintiff.
Clauses (law)	Specific provisions in law or a legal document.
Code of practice (legal)	Principles that set out expected standards or actions in relation to an area defined in law.
Confidee	A person who has received or holds information that is subject to a duty of confidence.
Confider	Someone who imparts information importing a duty of confidence to another person.
Consolidated (consolidating Act)	An Act that combines and replaces the remaining provisions of two or more Acts of the UK Parliament, or a devolved Parliament.
contractual provisions	The legally enforceable text of a contract.
Court of Protection	A specialist court that makes specific decisions on cases relating to individuals who lack capacity.

Term	Meaning
Crown Powers	Powers exercised by the monarch or ministers on behalf of the state (e.g. the Royal Prerogative)
Defence (civil law)	One or more reasons that can be used to evidence the fact that a particular set of actions were not unlawful. (e.g. not in breach of confidence).
Defendant (Civil)	An individual that is the subject of civil proceedings.
Delegated Legislation	Law created by ministers or other bodies with the statutory authority enabling to do so provided to them by Primary Legislation, such as an Act of Parliament, or an Act of the Welsh Parliament. Otherwise referred to as secondary legislation.
Devolved (legislative powers)	The transfer of powers from one body able to pass legislation to another. For example, the transfer of powers and responsibilities from central government to a nation or region of the UK, or the exercise of powers by a devolved administration to local government. The responsibility for health and social care was devolved from central government in Westminster to the former National Assembly for Wales, now known as the Welsh Parliament.
Devolved Authority (organisational)	A public body exercising functions under the instruction of a devolved government.
Devolved Government (UK)	A government in one of the UK nations exercising functions as the executive body within a legislature to which powers have been devolved.
Direction (creating functions)	Directions that confer functions are a type of delegated legislation by which a minister of the crown (including in devolved authorities) can formally create provisions.

Term	Meaning
Discharge of functions	The performance of legal functions.
Duty of care	A legal obligation owed by one person to any other person that they will not harm or loss to them due to anything they do, or anything they fail to do, as a result of their carelessness.
Equity	Equity refers to the principle of natural justice. It is a principle of law that aims to ensures fairness and justice in the way law is applied, particularly where the common law cannot resolve a dispute fairly. Equity consists of separate legal principles, but both be applied to the same situation, in the same action. If there is a conflict between the rigid rules of law and what is fair, equity is said to prevail
Establishment Order	The Statutory Instrument by which a public authority can be created pursuant to an Act of parliament.
Ethical obligations	Standards of morality, usually defined by professional bodies to define appropriate conduct in the activities to which they relate.
Executive (Government)	The body in government that is responsible for
Fraud	To obtain benefit by a misrepresentation
Government	The government is appointed by the most senior minister in a parliament (e.g. Prime Minister, First Minister). The most senior minister in a parliament is usually the leader of the party that achieves the most representatives in the parliament in an election.

Term	Meaning
Held (judgement)	Refers to the decision in the case. The reason for that decision is known as the ratio decidendi, which literally means 'the reason for deciding'.
Implied functions (statutory body)	Functions of a statutory body that can be implied from general organisational purposes or responsibilities.
Implied statutory gateways (information sharing)	A provision in legislation that enables the sharing of information on the basis that the sharing is necessary to fulfil any statutory function,
Information governance	A framework consisting of policy and assurance that ensures that information relating to individuals is used and stored lawfully and securely in line with good practice.
Injunction	An order from a court that restrains a legal person from doing a particular act. (For example, from disclosing information subject to the duty of confidence)
Intellectual property	A type of intangible property that is the product of the thought processes of humans. Examples of intellectual property include inventions, diagrams, designs, images, names, symbols, literary works, and artistic works.
J (Judicial positions)	Refers to the title of the judge holding the title 'Justice'. For example, 'Mr Justice Jones' or in abbreviated form Jones J.
Judgement (court)	The decision of a court.
Judicial Precedent	A doctrine that requires judges to follow the decisions of cases in specified courts of higher authority.

Term	Meaning
Judicial review	The review of the actions of an administrative body by a court. In the event the court has acted ultra vires the court can give a declaration of that fact, impose an order, or make an award to any party that has been detrimentally affected.
Law Commission	A statutory independent body created by the Law Commissions Act 1965 to review elements of the law of England and Wales and make recommendations to Parliament.
Lawful	Acting in accordance with the law.
legal excuse	Acting lawfully because of a legal defence.
legal persons	Any person or body that exists as a legal entity and therefore is capable of being sued.
Legislation	Laws passed by the legislature, or in the case of secondary legislation, laws passed by virtue of powers given to another person (e.g. a minister)
Legislative Competence (Welsh Parliament)	Refers to the extent of legal powers devolved to the Welsh Parliament, and the extent to which they can be exercised. Passing legislation in a non-devolved area of law would be outside of the legislative competence of the Welsh Parliament and the legislation would be ultra vires and therefore non effective.
M.R. or MR	Post nominal letters that signify that the holder is the holder of office of 'The Keeper of the Master of the Rolls and Records of the Chancery of England', or 'Master of the Rolls' in its commonly used form. The holder is the President of the Civil Division of the Court of Appeal of England and Wales and Head of Civil Justice

Term	Meaning
Master of the Rolls	The commonly used title for the office of the Keeper or Master of the Rolls and Records of the Chancery of England, known as the Master of the Rolls, is the President of the Civil Division of the Court of Appeal of England and Wales and Head of Civil Justice
medical ethics	Standards of morality, defined by professional bodies that determine what is considered appropriate conduct in the provision of any medical or other services. It includes connected activities such as the undertaking of medical trials and the use of information for research.
Misrepresentation (law)	A false statement of material fact that influences a decision.
National Data Guardian	A position created in Statute under The Health and Social Care (National Data Guardian) Act 2018 to advise health and adult social care bodies in England on the safe and ethical use of data.
Negligence	A tort which occurs when a person breaches a duty of care that results in damage or harm.
Obiter Dictum	(Latin) Meaning 'other things said'. Referring to things 'said in passing' that do not relate to the decision in the case and do not create a judicial precedent.
Obligation (legal)	An Act that someone is required to do by law (e.g. register a birth), or a duty in law that requires people not to do something (e.g. cause harm by negligence).
Order (legislation)	A Statutory Instrument that usually

Term	Meaning
Paragraph (number) (in legislation)	Used to denote specific provision in some legislation. More commonly a point of reference in schedules to legislation but sometimes used with varying consistency in other cases.
Parent Act	An Act that provides that secondary legislation to be created by a specific minister or body.
Plaintiff	A person applying for any relief from someone in a civil court prior to 1999. Not referred to as a Claimant.
Powers of Attorney	A legal power that grants authority for an individual to act for another person in specified matters.
Prima facie	(Latin) Meaning 'at first appearance'. In law the term is often used to describe something that is conclusive on first appearances but is not necessarily conclusive.
Primary legal sources	Documented sources of law maintained by bodies recognised as providing an authoritative account of those sources.
privity of contract	The principle that a person who is not party to a contract cannot enforce its terms.
Provision (legislation)	A general term that refers to the substance of any text of any legislation.
Public authorities	A publicly funded legal person that performs duties set out in Statute, or other activities consistent with functions of national, devolved or local government.

Term	Meaning
Queens Council / Q.C.	An award given to exceptional barristers, and solicitors (since 1995) when serving under a female monarch. The award provides recognition of their status as a senior lawyer given their competence in complex advocacy cases. The title is recognised in court. All holders of the title became Kings Counsel (or K.C.) on the death of Queen Elizabeth the second.
Ratio decidendi	(Latin) Meaning 'the rationale for the decision'. The term describes the reasons for the outcome of a case. Where it creates a judicial precedent, the ratio decidendi is binding on lower courts.
Regulation	A Statutory Instrument. The effect of a Regulation can be the same as that of any Statutory Instrument. Regulations usually create new law in the area permitted
Regulation (as a provision)	Used to describe a provision in Regulations established under Statute, unless otherwise defined by the more generic term 'article' therein.
Repeal	The act of removing or cancelling legal instruments, such as Statute or any legal instrument (e.g. Statutory Instrument, Direction etc). Also known as 'Revoking'.
Revoking (legislation)	The act of removing or cancelling legal instruments, such as Statute or any legal instrument (e.g. Statutory Instrument, Direction etc). Also known as 'Repealing'.

Term	Meaning
Secondary Legislation	Law created by ministers or other bodies with the statutory authority enabling to do so provided to them by Primary Legislation, such as an Act of Parliament, or an Act of the Welsh Parliament. Otherwise referred to as delegated legislation.
Set aside (an obligation)	Relates to the ability to be able to discount any legal obligation certain circumstances as provided by law. The obligation is not removed.
Statute	Legislation passed by a legislature.
statutory body	A legal body created by Statute / legislation.
statutory function	Those functions to undertake certain tasks or to have certain obligations, as conferred on a body by law.
Statutory Instrument	Secondary or subordinate legislation that can be created by Ministers of the UK Parliament or by devolved administrations or by His Majesty, with the power to do so having been permitted by primary legislation.
statutory interpretation	The set of principles by which judges interpret statutory provisions. Some methodology is derived from specific Statute's such as the Interpretation Act 1978, others by judicial precedent itself.
statutory provision	The text that appears in any law produced by a legislative body.
Subordinate Legislation	Legislation such as Statutory Instruments that are made by persons or bodies, with the power to do so having been permitted by primary legislation.
Sue / Sued	To instigate any legal proceedings against another person.

Term	Meaning
Tort	A wrongful act, or breach of a civil duty, other than under contract.
Trade secret	A type of intellectual property (IP) that has an economic value owing to the competitive advantage is maintains. A trade secret can include processes, designs, patterns, tools, instruments, working practices or information that is not generally known and is being protected by the owner of the secret.
Ultra Vires	(Latin) Meaning 'beyond power'. Used to describe the act of a person acting outside of their legal powers. Intra vires refers to a person with acting within their legal powers.
Unbroken chain of causation (civil law)	A concept that in order to succeed in an action, the cause and effect of the event undertaken by a defendant must have caused the result that any claim is seeking to remedy.
V.C. or VC	Post nominal letters that signify that the holder is the holder of office of Vice Chancellor. A position currently known as The Chancellor of the High Court. The holder is the President of the Chancery Division of the High Court and vice-president of the Court of Protection.
Vicariously liable	Where one person is liable for the acts of another due to a specific relationship (usually an employment relationship).
Vice Chancellor	The position currently known as The Chancellor of the High Court. The holder is the President of the Chancery Division of the High Court and vice-president of the Court of Protection.

Term	Meaning
Volenti non fit injuria'	(Latin) Meaning 'to a volunteer, injury is not done'. The maxim refers to the defence of consent, and the principle that if someone consents, there is no actionable breach.
Waive (duty of care)	Where a person relinquishes their right to sue a person who owes them a duty of care in the event of harm.
Welsh Government	Consisting of Welsh Ministers and the Welsh Government Civil Service, it is the executive body in the Welsh Parliament that creates and coordinates policy and law on behalf of a legislature.
Welsh Ministers	Members of the Welsh Government, the executive body in the Welsh Parliament. See 'Government',

Glossary of abbreviations of law reports

Abbreviation	Report title
A.C.	Law Reports, Appeal Cases (Third Series) (1891-)
All ER	All England Law Reports (1936-)
All ER (Comm)	All England Law Reports (Commercial Cases) (1998-)
All ER Rep	All England Law Reports Reprint (1558-1935)
BMLR	Butterworths Medico-Legal Reports (1992-)
Ch	Law Reports, Chancery Division (3rd Series) (1890-)
Ch.D.	Law Reports, Chancery Division (2nd Series) (1875-1890)
D	Dunlop's Session Cases (1838-1862)
EWCA civ	Court of Appeal (Civil Division) [Neutral Citation] (2000-)
EWHC	England & Wales High Court (Administrative Court) [Neutral Citation] (2000-2001)
EWHC (QB)	England & Wales High Court (Queen's Bench Division) [Neutral Citation] (2001-)
F.S.R.	Fleet Street Reports (1963-)
Fam	Family Law (1971-)
IP&T Digest	Intellectual Property and Technology (Digest)
K.B.	Law Reports, King's Bench (1901-1952, 2022-)
L.D.A.B.	Legal Decisions Affecting Bankers (1900-2001)
L.J.Ch.	Law Journal Reports, Chancery New Series (1831-1946)
Lloyd's Rep Med	Lloyd's Law Reports Medical (1998-2006)
Mac. & G.25	Macnaghten & Gordon's Chancery Reports (1848-1851)
Q.B	Law Reports, Queen's Bench (1891-1901, 1952-2022)
QBD	Law Reports, Queen's Bench Division (1875-1890)
R.P.C.	Reports of Patent, Design and Trade Mark Cases (1884-)
UKHL	United Kingdom House of Lords [Neutral Citation] (2000-2009)
UKIT	UK Information Tribunal (2010-)
WLR	Weekly Law Reports (1953-)

1. The common law duty of confidence, and the use of information in the health service in Wales

1.1 Introduction

'Confidentiality' is a concept that is embedded in healthcare processes. As a matter of common knowledge, with no need for reference, it is a common assumption that medical professionals are subject to The Hippocratic Oath. Attributed to the Greek physician Hippocrates, The Hippocratic Oath was written just under 2500 years ago. The oath is a pledge, by a physician, to *'Apollo the Physician and Asclepius and Hygieia and Panaceia and all the gods and goddesses* [1]' to maintain a catalogue of medical ethics while undertaking their medical duties. Part of the Hippocratic Oath includes the statement:

> 'What I may see or hear in the course of the treatment or even outside of the treatment in regard to the life of men, which on no account one must spread abroad, I will keep to myself holding such things shameful to be spoken about [1].'

This position is echoed in modern guidance such as the General Medical Councils current guidance on Good Medical practice which states:

> 'You must treat information about patients as confidential, including after a patient has died. [2].'

An obligation of confidence exists in law and furthermore a doctor cannot volunteer information obtained "save in very exceptional circumstances [3]". The development of the law relating to confidentiality is more apparent in more recent history. Cases such as Wyatt v. Wilson [4] in the early nineteenth century are illustrative of the concept that medical privacy in the law [4]. Referring to an etching made by George III as appeared in the Kings diary, Lord Eldon stated:

> 'If one of the late king's physicians had kept a diary of what he heard and saw, this Court would not, in the king's lifetime, have permitted him to print and publish it [4].'

When reporting to Parliament on the Common Law duty of confidence, The Law Commission concluded [5] that the origins of the current common law principles relating to the concept of the duty of confidence could be traced to two cases in particular, these were, Prince Albert v. Strange [6] and Morison v. Moat [7].

In Albert v. Strange [6], Prince Albert was successful in obtaining an injunction for the return of private drawings and etchings produced by Queen Victoria and Prince Albert and for preventing the publication of a catalogue detailing them.

Distinguishing the issue of the rights to the property with that of those of trust, confidence or contract, Lord Cottenham, then Lord Chancellor, stated that:

> 'Upon the first question therefore, that of property, I am clearly of opinion that the exclusive right and interest of the Plaintiff in the composition or work in question being established... ...and there being no right or interest whatever in the Defendant, the Plaintiff is entitled to the injunction of this Court to protect him against the invasion of such right and interest by the Defendant, which the publication of any catalogue would undoubted be; but this case by no means depends solely upon the question of property, for a breach of trust, confidence, or contract, would of itself entitle the Plaintiff to an injunction [8]'

In the latter case of Morison v. Moat [7], an injunction was granted to stop the defendants, the son of a former partner in the plaintiff's business, producing and selling a medicine made to a secret formula developed by the partnership. The case demonstrates the wider set of circumstances to which the obligation extended.

Prior to the creation of the National Health Service, it could be speculated that confidentiality considerations were often limited to the direct care relationship and the treatment of individuals. There were no national bodies to manage the general provision of healthcare services. On creation of a national system, the paper system could be assumed to

have limitations in how information could be used for the benefit of patients, with relevant information relating to a patient's health remaining in the records of those parties treating the patients with a likelihood that they would never be disclosed to anyone outside of their discipline.

Digital technology however could be assumed to have numerous benefits to ensure that patient care is delivered safely and efficiently, with any relevant information being retrievable wherever the person is seen. It could also be suggested that in having easier ways of compiling digital information for the purpose of improving healthcare, data can be better used to plan services and to ensure they are more effective. Particularly where information is shared outside of the healthcare environment, the understanding of the common law duty of confidence could be said to be key. The use of this information must be lawful. If it is not, it not only creates a potential for liability in Tort, but it could breach the first data protection principle as relates to lawful processing [9].

A number of publications do exist that define confidentiality in a healthcare setting; however, it is recognised that there is a distinction between what the law says and what good practice guidance says [10]. Academics have also recognised that there is sometimes conflicting advice between the guidance produced by different professional bodies [10], with differences in approach often confusing those who need to apply the law to scenarios [11]. This position is not limited to the few academic papers that have observed the issue. Where the UK Governments Department of Health tried to uphold the principles of their confidentiality guidance in the courts, the courts found that the policy position did not reflect the legal position. [12]. To this end, the author assumes that the difference between the law and the guidance is a reflection of differing ethical views on policy and how individuals should act in certain positions in a health service, and how these can contrast with legal principles.

More information relating to the rationale for this thesis is described below.

1.2 Purpose

1.2.1 Aims and objectives

The aim of this thesis is to set out the elements of the common law duty of confidence, and specifically to examine when disclosures can be made lawfully in various scenarios within the National Health Service in Wales. In order to deliver the aims of this thesis, the specific objectives of the work are:

- To review the relevant common law cases concerning the duty of confidence.
- To examine the statutory provisions that impact on the common law duty of confidence.
- To provide a detailed legal analysis of the operation of the common law duty of confidence as applies to healthcare in Wales.

1.2.2 The need for the research

In delivering his judgement in Kennedy v. The Charity Commission [13], Lord Mance said:

> 'Information is the key to sound decision-making, to accountability and development; it underpins democracy and assists in combatting poverty, oppression, corruption, prejudice and inefficiency. Administrators, judges, arbitrators, and persons conducting inquiries and investigations depend upon it; likewise, the press, NGOs and individuals concerned to report on issues of public interest. Unwillingness to disclose information may arise through habits of secrecy or reasons of self-protection. But information can be genuinely private, confidential or sensitive, and these interests merit respect in their own right and, in the case of those who depend on information to fulfil their functions, because this may not otherwise be forthcoming [14].'

The author of this thesis works in a senior information governance role in Digital Health and Care Wales. The purpose of undertaking the research originated from internal discussions following numerous incidents where there was uncertainty as to whether disclosures could be made lawfully without being in breach of confidence. The author can attest that there are often misconceptions as to what constitutes law and what represents good practice in certain situational scenarios with the result that where data can be lawfully shared, there is a high degree of doubt. There are no papers that explain the extent of the issue, but with the need to exploit the benefits of data in a modern NHS, there is internal recognition of the issue. The author can attest that it is perceived from within the service that there is often a confusion between the professional obligations of individuals in certain use cases, and organisational use of information for the operation of a joined-up health service. In particular, the following is observed:

- As of 30th October 2024, there are currently no fully referenced academic texts that provide a comprehensive explanation of the common law duty of confidence as applies to the use of information in the Health Service in Wales, particularly in relation to the defences of consent or the defence that a disclosure was made in the public interest.
- There have been no studies that have looked at the provisions of Section 251 of the National Health Service Act 2006 either before the functions were devolved to Welsh Ministers or after functions were devolved to Welsh Ministers to explore what the provisions say about Regulations that can be established.
- There are no academic texts that describe the full Health Service (Control of Patient Information) Regulations 2002 and describe their general application in relation to Wales.
- There is no specific legal text that describes the formation of the statutory bodies in Wales, and how data can be disclosed lawfully to those bodies in line with their statutory functions.

- There is no guidance nor any academic texts that describe the powers of Digital Health and Care Wales, or how it can operate efficiently and lawfully as a central digital function.

The issue of public bodies not understanding the law is not restricted to Wales. In October 2014 the report 'Data Sharing between Public Bodies, A Scoping Report [15]' was laid before parliament. Among findings, it found that many of the issues in effective data sharing in the health sector in all of the UK countries were as a result of a misunderstanding of the common law duty of confidence [16]. It noted that much of this confusion was mainly driven by the approach to confidentiality taken by the health professions, who impose specific approaches to confidentiality that extend beyond the scope of the common law requirements [16] and extends to professional duties subject to professional Regulation [17],

This Ph.D. has been partly funded by Digital Health and Care Wales, and its predecessor organisation the former NHS Wales Informatics Services through the Wales Institute of Digital Information and the University of Wales Trinity Saint David in a strategic alliance. The thesis aims to clarify the common law duty of confidence as applies to the use of information in the NHS in Wales.

1.3 Research and scope

1.3.1 Research questions

The title of this thesis is as follows:

> "The Common Law Duty of Confidence and the Use of Information in Healthcare in Wales".

This is a broad title, but essentially can be answered in the following research questions:

Duty of confidence

- When is information that relates to an individual subject to the duty of confidence?

Defences: consent

- What is the definition of a valid consent, and in what circumstances can it be applied?

Defences: public interest

- What is the definition of a public interest disclosure, in what known circumstances can it be applied?

Legal mechanisms for sharing in the NHS

- What types of Regulation can be created under Section 251 of the National Health Service Act 2006, and how to those provisions apply in Wales?
- What current Regulations exist under Section 251 of the National Health Service Act 2006, and what do they relate to?

Statutory functions, disclosures and use of information

- How do the crown powers, ministerial powers and statutory functions enable organisations to have information disclosed to them lawfully?
- How are statutory bodies in NHS Wales organised and how can statutory functions enable the lawful sharing of data?
- What legal mechanisms are there to enable Welsh bodies to request that NHS England undertake work to establish information systems on their behalf?

Questions as relate to the case study

- How was Digital Health and Care Wales Established, and how do its functions enable it to receive information subject to the duty of confidence?

- What disadvantage does Digital Health and Care Wales have in mandating the provision of data, and what possible solutions may be available to the organisation in its current form?

1.3.2 The scope of the research

The thesis will explore specific areas of the common law duty of confidence in order to define certain areas of the law. It is not the intention to thoroughly define the law, and the information is presented with the caveat that other areas of the law will also need to be considered.

The scope and structure are set out as follows:

- **Common law duty of confidence**

  The scope of the chapter includes:

  - Defining the duty of confidence as relates the confidential information that relates to individuals, with references to health data where appropriate.

  - Setting out the elements as relate to a potential breach of confidence in the following areas:

    - **Quality of confidence:** To explain relevant factors that are worthy of consideration, including:
      - The format of information
      - The effect of trivial confidences
      - The effect of information entering the public domain
      - The effect of anonymisation
      - The effect of death on confidential information
      - Such other incidental information that is of note, and relevant to the subject.

        - **Imparted in circumstances importing an obligation of confidence':** To explain when information is imparted with reference to the case law, and the various factors, including relationships as are relevant to imparting information.

        - **Breach of confidence:** Defining a breach of confidence and explaining the circumstances by which a breach of confidence may arise. Where there are breaches of the duty of confidence in relation to personal information, an explanation how this will also result in a breach of the UK GDPR.

    - The impact on the Human Rights Act 1998 and the action for misuse of private information as relates to any information that is private but may not be subject to the duty of confidence is not in scope of this thesis. The broader implications of the Human Rights Act 1998, including case law, will be made where it is relevant to areas of the text of this thesis.

- **Defences: consent**

    The scope of the chapter includes:

    - Defining valid consent as set out in general common law principles, acknowledging the lack of case law in relation to the duty of confidence.

    - Setting out the components for consent including:

        - **Knowledge:**
            - Defining the expectation as relates to knowledge and the concepts applied in relation to any express and complied consent.
            - The concept of reasonable expectations

- The impact of a misrepresentation on knowledge.
- An overview of key principles as relates to capacity, including at high level, and overview of the Mental Capacity Act 2005, and the law that creates considerations at common law in relation to adults and children.
- It is not intended to provide a detailed commentary beyond the effect of the Mental Capacity Act 2005 on capacity as this is a developed area. Discussions on the Power of Attorney and the operation of the Court of Protection are for this reason also out of scope of this thesis.

- **Freely given consent:**
  - Defining freely given consent
  - Describing how relationships can affect freely given consent
  - Explaining the effect of undue influence on whether consent has been freely given

- **Signifying consent:**
  - Demonstrating the ways consent can be signified.

- To explain the relevance of consent at common law, and how the two regimes operate in practice.

- **Defences: public interest**

The scope of the chapter includes:

- To define what is meant by a public interest disclosure.
- To illustrate where public interest defences have been applied.
- To set out the basic principle of the public interest test
- To explain the relevance of the timing of a disclosure and the parties to that disclosure.

- Setting out how the public interest test applies in the public sector,
- Explaining why the public interest test is relevant to any request for information under the Freedom of Information Act 2000.
- The two areas of public interest defence that relate to the administration of justice and national security are not in the scope of this thesis.

- **Defences: lawful Disclosures – disclosures permitted or required by Statute**

The scope of the chapter includes:

- Defining the purpose of Section 251 of the National Health Service Act 2006.
- Explaining the provisions that devolve functions to the Welsh Ministers.
- Explaining the powers conferred by the Act.
- Describing current Regulation under the Act, and in particular:
  - The scope of the Regulations
  - The effect on the common law duty of confidence
  - A high-level description of the operation and effect of Regulation 2 as relates to collections of information as relates to neoplasia,
  - A high-level description of the law and effect of Regulation 3 as relates to communicable diseases and other risks to public health, with a high-level overview of their use, considering the provisions contained in the Regulation, and the effect of a notice to process information.
  - An outline of the purpose of Regulation 5, and how it operates. As a well-known mechanism for setting aside the duty of confidence, the operation of Regulation 5 and

associated provisions are outside of the scope of this thesis.

- **Lawful disclosures: statutory functions**

The scope of the chapter includes:

- Describing the types of statutory gateway that may exist that enable confidential information to be acquired or disclosed in certain circumstances.
- Explaining other gateways that may be available that derive from government, but only to the extent as to explain their existence.
- Describing how the statutory bodies in Wales were formed and are organised at a high level. The specific functions of Health Boards and NHS Trusts in Wales, or the Functions of Health Education Improvement Wales, are not considered.
- Describing The Welsh Ministers powers to direct NHS organisations and in particular:
  - The statutory provisions that relate to specific directions
  - The format of directions
  - The amendment or revocation of directions
- Explaining how information can be lawfully disclosed to NHS England where they receive a request to create an information system on behalf of any other person, including where that 'other person' is a part of the NHS in Wales.
- Highlighting the impact of the Human Rights Act 1998 on statutory functions of a public authority.

- **Central digital functions in Wales: a case study**

The scope of the chapter includes:

- Explaining how Digital Health and Care Wales:
  - Is established in law

- Its functions and directions as apply to the use of information subject to the duty of confidence.
- The role of Digital Health and Care Wales
- How its functions enable it to have data disclosed to it lawfully despite the duty of confidence
- Difficulties with the established model in comparison with the powers enjoyed by NHS England, and potential solutions that could be applied with Digital Health Wales existing in its current form.

While incidental reference to the UK GDPR will be used to illustrate how the common law duty of confidence and the UK GDPR interact. A comprehensive description of provisions in the UK GDPR is outside of the scope of this thesis. Where personal data is processed, it is important to caveat that further UK GDPR considerations may apply based on the circumstances.

1.4 Research strategy

1.4.1 Research methodology

As this research is centred around researching the law, and is not specifically interested in ethical opinions, good practice guidance, or opinions as to what the law relating to confidentiality should be, this thesis uses a combination of doctrinal methodology and empirical methodology to review the law.

The doctrinal methodology is interested in the law as it presents itself and is not biased on sociolegal views such as ethics as may apply in certain scenarios. In connection with this approach, professional guidance is out of scope of this thesis. This traditional 'black letter' approach will enable sources of law to be researched and then presented

in an organised for that sets out the legal rules. Research in this manner is a core element of legal training.

The empirical element to the research will be qualitative legal research. This will be limited to establishing the legal rules from texts of cases and other documents as relate to the subject in hand.

The research does not seek to undertake a sociological study of the law or incorporate any views that fall outside of the legal principles of the duty of confidence. The thesis itself forms a review of the literature by definition of its construction and approach.

1.4.2 Approach to reviewing the literature

Given the research methodology and the intention to review primary legal sources, these resources will be reviewed in a manner which is consistent with legal research. The sources researched have been retrieved using standard legal research methods, including databases such a s LexisNexis and Westlaw.

1.4.3 Research limitations

As with any legal research, the answer to the research question is limited to the case law that can be identified and accessed.

1.5 Contribution to knowledge

As discussed in this chapter, information sharing causes many issues, due to uncertainty around whether that sharing is lawful at common law. Confidentiality guidance can be inconsistent as it relies on ethical principles and policy positions that do not reflect the law.

Given a clear remit of clarifying the specific common law principles, this thesis creates a new and substantial body of knowledge through original research of primary legal sources. The thesis:

- Provides a basic set of principles relevant to the NHS, that will contribute to a better understanding as to whether information is confidential.
- Provides an academic text systemising and explaining comprehensively existing knowledge in relation to the defence of consent as relates to the duty of confidence in the healthcare context.
- Provides an academic text systemising and explaining comprehensively existing knowledge in relation to the public interest defence as relates to the duty of confidence in the healthcare context.
- Represents the first comprehensive academic text of the powers to the Secretary of State for Health in England and the Welsh Ministers under section 251 of the National Health Services Wales Act 2006. The Chapter also describes the regulations currently in force.
- Provides an academic text systemising and explaining comprehensively existing knowledge in relation to the public law, and how this enables data to be shared or obtained lawfully where there is a duty of confidence. The chapter also represents the first comprehensive academic text of the basic statutory functions in place in NHS Wales and how these can enable data to be shared or obtained lawfully by NHS statutory bodies where there is a duty of confidence.
- Represents the first comprehensive academic text of the powers of Digital Health and Care Wales and how data can be lawfully used in line with those powers.

The research will be used to create guidance for information governance, and other leads in Wales. Most of this guidance will be created after this thesis has been submitted. Such guidance will be subject to consultation.

1.6 Generic information

1.6.1 Gender and numbers in the law

Modern usage of language is sensitive to gender and linguistic preferences in pronouns and explanation. The law and legal frameworks retain the generic use of "he" for most situations, although occasionally, “she” is used. Section 6 of the Interpretation Act 1978 provides that:

> ‘In any Act, unless the contrary intention appears:
>
> (a) Words importing the masculine gender include the feminine.
> (b) Words importing the feminine gender include the masculine.
> (c) Words in the singular include the plural and words in the plural include the singular [18].’

In order actively to quote the law as stated, the transcriptions in this thesis retain the gender provided by the published edition, which will apply to both genders unless the contrary is stated.

1.6.2 Time horizon

The case law was collected at multiple points in time, however a search for any updates to case law in the form of new cases was conducted on the 30th of October 2024. Practical constraints in any legal research will exist in ensuring the law will be as up to date as there will always be a delay in the publication of the law reports, and over time the study would in itself need to be updated. The law is therefore stated as correct as of 30th October 2024.

2. The duty of confidence

2.1 Introduction

In variety of situations in life, members of the public will be assured that their information will be treated confidentially. To many it could be the case that they assume that any information they provide to an organisation is confidential and will not be passed on to third parties or used for any other purpose. It is not the purpose of this study to establish what people think this refers to, but it could be suggested that many people would be of the view that this means that any information provided to an individual will not be passed on to another individual without their consent. In such circumstances, confidentiality would be more accurately described as something that relates to ethics or information security.

Where information relates to individuals many people will be familiar with the term 'data protection' if not the legislation itself. It could be said that the discussions that took place prior to the commencement of the General Data Protection Regulation [19] and Data Protection Act 2018 [20] brought data protection back into the media spotlight, and to many this may assure them that their information will be kept safe and secure, and they will have a route of complaint in the event that anyone loses or misuses their data.

The common law duty of confidence however is not solely concerned with personal information, and what is actually confidential at common law does not necessarily correlate to what is considered special category data within the meaning of the UK General Data Protection Regulation [21] or the Data Protection Act 2018 [20]. For example, a trade secret as falls within the scope of the common law duty of confidence [22] is not personal data within the meaning of the UK General Data Protection Regulation [23] which provides that:

> *'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person* [23]'

It is true that where data is unlawfully processed at common law, and that data consists of personal data within the meaning of the UK General Data Protection Regulation [24] that this may breach the first data protection principle which provides that:

> 'Personal data shall be:
>
> processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency') [9]'.

The requirements of article 6 with regard lawfulness of processing, and the exceptions to the prohibition on disclosing special category data contained in Article 9 of the GDPR are not within the scope of this research.

With the UK GDPR however, a data subject has a right to complain to the Information Commissioner if they suspect a breach [25]. With regards to a breach of the common law duty of confidence, however, there is no single body to which you can complain. Instead, the courts provide remedies to breaches, such as injunctions that stop confidential information being disclosed, or damages to compensate any loss, harm or embarrassment that a disclosure has caused. It is not proposed to discuss the remedies in any level of detail as part of this study. The emphasis will be placed on the law and disclosure mechanisms that may be available where confidential information is to be disclosed.

In the role of the information governance professional working in the National Health Service, given the nature of the business of the service, they will need to consistently be aware that certain types of information

will be subject to the protection of the common law duty of confidence. To ignore the fact that information is confidential may mean that the disclosure is unlawful at common law, and in the case of personal data, it could also breach the first data protection principle.

2.2 Rationale for establishing confidentiality

Healthcare professionals have robust good practice documentation issued to them by their professional bodies and regulating bodies to assist them on complying with their legal and ethical obligations, as well as ensuring that they meet the professional standards expected of them. For example, the British Medical Association as a trade union and professional body for doctors and medical students has published an 'Ethics Toolkit on Confidentiality' [26]. The General Medical Council, the independent regulator for doctors in the UK, published its good practice guidance entitled 'Confidentiality: good practice in handling patient information' [27].

Outside of the direct care relationship, organisations need to obtain and disseminate information from time to time, and for this purpose, where information is confidential, it is necessary to establish a lawful reason to disclose that information. Where information is not confidential, even where it is identifiable, the common law duty of confidence is not engaged. Whether or not that disclosure is ethical, or whether any other legislative requirements, such as the UK General Data Protection Regulation apply is a separate consideration. As a starting point it is useful therefore to define confidential information that is be subject to the common law duty of confidence, and those circumstances where information ceases to be confidential.

This chapter takes a broad approach to the topic, as the source of information will be relevant to any disclosure further down the line. Further chapters will concentrate more specifically on how data that is subject to the common law duty of confidence can be disclosed lawfully.

2.3 The importance of maintaining confidentiality

If any information is subject to the duty of confidence, it is important to ensure that it remains so, and no unlawful disclosures are made. The importance of maintaining this duty was summarised very concisely by Lord Bingham in the Court of Appeal in A.G. v. Guardian Newspapers [1988] [28], where he stated:

> 'It is a well-settled principle of law that where one party (the confidant) acquires confidential information from or during his service with, or by virtue of his relationship with, another (the confider), in circumstances importing a duty of confidence, the confidant is not ordinarily at liberty to divulge that information to a third party without the consent or against the wishes of the confider. The essence of the confidant's duty is to preserve the confidentiality of the confider's information [28].'

In addition to being a breach of the common law, as mentioned above, an if the common law duty of confidence is breached, this will breach the first data protection principle in the UK GDPR [9].

2.4 What is subject to the duty of confidence?

As outlined at the start of the chapter, the 'confidential' is a commonly used term and in many circumstances reassures that information is going to be kept safe and secure, regardless of whether it is actually subject to the common law duty of confidence.

Even legislation sometimes uses the term 'Confidential' to refer to information that is not subject to the duty of confidence, and it could be suggested that this could be confusing to some people. For example, Section 256(1) of the Health and Social Care Act 2012 has the title 'Requests for collection under section 255: confidential information'. It then defines a process known as a 'confidential collection request as being:

> '….a request for NHS England to establish and operate a system for the collection of information which is in a form which—
>
> (a)identifies any individual to whom the information relates who is not an individual who provides health care or adult social care, or
> (b)enables the identity of such an individual to be ascertained [29]'.

The provision, in theory, includes any information.

While the general principals of what constitutes the confidential information of patients in a health environment could appear well established, in order to ensure legal compliance, it is necessary to look at the common law.

The case of Coco v. A.N. Clark (Engineers) Limited [22] remains significant in explaining the features of information that is subject to the duty of confidence, in order for it to be defined with more certainty. The case related to a trade secret, the design of a moped engine. In assessing whether the designs of the engine were subject to the duty of confidence, Megarry J stated:

> 'In my judgment, three elements are normally required if, apart from contract, a case of breach of confidence is to succeed. First, the information itself, in the words of Lord Greene, M.R. in the Saltman case on page 215, must "have the necessary quality of confidence about it". Secondly, that information must have been imparted in circumstances importing an obligation of confidence. Thirdly, there must be an unauthorised use of that information to the detriment of the party communicating it [22]'.

Or to put more concisely, to be confidential information:

1. must have the *"necessary quality of confidence about it* [22]"
2. have been *"imparted in circumstances importing an obligation of confidence* [22]"; and
3. there must be an unauthorised use of that information to the detriment of the party communicating it [22].

The following paragraphs explore these principles in some detail.

2.5 The quality of confidence

2.5.1 Definition

If information is to be considered confidential, the information *"must have the necessary quality of confidence about it* [30]*".*

This relates to the information itself, and whether the information is of the type in question, although there could be overlap with how the information was 'imparted' in order to come to the conclusion as described below.

2.5.2 The general rule

In general, information as relates to an individual's health will usually be confidential. This in itself will usually be enough to demonstrate that information has the quality of confidence. In Venables and another v. Mirror Group Newspapers, Dame Elizabeth Butler-Sloss summed this up quite concisely:

> 'All information about the claimants, whether during their detention or at any other time, whether by records or otherwise, which relates to their medical, psychological, or therapeutic care is, in principle, confidential. That confidentiality would, in my view, extend to art, or any other form of therapy, and to all those taking part in group therapy, and not only the therapist [31].'

The overlap between the first principle with regard having the quality of confidence, and the second principle with regard being imparted in circumstances importing a quality of confidence is clear in these circumstances.

2.5.3 The format of the information

It is clear that information may have the quality of confidence regardless of the format it exists in.

2.5.3.1 Information conveyed verbally

Information that is conveyed by word of mouth can still have the quality of confidence. In Seager v. Copydex Ltd. [32] the verbal descriptions of an invention that accompanied rough sketches were found to have the quality of confidence. In a healthcare setting therefore, it is clear that symptomatic information relayed by patients, the diagnosis by a health professional, discussions in multi-disciplinary teams meetings, or any other information that may be conveyed in discussions by healthcare professionals is capable of having the quality of confidence, and this need not rely on any tangible information stored elsewhere, such as recordings, health records, scans, photographs or the like that may exist. It follows that repeating information overheard or conveyed directly by word of mouth without a legitimate reason to do so could be in breach of confidence.

2.5.3.2 Records, etchings, sounds and recordings

Information stored in a more permanent form the impact of a disclosure of the information has a higher impact than information passed by word of mouth [33]. The headings below provide an illustration that the format in which physical information is held is not a dependency when determining whether the quality of confidence exists.

Photographs and audio and video recordings

Photographs, audio and video recordings containing information that has the quality of confidence can, by their very nature, be seen to be more

acutely sensitive in circumstances where these go beyond just providing an account of the confidential information [33].

According to Waller LJ in D v. L [34]:

> ‘Just as a photograph can make a greater impact than an account of the matter depicted by that photograph, so the recorded details of the very words of a private conversation can make more impact, and cause greater embarrassment and distress, than a mere account of the conversation in question. [33]’

While there is not much case law that discusses the sensitivity of the various methods, it could be suggested that the sensitivity of the photograph, audio or video recording will depend on what they portray, and the circumstances to which they relate. For example, an audio recording of the call to a GP surgery to book an appointment may not contain any confidential information, but it is inevitable that a recording of a consultation will. Recordings of full consultations will inevitably include information in the patient’s own words together with any diagnosis or treatment provided at the consultation. Other information confidential information may be provided that is not relevant to the consultation that will not appear in the patient record but is nevertheless confidential.

Likewise, a photograph of a member of the public on a general NHS site that exhibits no indication of any condition or illness, whereas a photograph of any individual leaving a cancer clinic, or drug rehabilitation clinic could be confidential. The latter example was exhibited in the case of Campell v. Mirror Group Newspapers [35], where the Mirror newspaper published an article with the headline ‘Naomi: I am a drug addict’ accompanied by a photograph of the fashion model Naomi Campbell outside a drug rehabilitation clinic over the caption 'Therapy: Naomi outside meeting'. It was noted that while the venue was not named specifically, anyone was familiar with the area would have recognised the location of the meeting [36].

Given the above information, identifiable images such of those images providing the name of the patient, particularly that display bones, body parts, or symptoms of medical conditions would be particularly sensitive. This could relate to x-rays, photographs of injuries, scans and screening images.

There is even less guidance in the case law as to video recordings. It could be suggested however, where a video recording exists it could be suggested that there would usually be an elevated quality of confidence where this accompanied by video. It could further be suggested that such information is much more sensitive than photographs or videos alone. Nevertheless, all could have the characteristics of information that possesses the quality of confidence, and these factors may be of more use when assessing the harm suffered.

Health records and medical reports

More obviously, health records have the quality of confidence. The same applied to opinions in a medical report [37].

It could be suggested that health records, or official documents that identify patients, their conditions and their treatment would be more sensitive than unofficial documents. That is, they have an elevated quality of confidence. There is no legal guidance on this topic, however it could be suggested that official documents represent an authoritative account of the information contained therein, whereas arguably the scribbled notes of a journalist who is making observational assumptions would be on the other end of the scale and may be speculative.

Sketches, diagrams and etchings

In Prince Albert v. Strange [8], the subject matter of the breach of confidence consisted of unauthorised prints that had been made from copper plates of etchings made by Queen Victoria and Prince Albert. An employee of the printer entrusted to make prints that Queen Victoria and

Prince Albert could give as gifts had made unauthorised prints of the etchings, and a third party had purchased these and published a book of the etching. A key case in the development of the common law duty of confidence, these etchings had the quality of confidence. The resulting injunction provided for surrender of the prints, a prohibition on the exhibition of the images, and a prohibition on the publication of the prints [8].

It could be suggested that this authority clearly illustrates how diagrams, or sketches relating to the anatomy of individuals could be found to have the quality of confidence, particularly where those sketches relate to procedures. While the etchings could be said to represent intellectual property, the effect of recording confidential information in a particular format is relevant.

2.5.4 Trivial confidences

Confidential information which is considered to be 'trivial' does not have the quality of confidence and may not be protected by the common law duty regardless of what that information relates to [38]. In Coco v. A.N. Clark Engineers Limited [22] Megarry J stated that:

> 'I doubt whether equity would intervene unless the circumstances are of sufficient gravity; equity ought not to be invoked merely to protect trivial tittle-tattle, however confidential [38].'

This was discussed in the context of health information in the case of Cambel v. Mirror Group Newspapers [35]. The Baroness Hale of Richmond stated in her judgement that:

> 'The weight to be attached to these various considerations is a matter of fact and degree. Not every statement about a person's health will carry the badge of confidentiality or risk doing harm to that person's physical or moral integrity. The privacy interest in the fact that a public figure has a cold, or a broken leg is unlikely to be strong enough to justify restricting the press's freedom to report it.

> What harm could it possibly do? Sometimes there will be other justifications for publishing, especially where the information is relevant to the capacity of a public figure to do the job. But that is not this case, and, in this case, there was, as the judge found, a risk that publication would do harm. The risk of harm is what matters at this stage, rather than the proof that actual harm has occurred. People trying to recover from drug addiction need considerable dedication and commitment, along with constant reinforcement from those around them. That is why organisations like Narcotics Anonymous were set up and why they can do so much good. Blundering in when matters are acknowledged to be at a 'fragile' stage may do great harm [39]'.

From the above it is clear that there is a balance to be struck in assessing whether information is confidential. Much of that may depend on the circumstances in which information is collected or disclosed, what is disclosed, how it is disclosed, and whether disclosing that information is likely to cause harm. Another relevant factor to consider is the celebrity status of the Claimant, and the freedom of the press to report stories as relate to people who are in the spotlight, although in these circumstances it is recognised that this is a balancing act, and a significant consideration in assessing this is the harm that can be produced.

The Campbell v. Mirror Group Newspapers [35] is useful in demonstrating how health information could be trivial. It could suggested that despite the importance of staff and patients in medical establishments ensuring that information relating to specific patients should not be discussed outside of those professional team treating them, that in reality, if a patient with a broken leg, broken arm, or a visible wound tried to make a claim for breach of confidence for a mention of their injury in earshot of another patient, or even a member of staff, that the quality of confidence may not exist. It could be suggested that this will depend largely on the circumstances, such as whether the information forms part of an official record or whether the information is observational. It should also be noted that while not being subject to the duty of confidence such disclosures may not be ethical.

It may be that if a patient relays the fact that they have seen another patient in an accident and emergency department with a head injury, this would appear to be trivial tittle tattle, however if a medical professional discloses to a friend that an individual in their care attended with a head injury, while not necessarily causing any harm, this would clearly have the quality of confidence.

The source of the information also be a relevant factor. Disclosure of detailed health information by a medical professional for example would not ordinarily be considered trivial tittle tattle and will usually have the quality of confidence. Furthermore, disclosure of the health record would inevitably be much more sensitive.

In W v. Egdell [37] Lord Bingham stated:

> 'It has never been doubted that the circumstances here were such as to impose on Doctor Egdell a duty of confidence owed to W. He could not lawfully sell the contents of his report to a newspaper, as the judge held ... . nor could he without a breach of the law as well as professional etiquette, discuss the case in a learned article or in his memoirs or in gossiping with friends, unless he took appropriate steps to conceal the identity of W [40].'

2.5.5 Information generally accessible, or in the public domain

2.5.5.1 The basic principle

The basic principle is that where information is generally accessible, or in the public domain, this can mean it will lack the quality of confidence.

In Saltman Engineering Co. Ltd. v. Campbell Engineering Co. Ltd [41], in the Chancery Division of the High Court, Mr Justice Vaisey stated:

> 'The information, to be confidential, must, I apprehend, apart from contract, have the necessary quality of confidence about it, namely, it must not be something which is public property and public knowledge [30]'

The courts have however treated this in different ways depending on the circumstances of the disclosure. This is summarised below.

2.5.5.2 Deciding whether information is in the public domain or generally available

It should also be noted that for something to be in the public domain, the information must be available to the public. The fact that that a small number of people may know the information will not necessarily mean that this information is in the public domain [42].

The judgement of the Vice Chancellor, Sir Nicholas Brown-Wilkinson, in Stephens v. Avery makes clear that:

> 'The mere fact that two people know a secret does not mean that it is not confidential. If in fact information is secret [42]'

The Vice Chancellor continued in his judgement to clarify:

> 'Information only ceases to be capable of protection as confidential when it is in fact known to a substantial number of people [42].'

It is therefore clear that where work colleagues, friends, relatives or associates are all aware of confidential information that this does not mean that information is in the public domain, Information needs to be known by a *"substantial number of people* [42]*"*.

When assessing whether information has been disclosed to a substantial number of people it is important to look at the extent to which this has been disclosed. In Attorney-General v. Guardian Newspapers Ltd. (No. 2) [28] the Master of the Rolls, Sir John Donaldson, delivering his judgement in the Court of Appeal stated:

> 'As a general proposition, that which has no character of confidentiality because it has already been communicated to the world, i.e., made generally available to the relevant public, cannot thereafter be subjected to a right of confidentiality . . . However,

> this will not necessarily be the case if the information has previously only been disclosed to a limited part of that public. It is a question of degree [43].'

2.5.5.3 Information disclosed by the person to who a duty of confidence is owed

Where the person who is owed a duty of confidence and makes the information generally available or publishes the information, it appears to be the case that the courts generally find that any person who has a duty of confidence over that information is released from their obligations in keeping the information confidential.

In O. Mustad and Son v. Dosen [44] therefore, the patenting of a machine that could mass produce fish hooks meant that the design of the machine no longer had the quality of confidence with regard to a claim for breach of confidence [45]. In the words of Lord Buckmaster:

> '...after the disclosure had been made by the appellants to the world, it was impossible for them to get an injunction restraining the respondents from disclosing what was common knowledge. The secret, as a secret, had ceased to exist [45].'

In the context of the health service, it is inconceivable that certain disclosures would be ethically appropriate without the permission of the patient, even if information was to be released into the public domain by a patient and there was certainty that the information was no longer confidential at common law. Permission is used here to distinguish from a consented process for the very reason that consent would not be required at common law. It is however useful to be aware that such discharge of obligations is a definite possibility, although the source of the information being disclosed may be relevant as to what is discharged.

In Ashworth Hospital Authority v. Mirror Group Newspapers Ltd [46], the killer Ian Brady had already himself released certain information into the

public domain. Separately, Mirror Group Newspapers had obtained confidential records including medical, nursing and social work records from a member of staff. The article provided no further information than was already in the public domain.

On appeal to the House of Lords, Lord Woolf found that:

> 'While Ian Brady's conduct in putting similar information into the public domain could well mean that he would not be in a position to complain about the publication, this did not destroy the authority's independent interest in retaining the confidentiality of the medical records contained in Ashworth's files. So, the source who abstracted the information from the database not only acted in breach of confidence; he or she also acted in breach of contract.'

On this basis there is a clear distinction between that information that is extracted from health and care records that relate to the treatment of the patient, and that information which may otherwise be disclosed by healthcare organisations or other bodies in response to a publicly known event.

2.5.5.4 Information put in the public domain and used by a third party

Where a third party has disclosed or published confidential information that has unlawfully been put in the public domain, the courts have sometimes taken a different approach. If limited information is disclosed to the public from another source, the information that has not been made available may still be protected by the common law [43].

The case of Schering Chemicals v. Falkman [47] related to the making of a television programme about a pregnancy test drug that the scientific community believed could have caused abnormalities in children. Confidential information that was the subject of the programme had already been the subject of television programmes and newspaper articles. It was argued that as the information was already in the public

domain that the information lacked the quality of confidence. Shaw L.J. stated:

> '...though facts may be widely known they are not ever present in the minds of the public. To extend the knowledge or to revive the recollection of matters which may be detrimental or prejudicial to the interests of some person or organisation is not to be condoned because the facts are already known to some and linger in the memory of others … It is not the law that where confidentiality exists it is terminated or eroded by adventitious publicity [48]'

When considering whether information is confidential therefore, it would appear that even if information has been widely published in breach of confidence, that republication at any stage will still be confidential.

In summary, where the press has obtained a story of a celebrity illness and published extensively will not therefore mean that it becomes acceptable to disclose or confirm this as a professional or as an organisation. Accordingly, the common law duty of confidence exists, and in particular any person who has in their possession any confidential information must not *'take unfair advantage of it* [49]' or use that information *'to the prejudice of him who gave it without obtaining his consent* [49]'.

2.5.5.5 The quality of confidence, relationships and the Public Domain

A specific area of law that has developed through case law relates to relationships, and whether any specific information that could be disclosed is confidential, or whether the details are in the public domain. While a marriage will usually be of public record, details of the intimate details of the relationship, such as that of the individuals sex lives, will usually be confidential [50]. In some circumstances the existence of any form of a relationship will be confidential and possess the quality of confidence, and this will extend to placing an obligation on those parties who are subject to that relationship [51].

In Barrymore and another v. News Group Newspapers Ltd, Mr Justice Jacob held:

> 'I think that there is a strongly arguable case that the details of the relationship between Mr Barrymore and the second defendant, Mr Wincott, should be treated as confidential. I say that because, firstly, common sense dictates that, when people enter into a personal relationship of this nature, they do not do so for the purpose of it subsequently being published in 'The Sun', or any other newspaper. The information about the relationship is for the relationship and not for a wider purpose [51]'.

Whether a person is in a sexual relationship or not can clearly be identified as subject to the duty of confidence, providing the fact that they are in a relationship is not in the public domain [52]. In practical terms, in the healthcare system information relating to any relationship they may be in must be treated with caution as it may be subject to the duty of confidence.

In Stephens v. Avery [53], Sir Nicolas Browne-Wilkinson reiterated the principle that:

> 'To most people the details of their sexual lives are high on their list of those matters which they regard as confidential. The mere fact that two people know a secret does not mean that it is not confidential. If in fact information is secret, then in my judgment it is capable of being kept secret by the imposition of a duty of confidence on any person to whom it is communicated. Information only ceases to be capable of protection as confidential when it is in fact known to a substantial number of people [42].'

Such a position exists regardless of whether both parties are single, or whether one or both parties are in different relationships or are married to other people. It will obviously extend to the sexual relationship within a marriage. In A v. B Plc [54], Mr Justice Jack in his judgement stated:

> 'In my judgment the law should afford the protection of confidentiality to facts concerning sexual relations within marriage (which is surely straightforward) and, in the context of modern

> sexual relations, it should be no different with relationships outside marriage [50].'

In terms of identifying whether relationships are in the public domain it is clear that kissing in a club, or any knowledge held by any staff in a particular place, will not mean that the information is in the public domain and not therefore protected by the common law duty of confidence. In the words of Mr Justice Jack in A v. B Plc [54]:

> 'It is true that the claimant met with C and with D in places of public entertainment where they were seen by their companions and by others. On occasions they may have been seen kissing. Neither C nor D says that anyone knew that they were having an affair in the sense of sexual relations including sexual intercourse. I exclude from that hotel staff. Nor are the details of that intercourse known to any one save the participants. None of this information is in the public domain. It is capable of protection [52].'

In the context of the health service, this illustrates that knowledge of relationships cannot be assumed, and the confidentiality of relationships should be maintained. It may therefore be important to treat any relationship information confidential, particularly in large datasets where it may be difficult to assess whether this data is subject to the duty of confidence.

2.5.5.6 Information partly in the public domain

There may be circumstances where there is some information in the public domain and some connected information that still remains private. For example, a celebrity makes a public statement that they are due to have an operation to have a plate inserted into their leg following an accident. They may have requested coordination of any public communications with the communications teams in the hospital to ensure that any press enquiries are relayed in accordance with this narrative. During the stay in hospital however, it could be that they are also due to undergo a procedure for a hip replacement. Following the press communication the information that has been released into the

public domain will have lost the quality of confidence by the very nature of the disclosure [55], however, where additional information is not in the public domain, such as the hip replacement, this may stay remain confidential and should not be disclosed [55]. It follows that if the press were informed about the hip replacement there would be a breach of confidence.

In Seager v. Copydex [32], the then Master of the Rolls Lord Denning provides useful advice in relation to such information. In his judgement he says:

> 'When the information is mixed, being partly public and partly private, then the recipient must take special care to use only the material which is in the public domain. He should go to the public source and get it: or, at any rate, not be in a better position than if he had gone to the public source [55].'

The judgement highlights the importance of ensuring that where information is being disclosed because it is in the public domain, that no additional confidential information is disclosed. The advice that the disclosure should use the information in the public domain is sensible. An important factor is that the discloser should not be in a better position using the private source than they would be in accessing the public source [55]. As identified earlier, reproducing the same information with reference to health records would be in breach of confidence [40].

2.5.5.7 Ethics and information in the public domain

It is important to note that it would likely be unethical for a healthcare organisation or a clinician to disclose any information, even if it was in the public domain without the full authority of the patient regardless of whether there was a duty of confidence owed.

2.5.6 Protecting the identity of individuals to remove the quality of confidence

2.5.6.1 The general position

Where confidential information relates to an individual, and steps have been taken to conceal the identity of that individual, that data ceases to have the quality of confidence in relation to that individual [40]. Cases such as W v. Egdell [37] have highlighted that information that could not identify an individual would not be subject to the quality of confidence. In W v. Egdell [37], Bingham LJ stated:

> 'It has never been doubted that the circumstances here were such as to impose on Dr Egdell a duty of confidence owed to W. He could not lawfully sell the contents of his report to a newspaper, as the judge held . . . Nor could he, without a breach of the law as well as professional etiquette, discuss the case in a learned article or in his memoirs or in gossiping with friends, unless he took appropriate steps to conceal the identity of W. It is not in issue here that a duty of confidence existed [40].'

Specific measures that could be engaged to protect the identity of individuals have not been fully explored fully in the case law, however some case law does exist to reflect elements of the approaches that have been taken, as detailed under the below headings.

2.5.6.2 Making information non identifiable

Anonymisation as a means of lawfully disclosing information was considered in some detail in the case of R v. Department of Health, ex parte Source Informatics [56]. At the High Court of Justice, the argument that taking steps to conceal the identity of patients removed the quality of confidence as reflected in W v. Egdell [37] was rejected [12], however at the Court of Appeal, this view was reinstated [12].

The case related to a request to GPs and Pharmacists for anonymised data by a data collecting company. In response to the activity, the

Department of Health issued a policy position which was set out as follows:

> ‘Anonymisation (with or without aggregation) does not, in our view, remove the duty of confidence towards the patients who are the subject of the data. Apart from the risk of identification of a patient despite anonymisation, the patient would not have entrusted the information to the GP or the pharmacist for it to be provided to the data company. The patient would not be aware of or have consented to the information being given to the data company but would have given it to be used in connection with his care and treatment and wider NHS purposes. Anonymisation of the data (with or without aggregation) would not obviate a breach of confidence. The documents from the data company do not make clear who was responsible for separating patient details from the prescriber and prescription details. If it is the data company, then the pharmacist or GP will be in breach of duty of confidence towards the patient in allowing the data company access to this information [12].’

In a judicial review, Source applied to the court for a declaration that this position was incorrect. At the Queen’s Bench Division of the High Court of Justice, Latham J found that the Department of Health were correct in their position. In his Judgement, of the anonymisation process, he found:

> ‘In my view, it is impossible to escape the logic of Mr Sales' argument that the proposal involves the unauthorised use by the pharmacist of confidential information. I reject the sophistry of Mr Beloff's submission that the process can be divided into two stages. In my judgment what is proposed will result in a clear breach of confidence unless the patient gives consent, which is not part of the proposal at present. Nor is it suggested that the patient can be said to have given implied consent. This may be the position where doctors and the health service itself use anonymous material for the purposes of research, medical advancement or the proper administration of the service. That is not, however, a matter on which I have heard sufficient evidence or argument to enable me to come to any conclusion; nor is it necessary for me to do so for the purposes of these proceedings [12].’

If left unchallenged this judgement could have had a significant effect on the use of health data. Not only did it appear to contradict cases such as W v. Egdell [37] , but it suggested that confidences could be breached by

using the data for any other purpose, including where anonymised. It could be suggested that the proposal that consent was required from every patient in order to produce statistical information was not only impractical for other purposes, such where it was disclosed to a healthcare body, but could potentially have caused future issues in healthcare innovation. In addition, it appears to place some uncertainty about use of the data in the pharmacy beyond dispensing the prescription.

On appeal in the Court of Appeal [56] however the judgement was overturned. In a lengthy by well explained judgement Lord Brown discussed the principle of anonymisation in some detail:

> 'Mr Sales urges in particular these considerations. The patient's sole purpose in handing over the prescription is so that the pharmacist may dispense the drugs prescribed. That, therefore, is the only use of it that is authorised. By anonymising the information, the pharmacist does not cease to be under a duty of confidence with regard to it. Indeed, the very act of anonymisation involves "manipulation" of the information and is itself objectionable. The only reason the pharmacist has something to sell is because the patient has handed over his prescription. Even when it is anonymised, it is still not in the public domain. To sell any part of it is to misuse it.
>
> For my part I find these arguments not merely unconvincing but wholly unreal. True it is that even when stripped of anything capable of identifying the patient, the information which the pharmacist proposes to sell to Source is still not in 'the public domain'. But whether or not that matters must surely depend upon the interest at stake... [57].'

Further in his judgement, Lord Brown stated:

> '...In my judgment the answer is plain. The concern of the law here is to protect the confider's personal privacy. That and that alone is the right at issue in this case. The patient has no proprietorial claim to the prescription form or to the information it contains. Of course, he can bestow or withhold his custom as he pleases – the pharmacist, note, has no such right: he is by law bound to dispense to whoever presents a prescription. But that gives the patient no property in the information and no right to control its use provided only and always that his privacy is not put at risk. I referred earlier

> to Mr Sales' plea for respect for “the patient's autonomy”. At first blush the submission is a beguiling one. My difficulty with it, however, is in understanding how the patient's autonomy is compromised by Source's scheme. If, as I conclude, his only legitimate interest is in the protection of his privacy and if that is safeguarded, I fail to see how his will could be thought thwarted or his personal integrity undermined. By the same token that, in a case concerning Government information, “the principle of confidentiality can have no application to it . . . once it has entered . . . the public domain” (per Lord Goff), so too in a case involving personal confidences I would hold by analogy that the confidence is not breached where the confider's identity is protected.
>
> This appeal concerns, as all agree, the application of a broad principle of equity. I propose its resolution on a similarly broad basis. I would not distinguish between Source's first and second arguments and nor would I regard the case as turning on the question of detriment. Rather I would stand back from the many detailed arguments addressed to us and hold simply that pharmacists' consciences ought not reasonably to be troubled by cooperation with Source's proposed scheme. The patient's privacy will have been safeguarded, not invaded. The pharmacist's duty of confidence will not have been breached [12].’

The source judgement raises a couple of significant observations in relation to the use of the data in question in an organisation:

1. The undertaking of activities on data internally within an organisation does not usually constitute a disclosure.
2. When looking at the duty of confidence, it is important to understand what needs to be protected. If confidential patient information needs to be protected, where the person cannot be identified, this confidentiality is protected.
3. A patient has no proprietary right to a prescription, document, or their information.
4. Anonymisation protects patients’ privacy, it does not invade it.

2.5.6.3 Anonymisation

While the author has extensive experience in approaches to making individuals less identifiable, it is not proposed to discuss any of the anonymisation methodologies that could be applied, this is out of scope

of this thesis. Understanding the definitions of anonymisation within the common law, and how the UK GDPR interacts with the common law where data is anonymised at common law is in scope of this thesis.

R v. Department of Health, ex parte Source Informatics [56] uses the terminology 'anonymisation [12]. The term is one that, on face value, appears to be a straightforward concept. It could be interpreted as meaning that the process of anonymisation is the act of making data non-identifiable, and that anonymised information is information that no one can be identified from. There is however a distinct difference between the term anonymisation within the meaning of the common law, and how the same information is interpreted in the meaning of the UK GDPR.

The starting point in understanding how the UK GDPR interacts with the common law is to understand what is meant by anonymisation within the meaning of the common law.

While there is not a comprehensive body of case law that provides examples of where the quality of confidence has because of anonymisation, the case law does provide some guidance as to circumstances in information will be considered to have lost the quality of confidence.

At common law, the duty of confidence seeks to protect a confiders privacy [12]. Therefore, where a confider's identity is appropriately protected from the person receiving the information, there will be no breach of that duty [12]. For the purpose of the common law, that is not to say that the person seeking to disclose the information should not be able to identify the information [40]. In other words, the protection to conceal the person's identity is concerned with an individual being disclosed information [40]. Identity may be concealed in a number of ways. On an individual level it could be that simply removing the name will render information non identifiable in a discussion between two doctors

[40], but a publication of granular statistics to the world at large may cause someone to identify a person where there are a small number of people, and the analysis relates to a small geographical area. When making a judgement on whether data is identifiable therefore, steps should take into account the possibility that individuals may easily identify people from information already known to them, or information they can access [58]. It is therefore important to take appropriate steps to conceal the identity of the confider where such a disclosure is made [40], the detail of which will depend on the circumstances of the case [40]. The audience of the disclosure is considered in more detail under the next heading,

In the case of the UK GDPR however, where some information may be considered anonymised for the purpose of the common law, the UK GDPR may still be engaged. The UK GDPR applies to the processing of personal data. Article 4(1) states that:

> ''personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person [23].'

The UK GDPR therefore is indiscriminate of audience, who disclosed to, or what measures have been taken to conceal the identity of the confider. With row level data, if anyone, even the person who hold the information in confidence can identify the individual, this would be personal data within the definition of the UK GDPR.

While considering anonymisation processes at common law, it is also useful to consider the definition of pseudonymisation within the meaning of the UK GDPR. Article 4(5) of the UK GDPR states that:

> ‘pseudonymisation’ means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person [59].’

In this set of circumstances, from a confidentiality perspective, the measures put in place to conceal the data would almost certainly be considered to sufficiently protect the identity of individuals in compliance with the common law [40]. This creates an interesting position whereby data is not identifiable at common law, and therefore not subject to the duty of confidence, however for the purposes of the UK GDPR [21], this information remains subject to the UK GDPR [21].

2.5.6.4 Identification through other information

As stated above, the common law does not provide a robust set of guidance that sets out how data can be concealed to remove the quality of confidence, however it is know that in order to consider such information not subject to the duty of confidence that steps must be taken to conceal the identity of individuals [40]. Where there is any doubt, a risk assessment should be undertaken that takes into account the relevant factors, including those which make the risk tolerance more acceptable [60].

There is always a risk that information could be released, and other information may be available that could mean a person can be identified. H (a Healthworker) v. Associated Newspapers Ltd [61] related to a healthcare worker who had contracted HIV and had retired. A series of actions had taken place in relation to the restraint of information that would identity ‘H’. An injunction secured by ‘H’ prohibited Associated Newspapers Ltd from:

> ‘(a) the soliciting or publication of any information which may directly or indirectly lead to disclosure of the identify or whereabouts of the applicant or his patients.
> (b) in particular, publication of details of the applicant's speciality (other than the fact that he is a healthcare worker) or details as to when he was diagnosed as HIV positive and went off work sick [62]’

Associated Newspapers Ltd therefore published an article that said, ‘Judge’s gag over Aids threat to patients.’ The article provided clues as to the speciality of ‘H’. The case was one of a series of cases that sought to vary injunction on the release of information, including the name of the Health Authority (“N”) and other information.

In his judgement, Lord Phillips, Master of the Rolls recognised the information contained in the article published by Associated Newspapers Limited, in conjunction with details of the Health Authority and the fact that his ill health had led to his retirement, could identify him by anyone who had a personal knowledge. He stated:

> ‘The information in that article, coupled with the identification of N, could well lead anyone who had personal knowledge that H had retired through ill-health to deduce that the article was written about H. A prime, and not unreasonable, concern of H may well be that those whom he knows personally should not become aware of the nature of his illness. [58].’

In relation to his speciality however, Lord Phillips considered the risk of identification more remote. He stated:

> ‘There must be a risk that some who know the details of H's retirement may suspect, and it can be no more than a suspicion, that he is the healthcare worker in this action. Provided, however, that the other restraints in Gross J's Order remain in force, which we consider that they should, we do not consider that this risk justifies continuing the restraint on disclosing H's speciality. As we indicated early in our judgment, this restraint is inhibiting debate on what is a matter of public interest. We have concluded that this restraint is not justified [60].’

It is therefore apparent that a number of factors are relevant when considering whether information sufficiently conceals the identity of

individuals. A risk-based assessment of all relevant factors should be taken into account [60].

Where it can be easily deduced that information relates to a specific individual, then this information is considered to be subject to the duty of confidence to the extent that there should be protection against any breach of confidence [58], unless of course there was another lawful reason that the information could be disclosed at common law, such as with consent of the individual.

Where there is a small risk that a suspicion of someone's identity could be stablished and there is a public interest in making the public aware of certain information, it may be appropriate to disclose, providing other information that may confirm the identity of the individual is protected [60].

2.5.7 The quality of confidence beyond death

2.5.7.1 The general principle

Where the confidential information relates to a person, the general position is that confidentiality does not end with their death [63]. Prior to Lewis v. The Secretary of State for Health [64] the question had only been explored at Tribunal in cases such as Bluck v. Information Commissioner and Epsom & St Helier University NHS Trust [65]. In Lewis v. The Secretary of State for Health [64], with no precedent previously existing in the higher courts, a medical practitioner sought to clarify whether the record of deceased patients that were in his care were subject to the duty of confidence, and if so, whether they could be lawfully disclosed. For the purpose of this section, only the question as to whether the duty of confidence persists after death will be discussed.

Addressing the subject Lord Justice Foskett acknowledged at the start of a detailed judgement that:

> ‘I need go no further for present purposes than to reach the conclusion, if I do, that it is arguable that the duty does survive the patient's death [66].’

The effect of the judgment is to solidify the principle that confidentiality survives beyond death as discussed in tribunal cases such as Bluck v. Information Commissioner and Epsom & St Helier University NHS Trust [65] by creating a precedent on this principle.

2.5.7.2 Duration of confidentiality beyond death

With regard the amount of time by which confidentiality exists beyond death, prior to In Lewis v. The Secretary of State for Health [64], there was no judicial authority that discussed this with specific reference to personal information. This had however been discussed in relation to other confidential information.

In Attorney General v. Jonathan Cape Ltd [67], the court ruled on the confidential nature of diaries recording discussions at cabinet as recorded by a then deceased former Cabinet member. Of duration of the confidentiality, Lord Widgery CJ found that:

> ‘There must, however, be a limit in time after which the confidential character of the information, and the duty of the court to restrain publication, will lapse [68]’.

Further in the judgement he continued:

> ‘It may, of course, be intensely difficult in a particular case, to say at what point the material loses its confidential character, on the ground that publication will no longer undermine the doctrine of joint Cabinet responsibility. It is this difficulty which prompts some to argue that Cabinet discussions should retain their confidential character for a longer and arbitrary period such as 30 years, or even for all time, but this seems to me to be excessively restrictive. The court should intervene only in the clearest of cases where the continuing confidentiality of the material can be demonstrated. In less clear cases — and this, in my view, is certainly one — reliance

> must be placed on the good sense and good taste of the Minister or ex-Minister concerned [68].'

Lewis v. The Secretary of State for Health [64] however had a firmer response in relation to personal information such as medical examinations. Lord Justice Foskett held that:

> 'As will be apparent, it is likely that some of the material the subject of the request for disclosure will relate to examinations and analyses going back many years. It is, of course, just possible that there are, in some cases, no living next-of-kin of those affected. However, for my part, I would not regard that, or indeed the passage of time generally in a matter of this nature, as eradicating or diminishing significantly the strength of the obligation of confidentiality which, as I have concluded, arguably exists in each of the cases in respect of which disclosure is sought [69].'

There are two distinctions to be made in this regard. In the first instance, Lewis v. The Secretary of State for Health [64] is discussing cases which exist in living memory. While confidentiality may have slightly diminished over time, it has not diminished sufficiently to warrant disclosure in the timescales to which the case relates. The second distinction is the very fact that health confidences appear to be much more sensitive than other types of confidential information [40] providing it is not trivial [39]. The very fact that the quality of confidence could be seen as diminishing at all is suggestive of the fact that eventually information will lose its confidentiality [69], although the judgements are not helpful in defining this.

2.6 Imparted in circumstances importing an obligation of confidence

2.6.1 The general position

While cited as a requirement in the case law, this element is often not considered in any detail. In Coco v. A.N. Clarke (Engineers) Limited [22], the absence of guidance was highlighted [70], but no further guidance was provided, and beyond a short discussion around the relationships,

and communications between the parties, it was concluded that there was no requirement to explore the requirement further [71].

One key element to deciding if information has been imparted in circumstances importing an obligation of confidence does appear to revolve around the relationship and knowledge of the parties [22]. Whether information that has been imparted in circumstances importing a duty of confidence will usually be indicated by the fact that a person knows that the information is confidential [22].

There are a number of circumstances by which someone will usually be deemed to be aware that the circumstances are confidential, and the courts will conclude that information was imparted in circumstances importing a duty of confidence as required by the test for confidentiality [72]. For the purpose of this thesis, three of those circumstances will be explored:

- Where the information is imparted because of a contractual or business relationship.
- Where the information is imparted by the confider because of a service being provided.
- Where there is a non-business or service-related relationship between the parties

2.6.2 Imparted due to a contractual or business relationships

This section describes those contractual or other business relationships that may be encountered by NHS organisations, although the principle will be the same in other business relationships.

Where there is a contractual, or other business relationship, such terms are usually included in these arrangements for the avoidance of doubt [73]. If there are no clauses in the contracts however, the very existence of any commercial or other type of business relationship often infers that

any information imparted as part of that contract is subject to the duty of confidence where the subject matter has the quality of confidence [74].

The NHS potentially could impart information that has the quality of confidence for a number or reasons, but in illustrating the case using the example of healthcare data, the NHS could subcontract a private company to work on information systems that will be processing patient data, and those contractors could have access to this information as part of their work. In such circumstances, the law will infer confidentiality regardless of any contractual or other terms included in agreements [74], although in the case of personal data, where there is a processor, there must be a properly constituted agreement in accordance with the UK GDPR [75].

Aside from any Controller to Processor data transfers, it is also conceivable that any data that possesses the quality of confidence could be received from other parties. Examples of such a relationship include data received from contractors supplying NHS services on behalf of Health Boards in Wales. Other circumstances could include situations where data originates from another statutory body outside of the NHS in Wales such as the Office of National Statistics, a NHS service provider in England, or a private organisation in appropriate circumstances. It is clearly desirable to have such arrangement is writing [73], but in the absence of a written agreement, terms will be implied [74].

It should be noted that in the case of private healthcare, there will be a direct contractual relationship between the parties, and the same principles apply between the provider of that care. In other words, regardless of any written agreement that the care relationship imposes, there will be an implied term of confidentiality [74].

While enforcement of breach of confidence is explicitly out of scope of this thesis, for the benefit of understanding the effect of contractual provisions, it is useful to examine how any breach by a third party

recipient of confidential data (“the third party”) of any information that it has lawfully received from an organisation that holds it in confidence (“the confidee organisation”), could be remedied. In terms of any contract that may exist between the confidee organisation and the third party, the confidee organisation can of course seek to pursue a claim in breach of confidence and breach of contract [7], however, the confidee would not be privy to that contract, and therefore could not a claim in respect of that contract due to privity of contract [76]. As breach of confidence is a Tort however, the confidee could potentially sue the third party themselves in line with the basic legal principles that apply to any duty in tort law [77].

2.6.3 Relationships created through non contractual service provision

In circumstances where an individual interacts with a service and there is no contractual provision within the meaning of the law, it is clear that information can still be imparted in circumstances importing a duty of confidence [78]. This is reflected wherever those services may be accessed, and however that information is shared between the organisations or persons that provide of that service [78]. It can safely be assumed that any information collected in provision of services connected to their healthcare will be imparted in circumstances imposing a duty of confidence.

It is important to note that it is not only in circumstances where a clinician receives information that the information is deemed to have been imparted [31]. Anyone who is involved in any activity that comes to be informed of information as a result of a confidential situation, can be said to have received information that was imparted in circumstances importing a duty of confidence [31]. An example of circumstances where confidentiality could be said to have been imparted in circumstances importing a duty of confidence and will not only bind employees, but

members of the public, are where honest advice is shared by attendees of a group therapy session [31].

2.6.4 Non business or service-related relationships

Where information possesses the quality of confidence, even if there is no relationship between parties who become privy to that information, information may still have been imparted in circumstances importing a duty of confidence [52]. This could relate to information disclosed by the confidee to another patient at a GP surgery or hospital, to a non-clinical member of staff, although many of the communications under the latter heading could be included within circumstances of non-contractual service provision.

The fact that a confidee is discussing certain information to individuals in a public place so that others can overhear, does not mean that it either loses the quality of confidence, or is not being imparted in circumstances importing a duty of confidence [41]. Information must be known by a substantial number of people to be considered in the public domain[41], although the subject matter of the confidence, together with the fact it is being openly discussed could favour the argument that the information is trivial [39].

Parties in romantic relationships may also know certain information in relation to their partner, including health complaints or other information, and the law is prepared to restrain the partner from breaching confidence [51]. It should be noted that a defence to a disclosure may apply, and this is considered in the following chapters.

2.7 Unauthorised use causing a breach of confidence

2.7.1 The basic position

The basic position by which determining whether a breach of confidence has occurred is to consider whether there has been an unauthorised use of information that is subject to the duty of confidence [22]. There will be no breach of confidence where:

- There is a defence to the use of the information, such as where there is consent [28];
- There is a requirement to disclose information as set out in law, for example, where there is an obligation of reporting a notifiable disease [79];
- Where a duty of confidence is expressly set aside by law, for example, in the case of health research, on the advice of the Confidentiality Advisory Group under Regulation 5 of the Health Service (Control of Patient Information Regulations) 2002 [80]; or
- Where information needs to be disclosed to another person to fulfil a statutory function, for example, in the case of a Special Health Authority in Wales, they may be complying with their statutory functions in accordance with the legislation [81].

These are explained in more detail as part of this thesis. The remainder of this chapter will consider what is considered a breach of confidence.

2.7.2 Unauthorised use

In order to be in breach of confidence there must be an unauthorised use of that information [22].

The case law appears to identify two broad types of unauthorised use. These are:

- The use or disclosure of information by an individual who is acting outside of their contract of employment
- Other uses of information by legal persons in breach of confidence.

These are described in more detail below.

2.7.3 Use or disclosure by an employee in breach of an employment contract

2.7.3.1 The basic position

By a breach of the contract of employment, this includes the use of data that is subject to the duty of confidence that has been lawfully collected by an organisation but is being used for purposes other than those undertaken by the employer on their own initiative. An example of such a breach is illustrated by the case of X v. Y [82] where information on practicing doctors who had been diagnosed with AIDS was leaked to the press by employees. The case recognises a clear breach of contract [83] and also that the breach of confidence was by the employee themselves [83].

2.7.3.2 Liability

Where an employee misuses data, not only they, but the employer may be liable for the breach of confidence [84]. The test for establishing whether an employer is vicariously liable was explored in the case of Dubai Aluminium v. Salaam [84]. Mr Lord Justice Nichols held that:

> '...the circumstances in which an employer may be vicariously liable for his employee's intentional misconduct are not closed. All depends on the closeness of the connection between the duties which, in broad terms, the employee was engaged to perform and his wrongdoing [85].'

In Various Claimants v. Wm Morrison Supermarkets plc [86], a senior internal IT auditor with a grudge against Morrisons Supermarkets Plc

downloaded the data of around 100,000 employees onto a personal USB stick, took it home, and uploaded it to a file sharing website. He then sent links to three UK newspapers. In a group action, 9,263 effected employees issued a claim against Morrisons for damages for breach of the Data Protection Act 1998, the misuse of private information and for breach of confidence by the offending employee. Applying this case of Dubai Aluminium v. Salaam [87]., Lord Reed asked the question:

> '..disclosure of the data was so closely connected with acts he was authorised to do that, for the purposes of the liability of his employer to third parties, his wrongful disclosure may fairly and properly be regarded as done by him while acting in the ordinary course of his employment [87].'

The UK Supreme Court found that Morrisons were not liable for vicarious liability for a breach of confidence.

In relation to the scope of his employment, the court found that downloading and publishing employee data in this way not in the 'field of activities' that he had been employed to do, and was not an act he was authorised to do, and he was not 'doing acts of the same kind as those which it was within his authority to do'. [87]. It was also held that the 'mere opportunity' to commit a wrongful act by being in that position of trust was not enough to find Morrisons vicariously liable [87].

Lord Reed identified that while there was a 'close temporal link [87]' and an 'unbroken chain of causation [87]' between the provision of data to undertake employment and the subsequent publication on the internet a 'a temporal or causal connection does not in itself satisfy the close connection test [87]. Finally, Lord Reed held that motive was irrelevant. The important element to consider was whether he was acting on his employer's business or for a personal reason [87].

2.7.4 Other uses of information by a legal person in breach of confidence

In this section, it is the intention to set out, aside from breaches by employees, or the vicarious liability of an organisation, what constitutes an unauthorised use where an organisation uses information.

2.7.4.1 The basic position

The basic position is that a legal person who receives confidential information, discloses that information to a third party without a lawful excuse. In Taranto v. Cornelius [88] for example a psychiatrist who had been contracted privately to prepare a medico-legal report for the purposes of a civil claim, forwarded the report to her solicitor, a consultant psychiatrist at a hospital near the claimant's home, and to her general practitioner without consent in breach of confidence.

2.7.4.2 Defining “use”

It is not just individuals collect information that is subject to the duty of confidence. Legal entities such as Health Boards, NHS Trusts and Special Health Authorities also collect information. In the heading above as relates to employees breaching confidence, this is straightforward but as relates to organisations using information, the phrase ‘unauthorised use’ is vague. The case of R v. Department of Health ex parte Source Informatics [89] settled a point of law. Mr Lord Justice Brown, refused to allow the common law ‘distorted for the purpose [90]’ of the policy position of the Department of Health [90] stating:

> ‘The concern of the law here is to protect the confider's personal privacy. That and that alone is the right at issue in this case. The patient has no proprietorial claim to the prescription form or to the information it contains. Of course, he can bestow or withhold his custom as he pleases—the pharmacist, note, has no such right: he is by law bound to dispense to whoever presents a prescription. But that gives the patient no property in the information and no

> right to control its use provided only and always that his privacy is not put at risk [12].'

The judgement makes it clear that when an organisation holds information, it can use that information for a number of purposes without being in breach of the common law. The key consideration at all times, however, is maintaining the confiders privacy. It is therefore conceivable that in most situations, a breach of confidence will only occur where a disclosure is made. The common law is not concerned with uses of information where privacy is protected, and the patient has no control over the use of information [12].

2.7.5 Causation and the breach

2.7.5.1 The basic position

In order for there to be a breach of confidence the confider must have caused the breach [91]. The duty of confidence is a negative obligation not to disclose information that is subject to that duty [92]. Accordingly, there must be a 'positive action' by the confider that leads to a breach of confidence [93]. That positive action could be unintended use, or a reckless use, but nevertheless, the use must be an act [93]

.

Without a positive action, even if the person holding information has insufficient security measures and the data is stolen by hackers, there will be no causation to the breach [94]. It is important to note however, that the Controller of the information could be in breach of the UK GDPR data protection principles, and in particular the UK GDPR 'security principle [95]' if data has not been:

> '...processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures [95].'

This position has been affirmed as recently as 2022 in the case of Smith and Others v. Talktalk Telecom Group Plc [96].

2.7.5.2 The positive act

It is important to consider who has undertaken the positive act when considering who is liable. When a person makes a disclosure that contravenes the duty of confidence as part of their business activities, this is relatively straightforward. Where the positive act is undertaken by an employee who acts outside of his duties however, there may be a vicarious liability. This is explained in more detail above, but by way of summarising this differential, in Various Claimants v. Wm Morrison Supermarkets plc [86], the employee was in fact the one who breached confidentiality, and the employer was not vicariously liable for a number of reasons, including that the employee was working on his own initiative [87], and there was not a close connection between the employment and the breach [87].

2.7.6 Use of information for other purposes

Where information has been lawfully obtained, the general position is that any internal use of that information is lawful to the extent that the patient's privacy is protected [12]. Where information is held internally by an organisation, and a use is considered for a particular purpose, in some circumstances there may be a breach of confidence if a man of 'average intelligence and honesty' would think that a use of the information was for any improper purpose [97]. In the context of the health service, if a contractor supplying NHS services has information for one purpose, if they used information for their own purposes to promote healthcare related products, where authorised by the company, and without making a disclosure, it could be said that the use was improper in the mind of someone of 'average intelligence and honesty' [97], although this specific example is untested in law.

2.7.7 Breach of confidence and the UK GDPR

Processing of any personal data as defined by the UK GDPR [23] is defined by Article 4 as:

> '…any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction [24].'

The wide definition of 'processing' could be said to include most activities by which personal data is handled.

Where there is any breach of confidence relating to personal data, there will at the very least be a breach of the first data protection principle. The first data protection principle within the UK GDPR provides that personal data shall be:

> 'Processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency) [9].'

In breaching the common law duty of confidence, a breach of the first data protection principle as information would not be processed lawfully [98].

2.8 Summary of Chapter 2: Duty of Confidence

The chapter provides the basic set of principles relevant to the NHS, that will contribute to a better understanding as to whether information is confidential.

In order to be confidential, information must have:

- The quality of confidence[22]

- Been imparted in circumstances importing an obligation of confidence [22].

Any unauthorised use of that information to the detriment of the party communicating it will be in breach of confidence [22].

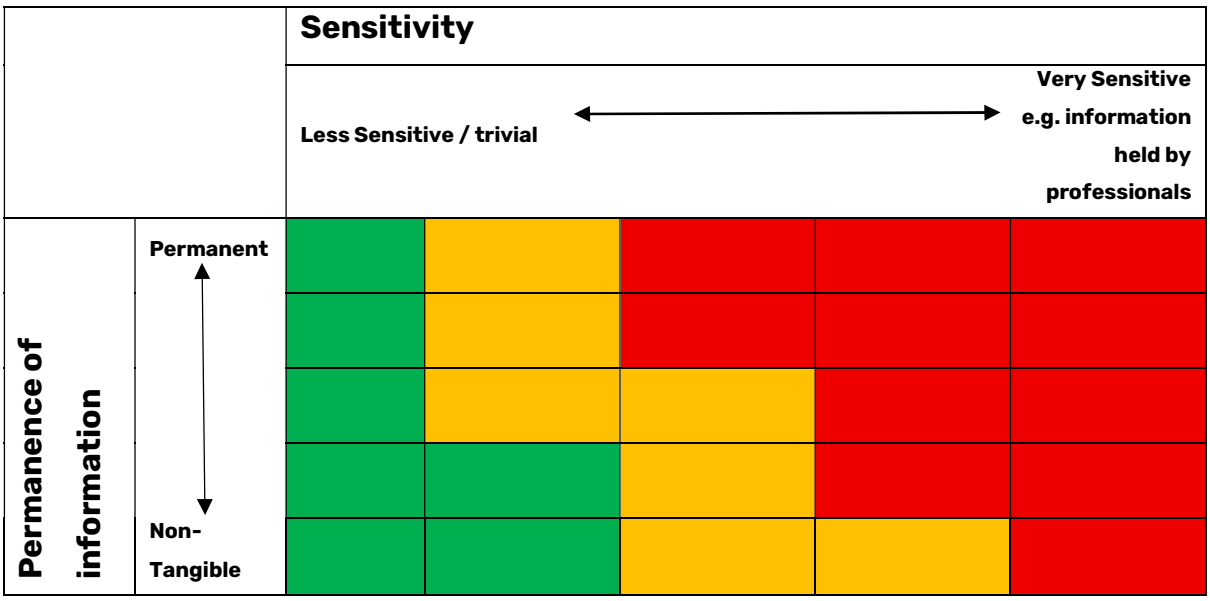
The quality of confidence

The following principles relate to the quality of confidence:

- Any information can have the quality of confidence, including that conveyed orally [32], photographs, audio and video recordings [33] and sketches, diagrams or etchings [8].
- Tangible information can be more confidential [33], with permanent records such as photographs [36] and official records such as medical records [37] being most sensitive
- Trivial information is unlikely to be confidential regardless of what it relates to [38]. In a health context, this will include observations that someone has a cold, or a broken leg [39]. This will not include records of an official diagnosis as these are more sensitive [40].

Figure 1 on the next page demonstrates the relationship between the permanence of information that has the quality of confidence and the sensitivity of the information.

There are many factors to be taken into account, and the approach represented by the diagram does not account for all scenarios, but it does demonstrate at a basic level how even minor health conditions that can be assumed from observation will not be confidential even if printed in permanent form [39], this becomes more sensitive where that information is conveyed by, or has been extracted from records made by professionals [40].



Level 1	Non confidential
Level 2	Confidential
Level 3	Highly Confidential

Figure 1: Permanency v's Sensitivity of Information

It can be noted that the above RAG table (Red, Amber, Green) table follows a different colour pattern to those used to assess risk. The table above follows the general proposition that trivial information is not confidential regardless of whether it is in a non-tangible form or a permanent form but becomes significantly more confidential where it becomes less trivial. The table takes into account very general principles and therefore the author would recommend that confidentiality is assessed on a case-by-case basis and considers the full set of factors.

The following summarised the position where information is in the public domain:

- Information in the public domain is not usually confidential [30], particularly where put in the public domain by the person to whom it relates [45]. An unlawful disclosure by a third party however will not mean that information has been made public [43].

- Where facts are put in the public domain by an individual, this does not mean that the official records, such as health records, cease to be confidential [46].
- Information partly released in the public domain loses the quality of confidence, but additional information remains confidential [55].

Table 1 (below) provides an indication as to whether information is in the public domain, based on the number of people that are made known of the information:

Quality of confidence	**No quality of confidence**
Known by a small number of people [42]'	Known by a substantial number of people [42]
Disclosed to a limited part of the public [43].'	

Table 1: Public domain - number of persons who know the information

Some relationships may be confidential. Table 2 (below) illustrates those relationships that will remain confidential.

Quality of confidence	**No quality of confidence**
Sex lives in or out of marriage [50].	Marriage (i.e. in the public domain) [50]
Secret relationships, including placing an obligation on the other party [51].	Sexual relationships in the public domain [52].
Relationships in a public place (e.g. a club) [52].	

Table 2: Relationships - Whether in the public domain

The following principles relate to the anonymisation of data:

- Anonymised data does not have the quality of confidence [12]
- To be considered anonymised at common law, a person should not be easily identifiable from the data [12] by putting measures in place to protect the identity of individuals [40].
- It is usually sufficient to establish whether information is sufficiently anonymised by assessing the risk of identification [60], however where there is a small public interest in data being disclosed, this may influence the argument that disclosure is sufficiently anonymised while not meeting the threshold for the public interest defence [60].
- Processes used to anonymise data that is lawfully held will not be an inappropriate use [12], and the patient has no right to object to the information being anonymised and disclosed [12].
- Anonymisation is a privacy protecting process [12] and therefore where the identity of an individual can be easily deduced from the data, the data is not sufficiently anonymised [58].

The following summarises the persistence of the quality of confidence:

- The quality of confidence does not end on death [63].
- The quality of confidence will decrease over time [68].
- Health confidences are likely to diminish at a much slower rate, particularly up to the point where a person is within living memory [69].'

Imparted in circumstances importing an obligation of confidence'

The following bullets summarise the concept of imparting information in circumstances importing an obligation of confidence:

- There is no precise definition around the imparting of information [70]

- The relationship of the parties can be factor in determining that the circumstances import an obligation of confidence, as can the fact that a person knows that the information is confidential [22].
- Knowledge that something is confidential is often inferred given the circumstances [72]. Examples include:
    - Contractual relationships: The fact information has been imparted in circumstances importing an obligation of confidence us usually indicated in contracts [73], or implied due to the nature of the relationship [74].
    - Non contractual relationships: The relationship need not be contractual [78], and can extend to anyone who comes across the information in a confidential situation[31].
    - No direct relationship: Information may still have been imparted even where there is no relationship [52]. Overhearing conversations in a public place may have the quality of confidence[41].

Breach of Confidence

To be considered a breach of confidence, there must be an unauthorised use [22]. There will be no breach of confidence where:

- There is a defence to the use of the information, such as where there is consent [28];
- There is a requirement to disclose information as set out in law, for example, where there is an obligation of reporting a notifiable disease [79];
- Where a duty of confidence is expressly set aside by law, for example, in the case of health research, on the advice of the Confidentiality Advisory Group under Regulation 5 of the Health Service (Control of Patient Information Regulations) 2002 [80]; or
- Where information needs to be disclosed to another person to fulfil a statutory function, for example, in the case of a Special Health Authority in Wales, they may be complying with their statutory functions in accordance with the legislation [81].

An unauthorised use has generally been accepted to have taken place where there has been an unlawful disclosure of information:

- By an employee in breach of their contract of employment [83].
- By an organisation where there is a disclosure or use of information where a man of 'average intelligence and honesty' would consider the use an improper purpose [97].

To identify that someone has breached their duty of confidence, it is necessary to demonstrate that the actions of the party holding the confidential information caused the breach themselves [94]. The actions of third parties who have hacked systems or stolen information will not satisfy this test under the common law [94]. To prove causation, it must be demonstrated that:

- There is a 'positive action' (e.g. reckless act) [93]
- That the positive act leads to information being disclosed [91].

Table 3 (on the next page) sets out the factors that may be considered when determining liability of breach of confidence where the unlawful use is based on the actions of the employee.

Employer Liable	**Employee Liable**
Close connection between the duties of the employee and the breach [85].'	Employee not authorised to do the act that caused the breach [87].
Temporal link and an unbroken chain of causation between the employee's duties and the breach[87]	Taking advantage of an opportunity to commit an act not authorised by the employer [87].
Acting on the employer's business [87]	

Table 3: Factors relevant to determining vicarious liability

The next chapter explains how the consent of the person to which the confidential information can release the holder of that information for their duty of confidence in making a disclosure. The elements of a valid consent, and those factors that would make a consent invalid is considered in some detail.

3. Defences – consent

3.1 Introduction

In the law of tort, consent is considered a defence. In other words, it provides a legal excuse for performing actions that may otherwise breach a duty to another. In law, the Latin maxim *'volenti non fit injuria'* (to a volunteer, injury is not done) is often used to describe consent, with Breach of confidence cases such as Freeman v. Home Office referring to the maxim to describe the application of the defence [99].

In A.G. v. Guardian Newspapers [1988], at the Court of Appeal, Lord Bingham stated:

> 'It is a well-settled principle of law that where one party (the confidant) acquires confidential information from or during his service with, or by virtue of his relationship with, another (the confider), in circumstances importing a duty of confidence, the confidant is not ordinarily at liberty to divulge that information to a third party without the consent or against the wishes of the confider. The essence of the confidant's duty is to preserve the confidentiality of the confider's information [28].'

The definition of consent has not been set out in any detail in cases that relate to confidentiality. There are however a variety of principles, both in tort, and other areas of the common law, that can be applied to define consent. These will be applied appropriately in this chapter.

The elements to a valid consent at common law can be summarised under three headings. In summary these are:

1. The person must have knowledge what they are consenting to [100], and have capacity to understand what they are consenting to [101]
2. Any consent must be given freely, without any influence or coercion [102]
3. Consent must be indicated [103].

3.2 Knowledge

3.2.1 The basic principle

The basic principle is that a person must know what they are consenting to for the consent to be valid [104]. If an individual does not know what they are consenting to, then any consent that has been provided cannot be not valid consent [104].

In Re Caughey ex p. Ford (1876) [100] Jessel MR stated:

> 'You cannot consent to a thing unless you have knowledge of it [100].'

The extent to which an individual needs to be informed appears to vary dependent on that to which the subject is consenting to [105].

3.2.2 Knowledge and implied consent

3.2.2.1 Reasonable expectations and knowledge

In some circumstances what is being consented to, albeit impliedly, may be more obvious. For example, in the absence of any statutory function by which an organisation can justify the requirement to have data disclosed to it[2], any use of information that would be in the reasonable expectations of the reasonable patient could be used on the basis that consent is implied [106].

It is important to note that the consent obtained prior to a medical procedure taking place, including the requirements to inform the patient of any risk [107], serve the purpose of providing consent to battery as is necessary before certain procedures take place [108]. In the case of an

[2] This is described in more detail in Chapter 6

implied consent to battery there are more limitations as to what will be accepted as implied consent, as explained in Marland v. Director of Public Prosecutions [109], although this falls outside of the scope of this thesis.

Where a patient has been treated within a healthcare system, knowledge of those circumstances relating to their care and management and financial processes are often inferred [106]. It could be suggested that where organisations are not established by Statute, such as where they are contractors of NHS services, implied consent can be relied upon as it is in the reasonable expectations of the patient.

In Murry v. Express Newspapers Plc [110] Lord Nicholls stated:

> 'Essentially the touchstone of private life is whether in respect of the disclosed facts the person in question had a reasonable expectation of privacy [111].'

Where it is within the reasonable expectations of individuals that information will be shared in certain circumstances therefore, the use of that information will be lawful [111].

In R (W and others) v. Secretary of State for Health (British Medical Association intervening) [112] it was stated that:

> 'The duty of confidence originates as a professional duty of the treating doctors, nurses and ancillary staff. Plainly they are entitled, without being in breach of that duty, to pass the Information to hospital administrators for the purpose of record keeping and of recovery of the charges [106].'

On analysis of this statement, it appears obvious that passing information collected in the hospital to local administrators would not amount to a breach as there has been no disclosure outside of the organisation. This said, disclosures to other bodies who undertake normal business activities on behalf of the hospital would also fall into this bracket of disclosure. The example here could be those administrative activities undertaken by the NHS Wales Shared Services Partnership in Wales on

behalf of the Health Boards, although in these circumstances, it could be argued that the broader statutory functions of those organisations would mean that there would be no need to imply consent [113][3].

It could be noted at this stage that where implied consent relies on the principle of reasonable expectations of individuals, it is unlikely that any use of information that poses a high risk could be in the reasonable expectations of individuals. Even if patients are informed of a risk of any specified use at the point of collecting data, albeit on the ward, the simple fact that an individual is aware of the risk does not mean that any breach of the common law duty of confidence, or any other tort, has been waived [114]. There must be an agreement to expressly or impliedly waive the common law duty of care to demonstrate acceptance of that risk [114]. This is described in more detail in the section below as relates to knowledge where consent has been expressly provided.

While it may be easy to justify the disclosure of information in a healthcare system, there may be circumstances where innovation or other activities could be viewed as being in the reasonable expectations of patients. One of the difficulties with the common law in this regard is how broadly it could be said that something is in the reasonable expectations of an individual. Information in digital format is much easier to compile and use for a variety of purposes. Data analytics can be undertaken outside of the treating body for the most legitimate purposes, but because the information has been disclosed a lawful excuse must be established, otherwise there will be a breach of confidence [88].

The late Dame Fiona Caldicott as National Data Guardian wrote to the Information Commissioner following reports that 1.6 million patient records had been shared by the Royal Free NHS Foundation Trust with DeepMind [115]. The Trust maintained that the disclosure was lawful as the system was to be used for direct care purposes and therefore

[3] See Chapter 6 for an explanation as to how the powers of statutory organisations enable information to be shared to satisfy those functions.

consent was implied. In her investigation, the National Data Guardian discovered that the system was not yet in use in the hospital and that only a prototype system had been developed. She therefore concluded that the sharing of these records was not for a direct care purpose and therefore it was not in the reasonable expectations of patients that this type of sharing would take place. Consent could therefore not be implied [115].

The legal requirements of all organisations to ensure transparency are described in the next section, and from a UK GDPR perspective are a requirement of all organisations processing personal data but are of particular use in informing explicit consent.

3.2.3 Knowledge and explicit consent

3.2.3.1 Preamble

Where a use of information is not within the reasonable expectations of a patient, explicit consent can be obtained as evidence of that consent. Only the elements of consent that relate to informing the patient are included in this section. Other information is explained in more detail throughout the course of the chapter.

3.2.3.2 Informing the patient

Where the explicit consent of a patient is to be relied upon to disclose confidential information, they must have knowledge of what they are consenting to prior to signifying their consent [116]. Informing individuals after they have signified consent will mean that the consent is not valid [116]. In such circumstances, unless another lawful excuse at common law can be identified, the patient would need to signify their consent again [116].

Providing information to a data subject in compliance with the fair processing requirements under the UK GDPR [9] may be useful in demonstrating that individuals have knowledge of the use of information. There is a requirement that information is provided to a data subject where data is collected from an individual [117], or where the data has not been obtained from an individual [118] regardless of the lawful basis.

3.2.3.3 Information on higher risk activities

Where the use of information carries any risk, it could be argued that the risks must be explained for consent to be valid [105]. There is no case law that sets out this approach in relation to the common law duty of confidence, however similar principles are adopted in other areas of the common law, including in the law of tort.

In Chatterton v. Gerson [105] a patient signed a consent form to undergo a medical procedure. The general nature of the injection that was due to be administered was known to her, but the doctor had not explained to her the significant risks associated with the injection. Therefore, even though the claimant has signed the claim form, as she did not have knowledge to the full extent as to what she was consenting to, the consent was not valid [119].

It could be suggested that the explicit consent of individuals would usually be required given that it could never be within the reasonable expectations of an individual that their data be used for high-risk processing. In the law of tort there is authority that suggests that even if there was knowledge of a risk and an individual was to participate anyway, this would not be enough to satisfy the requirements of valid consent. In Nettleship v. Weston, the doctrine of volenti non fit injuria was considered in relation to the tort of negligence. Lord Denning Master of the Rolls held that:

> ‘Knowledge of the risk of injury is not enough. Nor is a willingness to take the risk of injury. Nothing will suffice short of an agreement to waive any claim for negligence. The plaintiff must agree, expressly or impliedly, to waive any claim for any injury that may befall him due to the lack of reasonable care by the defendant: or more accurately, due to the failure of the defendant to measure up to the standard of care that the law requires of him [114].’

In other words, there needs to be an express or implied acceptance of that risk. It therefore seems clear that even an implied waiver must have knowledge and evidence of accepting that risk [114], otherwise, consent would be invalid.

Where the extent of a risk is properly explained to individuals [120], and the individual is fully aware of the consequences of any disclosure [121], they cannot then allege that there is a breach of confidence on the basis that they did not have knowledge [121]. The operation of this is illustrated by two cases. In Morris v. Murray [121] the plaintiff and his friend had been drinking all afternoon. They decided to go on a flight in the friend’s aircraft, and the plaintiff drove them to the airfield. The plaintiff helped refuel and start the aircraft. Early into the flight, the aircraft crashed, killing the plaintiff’s friend, and injuring the plaintiff. The plaintiff sued the estate of his friend.

In the Court of Appeal, Stocker L.J. stated that:

> ‘…on the basis that the plaintiff himself was capable of appreciating the full nature and extent of the risk and voluntarily accepted it, I would have no doubt whatever that this maxim would have applied to defeat his claim [122].’

Therefore, where an individual is made aware of a risk, or should reasonably have known about the risk but has expressly or impliedly agreed to that risk, the knowledge element of consent will be satisfied [123]. Where an individual is made aware of a risk, or should reasonably have known about the risk, but could not reasonably have known about the extent of the risk and wasn’t made aware of it, the consent defence will fail [123]. It is difficult to conceive examples of this happening in the

context of health services, but insofar as health information is used in a context unrelated to healthcare, it is possible that this consideration could prove relevant where information has been disclosed. It is nevertheless important to outline this principle, as this is relevant to the body of law being examined.

3.2.4 Misrepresentation and knowledge

Misrepresentation could apply as easily to the misrepresentation of risks, particularly where the extent of the risk is understated [123]. Misrepresentation as to any of the information around the use of data will mean consent is invalid [116].

When providing a patient with information on which to base their consent, that information must be honest and factual [116]. As stated above, it is important that any risks should be properly explained [119] and no misrepresentations should be made about the use or benefits of the obtaining or disclosing of data, or any of the uses of the data by which that data is to be used [116]. In some cases, it may be necessary to explain to the patient in such a way that the patient understands what they are consenting to [124].

In Freeman v. the Home Office (No 2) [125], Sir John Donaldson MR stated that:

> 'Consent would not be real if procured by fraud or misrepresentation but, subject to this and subject to the patient having been informed in broad terms of the nature of the treatment, consent in fact amounts to consent in law [116].'

Where consent is sought from an individual and role or qualifications of the person seeking the consent has been misrepresented to the patient, or has been used in a way to fraudulently ensure that consent is secured, the consent will not be valid [126].

In R v. Tabassum [126] the defendant was creating a database relating to breast cancer to sell to doctors. He had some medical knowledge and experience in relation to breast cancer; however, his training was not formal, and he had no medical qualifications. He convinced three women to allow him to examine their breasts for the purpose of creating the database. While there was no evidence of sexual motive, his conduct inferred he was a doctor and therefore the consent was not a valid consent [126].

From an information law perspective, the same could be said for those obtaining consent for purposes not connected to their treatment. For example, if a researcher impersonated a doctor in order to encourage a person to sign up to a study for the benefit of people with their condition, they may not only be misrepresenting the benefits of the sign up, but could mean that consent was invalid on the basis that the patient had made that consent on the basis of their professional integrity and qualifications.

3.2.5 Knowledge and capacity

At common law, a person can only consent if they have the capacity to do so [101]. It follows that to imply their consent; an individual would also need to have capacity. Capacity can apply to those who lack mental capacity or those that are incapacitated.

The question of mental capacity is a developed area; however, a summary of the main legal principles is included for completeness.

3.2.5.1 The Mental Capacity Act 2005

Section 2(1) of the Mental Capacity Act 2005 states that:

> 'A person lacks capacity in relation to a matter if at the material time he is unable to make a decision for himself in relation to the

matter because of an impairment of, or a disturbance in the functioning of, the mind or brain [127].'

The definition makes clear that the lack of capacity is relevant at that material time that they need to make the decision. The lack of capacity may be of a permanent or temporary nature [128].

A person can only be said not to have capacity under the statutory regime where on the balance of probabilities [129]:

'...he is unable to:

(a) to understand the information relevant to the decision [130],
(b) to retain that information [131],
(c) to use or weigh that information as part of the process of making the decision [132], or
(d) to communicate his decision (whether by talking, using sign language or any other means [133].'

Unless it can be demonstrated that a person does not have capacity, individuals over the age of 16 [134] are assumed to have capacity [135]. Capacity or lack of capacity cannot be assessed on the basis of a person's age or appearance [136]; or any condition or any aspect of their behaviour that could lead to unjustified assumptions about capacity [137].

It should be reiterated that where someone has presumed capacity, information must be explained to them in a way that they understand to ensure they know what they are consenting to [124].

3.2.5.1.1 Understanding information relevant to the decision

An individual must be able to understand the information relevant to the decision [130] to have competence to make that decision. If it is possible to explain to an individual in a way that they can understand such as using simple language, visual aids or any other means [138] then an individual will not lack capacity. It is important to note that an individual must not be treated as being unable to make a decision unless all practical steps that can be made have been taken to assist them [139].

3.2.5.1.2 Retaining the information

An individual who is only able to remember information relevant to the decision that they need to make for a very short time may still have mental capacity under the Act [140].

3.2.5.1.3 Using or weighing that information as part of the process of making the decision

'Deciding one way or another [141]', or '*failing to make the decision* [142]' are both factors demonstrating capacity. It is important to note that a person must not be treated as unable to make a decision because the decision they take is 'unwise [143]'.

3.2.5.1.4 Communicating his decision

A person must be able to communicate their decision to demonstrate that a decision has been taken either way. The communication may be by any means to demonstrate that their decision has been made *(whether by talking, using sign language or any other means* [144]*).*

3.2.5.2 Lack of capacity and competence in adults at common law

Where a person is deemed to have capacity under the Mental Capacity Act [145], they may still not be competent to make a decision. In the case of In Re L (Vulnerable Adults: Court's Jurisdiction) (No 2) (CA) [146], the court held that the common law definition of capacity existed notwithstanding the passing of the 2005 Act and therefore even where there was not an 'impairment of, or disturbance in the functioning of, the mind or brain' they may nevertheless lack capacity at common law [147].

Outside of the legislation the picture as to whether an adult has capacity is a complex one and has not been tested in the courts. There is however

some guidance of the characteristics that capacity may possess, however. The House of Lords in Gillick v. West Norfolk and Wisbech Area Health Authority [1986] [148] for example identifies a child as having mental capacity where:

> 'He reaches a sufficient understanding and intelligence to be capable of making up his own mind on the matter requiring decision [149].'

Similarly in the case of capacity to make a will, in the much earlier case of Banks v. Goodfellow [150] it was held that:

> 'It is essential to the exercise of such a power that a testator shall understand the nature of the act and its effects; shall understand the extent of the property of which he is disposing; shall be able to comprehend end appreciate the claims to which he ought to give effect; and with a view to the latter object that no disorder of the mind shall poison his affections, pervert his sense of right, or prevent the exercise of his natural faculties; that no insane delusion shall influence his will on disposing of his property, and bring about a disposal of it which would not have been made otherwise [150].'

In assessing capacity at common law therefore, in order for consent to be valid, it is necessary that the person consenting has sufficient intelligence and understanding of making decisions [149] so as to properly understand the effect of such consent [150].

3.2.5.3 Powers of Attorney and the Court of Protection

Powers of Attorney and the role of the Court of Protection is out of scope of this thesis.

3.2.5.4 Children aged 16 and 18

The Children's Act 1989 [151] Act defines a child as being an individual under the age of eighteen [152] years of age. The Family Law Reform Act 1969 [153] further confirms that a child over the age of sixteen can

consent to receiving surgical, medical or dental treatment and therefore does not need to have parental consent [154]. If a child has not reached the age of sixteen however, this does not mean that they cannot consent [155].

It is the accepted position that a child of a very young age does not have the intelligence or understanding to give consent [56]. Insofar as a child without competence is concerned, the parents have parental rights in making a decision for the child [148]. As Lord Fraser identified in the key case of Gillick v. West Norfolk and Wisbech Area Health Authority [1986]:

> 'I hold, that parental rights to control a child do not exist for the benefit of the parent. They exist for the benefit of the child, and they are justified only in so far as they enable the parent to perform his duties towards the child, and towards other children in the family [156].'

As the child gets older however, their intelligence and understanding matures, and so too does the influence of the of the parent over the child [157]. The courts recognise that independence occurs gradually as the child gains more maturity and understanding [158]. This is a '*dwindling right* [157]' that is eventually extinguished at child's eighteenth birthday [157] that starts with control at a young age and ends with the parent presenting an advisory role [157]. There is therefore no fixed age at which a child may be deemed competent to consent [159]. As Lord Scarman said in Gillick v. West Norfolk and Wisbech Area Health Authority [1986] [148]:

> 'Parental right yields to the child's right to make his own decisions when he reaches a sufficient understanding and intelligence to be capable of making up his own mind on the matter requiring decision [159].'

3.3 Consent must be freely given

3.3.1 The basic principle

The basic principle is that for consent to be valid, it must be freely given. In other words, for the defence of consent to be used for a disclosure of information that is subject to the duty of confidence, the consent must have been signified by a voluntary act [40].

3.3.2 Freedom of choice

An indication that the act of consent has been made voluntarily can be indicated by the freedom of choice. If someone does not have freedom of choice, then consent will be invalid [160].

3.3.3 Perceived obligations

The courts have recognised that where consent is only provided because of the perception that they have no alternative to consent because of a given set of circumstances or perform actions consistent with an implied consent because they feel they have no choice in the matter, the consent will not be voluntary and therefore cannot be valid. This is illustrated by the case of Bowater v. Rowley Regis Corp [160], where the claimant was employed as a road sweeper. He undertook his work with a horse drawn cart, however had protested that a particular horse that he had been provided with was known to misbehave, His manager ordered him to work with the horse. On one occasion thereafter, the horse bolted causing him serious injury. In defence to the resulting claim in tort, the Rowley Regis Corporation had argued that he had consented to take the horse in performing his duties. This defence failed, as Mr Bowater was seen to have no choice in the matter and therefore consent was not valid [160].

The principles of perceived obligations in relation to consent have been considered in other areas of information law. While the UK GDPR provisions around the lawful basis of consent [161] are out of scope of this thesis, it is interesting to note that Article 7 of the UK GDPR provides that:

> 'When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract [162].'

In applying consent as a lawful basis as a public authority or other organisation where an individual may feel that the provision of a service is dependent on that consent, the Information Commissioners Office advises:

> 'If you make consent a precondition of a service, it is unlikely to be the most appropriate lawful basis.
>
> Public authorities, employers and other organisations in a position of power over individuals should avoid relying on consent unless they are confident, they can demonstrate it is freely given [163].'

While this guidance does not relate to consent within the meaning of the common law duty of confidence, it is useful in setting out the principle explained in Bowater v. Rowley Regis Corp [160] can operate.

3.3.4 Undue influence and decisions

Where consent has been made under duress or obtained by persuasion, it can be said that the consent was obtained by undue influence and therefore will be invalid [164]. An important observation with any undue influence is that there is no requirement for there to be any bad intention in the persuading or pressurising an individual to consent [165]. It could simply be that the individual unduly influencing another person believes that it is in their best interests to consent in certain circumstances. For example, a person may be persuaded to consent to a family member such

as a spouse or parent having access to medical records as the family member perceives that they need to be guided in healthcare decisions.

Forms of unacceptable conduct that would amount to undue influence were identified in Royal Bank of Scotland plc v. Etridge [166]. It was explained there were two types of undue influence that could arise:

> 'The first comprises overt acts of improper pressure or coercion such as unlawful threats. Today there is much overlap with the principle of duress as this principle has subsequently developed. The second form arises out of a relationship between two persons where one has acquired over another a measure of influence, or ascendancy, of which the ascendant person then takes unfair advantage [164].'

It could be argued that the second example is too restrictive. There is a real possibility that more than two people could be involved in persuading or influencing someone to consent in a sustained way. That said, the statement is not incompatible with that possibility.

3.3.4.1 Undue influence and health

Where there is a lesser degree of discussion on the subject of consent, that would not appear to amount to persuasion with a person who is well, where a patient is unwell, it could be perceived that consent was only made so that they could have peace while they were feeling unwell [167]. Where consent is obtained from anyone who is unwell therefore, this should be treated with caution [167]. In Re T (Adult: refusal of medical treatment) [168] the susceptibility of a claimant to be unduly influenced by being persuaded to consent was particularly emphasised:

> 'Does the patient really mean what he says or is he merely saying it for a quiet life, to satisfy someone else or because the advice and persuasion to which he has been subjected is such that he can no longer think and decide for himself? [167]'

Further into his judgement, on the case Lord Donaldson of Lymington, the Master of the Rolls explained that the strength of the patient was one of the key factors that could lead to an undue influence. He explained:

> 'One who is very tired, in pain or depressed will be much less able to resist having his will overborne than one who is rested, free from pain and cheerful [167].'

It is suggested that this stands to reason. Where someone is unwell, to have a break from any repeated requests for permission, or even to avoid being asked again, an agreement to consent could be made that is one that would not otherwise have been made. This could cause real concern where consent is sought from patients on wards to obtain information for medical research, and researchers should be acutely aware of this, particularly where someone is very weak or in pain.

3.3.4.2 Undue influence and relationships

The case of Re T (Adult: refusal of medical treatment) [168] also identified another situation in which undue influence could be more obvious, that of the relationship of the person seeking influence the consent to the person giving the consent. It was said that:

> '...the relationship of the 'persuader' to the patient may be of crucial importance. The influence of parents on their children or of one spouse on the other can be, but is by no means necessarily, much stronger than would be the case in other relationships [167].'

It is submitted that this makes sense. A stranger may have little influence in persuading someone to consent. Individuals may feel less pressure in walking away from a position where there is no relationship. The closer the individual is to a person however, the more opportunity they have to try and influence someone, and the more influence they may have. The age of the parties in any relationship may be a factor in influence as well [169]. This is described under the next heading.

3.3.4.3 Undue influence and Age

The age of the parties involved may impact undue influence. Where a person is older and more mature, there is less likelihood of an influence being inferred [169]. A younger person however may feel more at pressure to oblige and give their consent [169]. This was highlighted quite succinctly in Powell v. Powel [170]. It was observed that:

> 'A man of mature age and experience can make a gift to his father or mother because he stands free of all overriding influence except such as may spring from what I may call filial piety; but a young person (male or female) just of age requires the intervention of an independent mind and will, acting on his or her behalf and interest solely, in order to put him or her on an equality with the maturer donor who is capable of taking care of himself [169].'

There could be any number of reasons an older person could want to influence and access the record of a younger person, such as a child who is competent. The suggestion is that intervention is important to ensure that consent is valid [169]. In a practical scenario, this could involve a discussion with individual, away from the party influencing the party. The appropriate methodology is not in scope of this thesis.

3.3.4.3 Undue influence and Religion

The law has also recognised situations where undue influence has occurred that relate to religious belief, particularly where someone is of the same faith. In Re T (Adult: refusal of medical treatment) [168] it was stated that:

> 'Persuasion based upon religious belief can also be much more compelling and the fact that arguments based upon religious beliefs are being deployed by someone in a very close relationship with the patient will give them added force and should alert the doctors to the possibility—no more—that the patient's capacity or will to decide has been overborne. In other words, the patient may not mean what he says [167].'

It is possible that the type of scenario where a religious organisation may influence consent to view health information, would be where a religious organisation, or a family member with strong beliefs sought to ensure that a medical intervention that conflicted with the religion has not occurred. Examples include, to find evidence of certain prescribed medications, to find evidence of an abortion, or to find evidence of a medical procedure such as a blood transfusion. These could be the kinds of things that are influenced for other reasons of course, such as where a parent wants to check if a child is on birth control medication.

3.3.4.4 Undue influence but free choice

Many of the circumstances explained in the above headings indicate the types of influence that may be more obvious when someone gives consent, and it may be that an undue influence can be proven in certain circumstances, The fact that someone has been trying to unduly influencing someone is not necessarily conclusive where a decision is subsequently made of the individuals own free will [171]. In such circumstances, consent will be valid [171].

3.4 Indication of consent

3.4.1 The basic position

For consent to be valid, the consent must be signified by the person giving that consent. In other words, their actions must indicate consent. In Bell v. Alfred Franks and Bartlett Co Ltd and another [172] Megaw LJ stated that:

> ''consent' involves some affirmative acceptance, not merely a standing by and absence of objection. The affirmative acceptance may be in writing, which is obviously the clearest; it may be oral; it may conceivably even be by conduct, such as nodding the head in a specific way in response to an express request for consent. But it

> must be something more than merely standing by and not objecting [103].'

As noted previously in this chapter, any indication of consent does not necessarily amount to a valid consent [119]. The person consenting must have knowledge and capacity [119].

3.4.2 Express consent

3.4.2.1 Consent in writing

It is accepted that written consent is the clearest form of consent [103].

At common law, written consent is not a requirement, and the absence of a consent form does not invalidate consent [173]. In Taylor v. Shropshire Health Authority [173] therefore, where a patient with capacity was provided sufficient information on which to consent, and then had voluntarily signified consent, the consent was held to be valid.

Mr. Justice Popplewell held:

> 'For my part I regard the consent form immediately before operation as pure window dressing in this case and designed simply to avoid the suggestion that a patient has not been told. I do not regard the failure to have a specialised consent form at the time to be any indication of negligence [174].'

While a consent form is not required to demonstrate that consent to any tort, including breach of confidence has been given, it provides clear evidence of the act of consent [103]. This does not however remove the requirement that the patient must know what they are consenting to for consent to be valid [175].

3.4.2.2 Oral consent

Consent can be communicated orally [103].

3.4.2.3 Consent by silence is not consent

Where someone is informed about what the nature of something that they are being asked to consent to, such as sharing medical records, their silence on the matter does not signify consent [103].

As stated above, in the case of Bell v. Alfred Franks and Bartlett Co Ltd and another [172] Megaw LJ stated that:

> ''consent' involves some affirmative acceptance, not merely a standing by and absence of objection… …but it must be something more than merely standing by and not objecting [103].'

That said, if there is no written consent, and the person has not spoken to confirm their consent, this does not mean that the individual has been silent about signifying consent. Consent may be implied.

3.4.3 Implied consent

3.4.3.1 'Expressly implied' consent

The type of consent described in this section is where consent is signified by positive actions that can be implied to amount to consent. These include the more obvious actions from which consent may be implied, such as where individuals have given a positive gesture such as giving a gesture such as nodding their head or by giving a 'thumbs up' [103]. In some circumstances there may be no specific gesture to signify consent, but the conduct of a person will signify that consent.

In Sunderland v. Barclays Bank Ltd [176] where a bank manager telephoned Mrs Sunderland about a cheque that the bank had refused to honour, and Mrs Sunderland handed the phone to her husband, it was held that the Bank Manager was entitled to consider that she had implied consent to speak to her husband. It could therefore be suggested that this objective view is relevant in such circumstances.

The Sunderland case also identifies one other element of relevance in forming such a view – the relationship of the parties. Parque L.J. stated that:

> 'There were many things which a doctor, for example, would not repeat to anyone else, but would not hesitate to repeat to a husband about his wife or vice versa [176].'

While attitudes could be considered as having changed since the 1930s when the Sunderland case was heard, this is nevertheless relatable. Spouses, or even other relatives are often asked to attend appointments and will be present to provide support. It would not therefore be unusual for a medical professional to openly describe the nature of any medical condition while a partner or other individual is in the consulting room. Obviously the same would not apply to any support a person may have in the doctors waiting room. It would also be wise to seek consent to discuss where a patient is on a ward and has visitors, as it may not necessarily be the case that the patient is content with them hearing details around their health. In any cases however it could be useful to check with the patient that they are happy to discuss matters relating to their health to avoid any doubt and to avoid an unlawful disclosure.

3.4.3.2 Consent implied by participation

The heading is an invention of the author, as there is no standard definition of this concept as relates to the common law. In the NHS and other healthcare services, the more familiar terms such as 'direct care' and 'indirect care'. would fall under this heading, although for many

organisations the provision of healthcare or other services forms part of their statutory functions[4]. The requirement for consent in connection with the undertaking of a medical procedure should not be confused with consent to share information.

Where an organisation is not subject to a statutory function, the argument could be made that in attending a healthcare environment for a consultation or treatment, that there is an expectation that certain uses of information will be inevitable from any consultation [106]. It inevitable that information will be required for several purposes, both in connection with their care, and to effectively manage NHS services [106]. In any case, for the purpose of the function and operation of the NHS, implied consent is more readily applied to the various transfers of information than it is to transfers outside of the service [40].

3.4.3.3 Implied consent without capacity

For completeness, it is useful to observe, that where a patient is unconscious and information needs to be shared in relation to that patient, there can be no consent [177], and consent cannot be said to be implied in any circumstances [178]. In such circumstances, the provisions of the Mental Capacity Act 2005 apply [178].

.

From an information law perspective, as with consent where individuals have capacity, it could be suggested that as the information has been lawfully disclosed or collected, there is no reason why the NHS organisation cannot use that information for any other purpose, providing they maintain the confidentiality of the patient [12], and any onward disclosure to other organisations relating to the wider NHS, or the recovery of costs will usually either be lawful because it forms part of those organisations statutory functions as set out in their Establishment Order, or in directions, or the data could be disclosed lawfully anyway because it is permitted in legislation [106].

[4] See chapter 6 for more information as to how statutory functions operate in Wales

3.5 Consent: a common law and UK GDPR comparison

3.5.1 The basic definition in the GDPR

The UK GDPR defines consent as:

> '…any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her [179].'

Particularly where the express consent of an individual is sought to obtain or disclose data, it could be tempting to assume that the same lawful basis and condition of processing should be used when processing health information in the UK GDPR and the Data Protection Act 2018. The following section explores the data protection definitions of consent and explains why consent may not always be the most appropriate lawful basis to use for the purposes of the data protection legislation.

3.5.2 The UK GDPR: Establishing a lawful basis for processing and a condition of processing.

For personal data within the meaning of the UK GDPR [23] to be processed lawfully, at least one lawful basis under Article 6 must be identified. There are six provisions under Article 6, each presenting a different lawful basis. Information that is subject to the common law duty of confidence, where it meets the definition of a data subject, will also be subject to the UK GDPR. One of these lawful bases is consent [161]. The UK GDPR provides that personal data may be processed lawfully if:

> 'The data subject has given consent to the processing of his or her personal data for one or more specific purposes [161].'

Article 9 of the UK GDPR prohibits the processing of special category data by default [180]. special category data is defined as those:

> '..personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation... [180].'

Article 9(2) of the UK GDPR provides that the prohibition on processing Special Category does not apply where one of ten conditions of processing this data can be met [181]. One of these conditions of processing is explicit consent [182]. Article 9(1)(a) provides that special category data can be lawfully processed where:

> 'The data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where domestic law provides that the prohibition referred to in paragraph 1 may not be lifted by the data subject [182].'

The definition of consent and compatibility with the common law duty of confidence is explored in more detail below.

3.5.3 A note on personal data, special category data, and the duty of confidence.

It should be noted that not all information that is personal data or special category data will be data that is subject to the duty of confidence. For example, ethnic origin, political opinions, religious or philosophical beliefs, and trade union membership are unlikely to be considered subject to the duty of confidence. Also, not all information subject to the duty of confidence will be personal data or special category data; for example in the case of health data, on the death of a data subject, the UK GDPR will no longer apply [183], however the duty of confidence will persist [63].

3.5.4 Comparison between the common law and UK GDPR definitions

3.5.4.1 Knowledge

In terms of the common law duty of confidence, knowledge also features as an important part of establishing a valid consent [100], and a lack of knowledge clearly means that consent will not be valid. This said, what consent may be required as acceptable in common law will very much depend on what the situation is. For example, if there is a risk attached [105] or the reasonable expectation of the use of data is more remote [106] more explanation may be required. [119] and it may be necessary to present consent in a way the patient understands [124]. However, where a patient visits a NHS General Practitioner, or has treatment in a NHS hospital the knowledge of the consent they impliedly provide is based on what is reasonably expected in the circumstances [106]. The reasonable expectation could be said to include a broad number of activities [106].

The UK GDPR requires a significant amount of detail to be provided to data subjects in order to rely on consent as a lawful basis to process personal data [161], and consent as a condition of processing special category data [182].

Details of what the consent specifically relates to must be clearly described and distinguishable from any other information that may be provided [184]. The language used must be plain and clear, and presented in a way that is accessible to the data subjects [184]. It could be suggested that this will include communication methods by which specific data subjects may rely on such as braille, or where relevant, translated into a language best understood by the data subject.

When asking individuals for consent, the identity of all the relevant controllers must be made known to the data subject [185], full details of each processing activity must be identified, and it may be necessary to

identify a different consent for each type of processing [186]. It could be suggested that in approaching the issue of consent in this way, individuals would have a better choice as to what they are consenting to, and what they are not consenting to, and consent can be taken to be better informed.

On asking the data subject for their consent, a data subject must be informed that they can withdraw their consent [187]. Withdrawal of consent must be as straightforward as giving consent [187]. There are no such information requirements for a consent at common law.

Where consent is explicit, this must be honest and factual [116], with risks explained [119] and no misrepresentation as to the extent of the use of data [116].

The consent process in the GDPR relates to processing which encompasses all uses of personal data including *'collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction* [24]', whereas within the meaning of the common law, it stands to reason that once disclosed, data cannot be undisclosed.

In the event consent was appropriate to cover both common law and GDPR uses, the model of consent set out in the UK GDPR would clearly be the model that should be followed, as the requirements are more robust.

3.5.4.2 Freely given consent.

The common law recognises that in order for consent to be valid the consent must be a voluntary act [40] by which the person giving consent is exercising freedom of choice [160]. Where consent is signified, but they are only consenting because they have no choice in the matter, this

cannot amount to a valid consent [160]. The UK GDPR takes a similar approach in requiring that consent must be freely given [179].

There is however a clear distinction between how the common law operates, and the expectations of the UK GDPR. While perceived obligations[58] evidenced from the circumstances of the consent[6], or lack of choice would invalidate consent in both situation, as would any undue influence [160] it is clear that where there is a contract or a particular service consent may be invalid if it reliant on that service taking place [162].

Article 7 provides that when assessing whether consent is freely given 'utmost account [162]' should be taken of whether:

> '...the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract [162].'

The definition is further clarified in the recitals to the UK GDPR which state that:

> 'In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation [186].'

In the case of the NHS therefore, the concept of freely given consent as described by the UK GDPR [162] and the Recitals to the UK GDPR [186] would be difficult to apply in the general concept of the service they provide. It could be suggested that if ever a situation arose that explicit consent needed to be relied upon for the purposes of any activity, it would need to be made clear that those services they would be receiving are unaffected by the consent. Such a scenario is unlikely given the other provisions that can be relied on to lawfully process personal data [188]

and those conditions of processing that can be relied on to process special category data [181] in the UK GDPR.

3.5.4.3 Indication of consent

In order to be valid consent for the purposes of the UK GDPR, consent must be made by a statement or by a clear affirmative action that signifies agreement to the processing of personal data relating to him or her for specific purposes [179]. Recital 32 provides some guidance as to what consists of an affirmative act. It states:

> 'Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent [189].'

The UK GDPR places an obligation on the Controller to be able to prove consent [190]. If the controller is unable to prove consent, the consent will be invalid [190]. It could be suggested that any use of consent under the UK GDPR must be supported by sufficient records proving that consent has taken place.

The common law duty of confidence has similar considerations. As stated in Bell v. Alfred Franks and Bartlett Co Ltd and another [172] by Mr. Lord Justice Megaw LJ:

> ''consent' involves some affirmative acceptance, not merely a standing by and absence of objection. The affirmative acceptance may be in writing, which is obviously the clearest; it may be oral; it may conceivably even be by conduct, such as nodding the head in a specific way in response to an express request for consent. But it must be something more than merely standing by and not objecting [103].'

At common law, written consent is the clearest form of consent [103], however consent can be communicated orally. Like the UK GDPR, consent must be a positive action [103]. Where the common law and UK GDPR differ however, is that the common law is more accepting of the principle of implied consent such as gesture such as nodding, or giving a 'thumbs up' [103], or that which is implied from actions [176]. It would be difficult for public services to rely on explicit consent within the meaning of the UK GDPR as many flows of data will be inevitable in connection with the effective operation of those services [106].

3.5.4.4 GDPR and common law consent: general comments

The purpose of the above analysis of consent as defined in the UK GDPR in comparison with the duty of confidence was to illustrate the increased expectations of the UK GDPR. There are clear differences in the standards required in each area of the common law and the UK GDPR. While it could be suggested that some of the expectations of the UK GDPR with regard to specific opt in for every data use would be impractical to use in the healthcare environment, it would be difficult to obtain consent on the basis that consent is not considered freely given where a particular service is being provided, and it is perceived that the consent is a prerequisite of that service taking place [162], particularly given that the NHS is a public body [186].

Consent is not, however, the only lawful basis for processing personal data. It is also not the only condition of processing special category data.

3.5.4.5 Establishing another lawful basis under GDPR.

In addition to consent, there are other types of lawful basis that can be relied upon when processing personal data. For example, in the case of a public authority that is undertaking responsibilities relating to their

functions, they may be able to rely on Article 6(1)(e) of the UK GDPR. This provides that personal data may be processed where the:

> 'Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller [191].'

Where a Public Body is required by law to collect personal data, for example Digital Health and Care Wales may have received a Direction under Section 23(1) of the National Health Service (Wales) Act 2006 to undertake a specific exercise that requires the processing of personal data, they can rely on the legal basis under processing under Article 6(1)(c) of the UK GDPR, which provides that:

> '...processing is necessary for compliance with a legal obligation to which the controller is subject [192].'

In addition to the consent [161], Public Task [191], and the Legal Obligation [192] lawful basis for processing, there are a further three lawful basis that can be relied upon. Further discussion on the lawful basis in the UK GDPR is out of scope of this paper.

3.5.4.6 Other conditions of processing special category data

There are also other conditions for processing special category data. Insofar as the NHS is concerned, where it relates to health and social care treatment or services, organisations can rely on Article 9(2)(h) of the UK GDPR which disapplies the prohibition on the processing of special category data where:

> '..processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of 6domestic law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph [193].'

In certain circumstances relating to the use of special category data for the purpose of public health, medical products, or medical devices where it is the public interest, the condition of processing contained in Article 9(2) may also be appropriate where the:

> 'Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of domestic law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy [194].'

In addition to the consent [182], healthcare purposes [193], and the public health [194] conditions of processing there are seven other conditions of processing. Further discussion on the conditions of processing contained in the UK GDPR is out of scope of this paper.

3.6 Summary of Chapter 3: Consent

The chapter provides an academic text systemising and explaining comprehensively existing knowledge in relation to the defence of consent as relates to the duty of confidence in the healthcare context. Table 4 (below) summarises the elements of a valid consent:

Principle	
The person consenting must be fully informed	Consent will be valid where the person is informed: • In an honest and factual way [116] • In a way that the person consenting will understand [124]. • Of any risks [120] and any potential consequences of them giving that consent [121]

Principle	
Continued	Consent will not be valid where: • The use or benefits are misrepresented to the person consenting [116] • The person consenting does not fully understand what they are consenting to [124]. • The role or qualifications of the person seeking consent has been misrepresented [126]. • Risks in the use of information are not highlighted or are misrepresented [119].
The person consenting must have capacity to consent	• Individuals over the age of 16 [134] are assumed to have capacity [135] unless demonstrated otherwise. • Capacity or lack of capacity cannot be assessed on the basis of a person's age or appearance [136]; or any condition or any aspect of their behaviour that could lead to unjustified assumptions about that person not having capacity [137]. • A child under 16 with sufficient understanding and intelligence to be capable of making up his own mind on the matter requiring decision has capacity [149]. The Mental Capacity Act specifies that a person lacks capacity if they are unable to make a decision in relation to something for themselves because of an impairment of, or a disturbance in the functioning of, the mind or brain [127].' A person lacks capacity where they are unable to: ▪ Understand factors relevant to a decision [130]. A person should not be treated as lacking capacity until all practical steps have been taken to assist them [139].

Principle	
Continued	▪ Retain that information [131] for enough time to make a decision [140]. ▪ Use or weigh-up information as part of the process of making the decision [132]. The process of weighing up information may mean a person makes a decision [141], or is unable to reach a decision [142]. An unwise decision is still a decision, even if it is unwise [143]. ▪ Communicate the decision [133], whether by talking, using sign language or any other means [144].
Consent must be given with the free will of the person consenting, without coercion or force.	A valid consent must be made with the free will of the person without coercion or force [40]. Consent is invalid where the consent has only been provided: • Because it is a precondition of receiving some other service [160]. • Because someone has persuaded or forced the person consenting [40] • As a result of improper pressure or an unlawful threat [164]. • Because of the relationship of the parties [164] • Because of some undue influence of what the person seeking consent says or does, even where this is meant with the best of intentions [165]. • Due to some the vulnerability of the person consenting, such where they are unwell and they believe that providing consent will mean they can have some peace and quiet [167].

Principle	
Consent must be signified by a positive act	Consent must be signified in some way, such as: • In writing [103] (a consent form is not necessary [174].) • By a gesture (e.g. a nod of the head or a 'thumbs up' [103]. • Some other conduct signifying consent (e.g. handing the phone to someone [176]).

Table 4: Elements indicating valid consent

Where a person receives a service (e.g. healthcare treatment), disclosures of information within the reasonable expectations of a person receiving the service are lawful [106]. In such circumstances consent is implied [106].

The next chapter relates to the public interest defence, and how information subject to the duty of confidence can be disclosed in circumstances where it is in the public interest to do so.

4. Defences - public interest

4.1 Introduction

Confidential information may sometimes be disclosed where it is the public interest to do so. In Attorney General v. Guardian (no 2) [91], Lord Goff stated:

> '...although the basis of the law's protection of confidence is that there is a public interest that confidences should be preserved and protected by the law, nevertheless that public interest may be outweighed by some other countervailing public interest which favours disclosure. This limitation may apply, as the learned judge pointed out, to all types of confidential information. It is this limiting principle which may require a court to carry out a balancing operation, weighing the public interest in maintaining confidence against a countervailing public interest favouring disclosure [195].'

In other words, wherever there is a question as to whether there is a public interest in disclosure, the starting point will always be maintaining the duty of confidence.

4.2 Public interest disclosures

4.2.1 Defining whether something is in the public interest

What is considered in the public interest has not been specifically defined in relation to the common law duty of confidence, but there are some cases that can assist in interpreting when public interest disclosures can be made. Official publications, such the Public Interest Supplementary Guidance produced by the Department of Health, recognise the significant lack of case law that set out the extent that public interest disclosures will be applied [196]. This chapter sets out the law as known.

In identifying whether it is in the public interest to disclose anything, the starting point is to establish the reason for the proposed disclosure and whether it is in the public interest to disclose in the first place. There is a distinction between what is considered in the public interest and what people may find interesting to know [197]. As Lord Wilberforce stated in British Steel Corporation v. Granada Television Ltd [198]:

> 'There is a wide difference between what is interesting to the public and what it is in the public interest to make known [197].'

In Lion Laboratories Ltd v. Evans [199] Mr Lord Justice Stephenson explained this in further detail stating:

> 'The public are interested in many private matters which are no real concern of theirs and which the public have no pressing need to know [200].'

When assessing whether something is in the public interest therefore, it is important to assess whether there is a pressing need to disclose information to the persons that the information is being disclosed to, and even then, only what is relevant to that pressing need should be disclosed [201].

4.3 Public interest as a defence

4.3.1 The basics

The public interest as relates to the common law duty of confidence is predominantly applied where there is wrongdoing or there is a likelihood of harm occurring.

The public interest defence was originally referred to the 'Iniquity Defence' following the case of Gartside v. Outram [202], and in particular the judgement of the then Vice Chancellor, Sir William Page Wood [203]. The case involved the disclosure of confidential information by a former

employee of a firm that undertook business as wool brokers to expose the fraudulent practices of his former employer, the Plaintiff, who was suing for breach of confidence. The Vice Chancellor found for the defence that the information had been disclosed lawfully, ruling that:

> 'The true doctrine is, that there is no confidence as to the disclosure of an iniquity. You cannot make me the confident of a crime or fraud and be entitled to close up my lips upon any secret which you have the audacity to disclose to me relating to any fraudulent intention on your part: such a confidence cannot exist [203].'

Over time the defence widened further to include situations that did not involve a criminal act or a fraud. In Initial Services Ltd v. Putterill [204], the defence had argued that as no crime or fraud had been committed that the defence could not be relied upon. Lord Denning, Master of the Rolls at the time, noted that the Queen's Council for the Plaintiff had:

> '...suggested that the exception was confined to cases where the master has been 'guilty of a crime or fraud.' But I do not think that it is so limited. It extends to any misconduct of such a nature that it ought to be in the public interest to be disclosed to others. Wood V. C. put it in a vivid phrase: 'There is no confidence as to the disclosure of inequity' [205].'

Lord Denning continued, that the Queens Council for the Plaintiff had:

> '...suggested that the exception is limited to the proposed or contemplated commission of a crime or a civil wrong. But I should have thought that was too limited. The exception should extend to crimes, frauds and misdeeds, both those actually committed as well as those in contemplation, provided always—and this is essential— that the disclosure is justified in the public interest. The reason is because " no private obligations can dispense with that universal one which lies on every member of the society to discover every design which may be formed, contrary to the laws of the society, to destroy the public welfare [205].'

The 'misdeed' to which Lord Denning was referring was the practice of price fixing that had been undertaken by a network of local launderettes to inflate prices for increased profits. While any business working in

collaboration with other businesses in any scheme should have been registered with the Board of Trade under the Restrictive Trade Practices Act 1956, they had not done so. Therefore, not only did Mr Putterill expose information that should have been public had the practice been properly registered, but he had also exposed a misdeed to which the duty of confidence would not be upheld [205].

It is also therefore clear that it is not only crimes, frauds or misdeeds that have been committed that can be disclosed, but also 'those in contemplation' of being committed [205], but only where 'the disclosure is *justified*[5]' in the public interest [205].

Soon after Initial Services Ltd v. Putterill, Lord Denning heard the appeal Fraser v. Evans [206]. Lord Denning, Master of the Rolls again presided over the case, and ruled that information subject to the duty of confidence could be disclosed where there was 'just cause and excuse' in the public interest, and specifically:

> 'It is merely an instance of just cause or excuse for breaking confidence. There are some things which may be required to be disclosed in the public interest, in which event no confidence can be prayed in aid to keep them secret [207].'

The case acts as a milestone in the changes that were to follow in the public interest defence and widens the scope of what may be considered in the public interest.

The case of Malone v. Metropolitan Police Commissioner [208] demonstrated that a more liberal approach was likely to be adopted where it may be important to disclose information where it was in the public interest. Megarry VC stated:

> 'There may be cases where there is no misconduct or misdeed but yet there is a just cause or excuse for breaking confidence. The confidential information may relate to some apprehension of an

[5] (Emphasis added)

> impending chemical or other disaster, arising without misconduct, of which the authorities are not aware, but which ought in the public interest to be disclosed to them [209].'

To date there have been several cases that demonstrate that information subject to the duty of confidence can be disclosed in circumstances.

It has been found in the public interest to expose cases of serious corruption [210]. Where there is evidence of malpractice that is identified, it may also be in the public interest to disclose confidential information to professional bodies, whether or not a criminal offence has taken place [211].

4.3.2 Exceptions to the rules as relate to wrongdoing

The case law indicates that the seriousness of the wrongdoing is a relevant factor when deciding on whether the defence can be relied upon [212], and even then, any disclosure must be proportionate to the public interest that it creates [212].

Therefore incidents such as minor criminal acts, such the fact an individual has smoked cannabis in their own home [213] will not defeat a breach of confidence claim, neither will private acts of consensual sexual activity between adults, even if this consisted of an offence of prostitution [214]. Although minor criminal acts that cause serious harm, may potentially be able to rely on this defence [215]. The public interest defence as relates to preventing harm is discussed under the heading below.

4.3.3 Safety and health

There is surprisingly very little case law to reflect any disclosures that have been made on the ground of safety health. Disclosures in this area of the defence of public interest are those that do not necessarily need to have any wrongdoing or misconduct associated to them. The primary

purpose is to protect people from harm, even where no crime has been committed [37].

It is important to note that, with regard public health, there are currently statutory mechanisms to make disclosures in some circumstances. An example of a statutory provision as relates to the processing of information for communicable disease surveillance is illustrated by the provisions of Regulation 3 of the Health Service (Control of Patient Information) Regulations 2002 [216]. The provisions relate to processing by to those employed or engaged for the purposes of the health service [217], a Government Department or other public authority in communicable disease surveillance [218]. This is explained in more detail in Chapter 5.

An extreme example of the public interest that may apply to protect public health and safety is illustrated in *obiter dictum* in the case of Malone v. Metropolitan Police Commissioner [208]. It was stated that information may be disclosed in:

> '...apprehension of an impending chemical or other disaster, arising without misconduct, of which the authorities are not aware, but which ought in the public interest to be disclosed to them [209].'

The gravity of such events described in this description are illustrative of situations where there may be a catastrophic disaster to protect the public, but it is illustrative of the public interest that exists to protect the public from harm [209]. It could be easily applied in situations where there may be a risk to the public from a communicable disease and information needs to be disclosed in relation to individuals who have that disease.

Where there is a threat to public a disclosure of health information subject to the duty of confidence may also be disclosed to the appropriate parties. In W v. Egdell [37], W had been diagnosed as a paranoid schizophrenic having shot several people, killing five. He had

been convicted of manslaughter by diminished responsibility and transferred to a secure hospital. Some years later, his lawyers were preparing an application for transfer to a less secure unit with a view to seek eventually discharge. Dr Egdell had been appointed to provide an independent psychiatric report which W hoped to use to demonstrate that he was safe to be rehabilitated in the community. In finding that the patient was more dangerous than other doctors had realised, he had disclosed his findings to the hospital, and later the Mental Health Review Tribunal on the grounds that W was a danger to the public. W sued for breach of confidence. It was held that despite the duty of confidence owed by Dr Egdell, the disclosure of information was lawful in that it was justified in the public interest based on legitimate concerns for public safety. Lord Bingham stated that:

> 'A consultant psychiatrist who becomes aware, even in the course of a confidential relationship, of information which leads him, in the exercise of what the court considers a sound professional judgment, to fear that such decisions may be made on the basis of inadequate information and with a real risk of consequent danger to the public is entitled to take such steps as are reasonable in all the circumstances to communicate the grounds of his concern to the responsible authorities [219].'

4.3.4 Other areas

It is conceivable that the defence could apply in other circumstances, but there is a lack of case law to be able to speculate on those areas. In the historic case of A B v. C D [220], in obiter dictum, Lord Fullerton stated of the duty of confidence:

> 'The obligation may not be absolute. It may and must yield to the demands of justice, if disclosure is demanded in a competent Court. It may be modified, perhaps, in the case alluded to in the argument, of the disclosure being conducive to the ends of science—though even there, concealment of individuals is usual.'

Reliance on this concept is uncertain. As a statement in *obiter dictum.* it is not binding, and in any case, given the passage of time, and the

existing mechanisms available in England and Wales law, such as Regulation 5 of the Health Service (Control of Patient Information) Regulations 2002[6], it could be suggested that reliance on such a defence would be unlikely to be accepted.

The full extent to which the courts will apply the public interest defence is therefore uncertain, with the Department of Health (England) guidance on public interest disclosures published in 2010 recognising this being an obstacle in making decisions as to whether other disclosures would be in the public interest [196]. The guidance recommended that where disclosures were proposed to be made that advice of the National Information Governance Board should be sought [196]. The National Information Governance Board were a body that once undertook functions to advise the Secretary of State for Health whether to approve disclosures utilising Regulation 5 of the Health Service (Control of Patient Information) Regulations 2002. The operation of Regulation 5 is discussed in more detail in Chapter 5. The role is currently undertaken by the Confidentiality Advisory Committee of the Health Research Authority.

4.3.5 Other public Interests out of scope of this thesis

The public interest as relates to the Administration of Justice, and National Security are out of scope of this thesis. It can be noted that this does not however mean they may have no relevance.

4.4 The public interest test

In demonstrating that disclosure is in the public interest, the public interest in disclosure must outweigh the duty to maintain confidentiality [212]. In making the assessment, it is important to recognise that maintaining the duty of confidence should always be an overriding consideration [195], and the argument in favour of disclosure must be

[6] See chapter 5 for further discussion on the Health Service (Control of Patient Information) Regulations 2002

significant enough in order to override the duty of confidence owed to an individual [212]. Adding weight to the argument based on multiple minor factors including minor or irrelevant criminal offences, or minor public interests will not be sufficient to override the duty [212].

4.5 Timing of the disclosure

The general principle is that the public interest defence can only be relied upon where the public interest exists at the time the disclosure takes place [221]. This can include past events, current events and events that could happen in the future [204] providing the public interest still exists in making the disclosure.

Where the public interest no longer exists, the defence cannot be relied upon. The case of Schering Chemicals Ltd. v. Falkman Ltd [47] related to the production of a drug that allegedly caused birth defects. There had been since been numerous scientific studies in relation to the drug. Given that the drug had been withdrawn from the market however, there was no longer a risk to safety. As Mr Lord Justice Shaw stated:

> 'The obligation of confidentiality may in some circumstances be overborne. If the subject matter is something which is inimical to the public interest or threatens individual safety, a person in possession of knowledge of that subject matter cannot be obliged to conceal it although he acquired that knowledge in confidence. In some situations, it may be his duty to reveal what he knows. No such consideration has existed in this case since the time that Primodos was withdrawn from the market. Neither the public nor any individual stands in need of protection from its use at this stage in the history. There is no occasion to beat the drum again. As to any rights or liability which may have arisen from the use of Primodos in the past, these will be determined by the outcome of the pending litigation [221].'

4.6 What can be disclosed and to who?

Only the information that there is a pressing social need to disclose should be disclosed [200]. Any other matters that are not in the public

interest to disclose should remain protected by the duty of confidence [200]. It is therefore important to distinguish between what is in the public interest to make known and to whom, and what the public may find interesting [197].

Where it is in the public interest to disclose information that is subject to the duty of confidence, this does not mean that the information can be disclosed to the world at large. When assessing the public interest, it is important to consider what information needs to be disclosed, and the parties the information is being disclosed to in order to fulfil that public interest. In Francome v. Mirror Group Newspapers Ltd [222] the Plaintiffs were spouses. The husband was a champion jockey. The Mirror Group had obtained tapes of private telephone calls made between the plaintiffs from a third party who had unlawfully recorded them. The defendants maintained that they exposed breaches of the rules of racing and sought to publish a story relating to this. Sir John Donaldson, Master of the Rolls stated:

> 'In the instant case, pending a trial, it is impossible to see what public interest would be served by publishing the contents of the tapes which would not equally be served by giving them to the police or to the Jockey Club. Any wider publication could only serve the interests of the Daily Mirror [223].'

Later in his judgement he added:

> 'Assuming that the tapes reveal evidence of the commission of a criminal offence or a breach of the rules of racing, and I stress that this is an assumption, it may well be in the public interest that the tapes and all the information to be gleaned there from be made available to the police and to the Jockey Club [224].'

This limiting principle is key to the operation of the defence. In Re A Company's Application [225], a company was refused an injunction preventing disclosure to the financial regulator and the inland revenue on the basis that it was in the public interest to disclose financial irregularities, but that such disclosure could only be made to them [226].

It is therefore important to consider where the public interest lies, and to distinguish whether instead that interest is one that the proposed recipient may find interesting for their own personal gain. As Lord Denning explained in Initial Services Ltd v. Putterill [204]:

> 'The disclosure must, I should think, be to one who has a proper interest to receive the information. Thus, it would be proper to disclose a crime to the police; or a breach of the Restrictive Trade Practices Act to the registrar. There may be cases where the misdeed is of such a character that the public interest may demand, or at least excuse, publication on a broader field, even to the press [205].'

This appears to make clear that sometimes the act is so serious that the wider population may have a public interest in knowing what has taken place.

4.7 The burden of proof

The basic position is that, to rely on the defence of public interest in disclosing information that is subject to the duty of confidence, the person seeking to disclose the information must be able to defend the position on the basis that the allegation has some substance. As Lord Keith stated in the Spycatcher case [91]

> 'As to just cause or excuse, it is not sufficient to set up the defence merely to show that allegations of wrongdoing have been made. There must be at least a prima facie case that the allegations have substance [195].'

In other words, where in any circumstances an allegation is made, it is important to avoid impulse and establish whether there is any substance to any suspected wrongdoing.

The exception to this rule is whereby the person to whom the information is being communicated to is a regulatory body, and the confidential information is evidence of a suspected breach [226]

4.8 Application in information in the National Health Service

In the National Health Service, there may be many situations by which health information may need to be disclosed to certain individuals or organisations depending on the situation in hand.

For example, where the individual poses a serious threat to the public because they have a mental health condition, it likely that they will need to furnish the police or other authorities with sufficient information to explain the risk [37]. Obviously, only the relevant health information should be considered for disclosure and be subject to the public interest test.

It is conceivable that a public interest defence could be used to disclose information to the relevant authorities where injuries have been incurred by a patient who has been the victim of a serious crime, or where they are the perpetrator of a serious crime [203]. Where the victim is conscious and competent, it could be suggested that their consent be sought in such circumstances in the first instance, especially considering that health information may need to be disclosed as part of any report to the police.

The public interest defence could also be relied upon where there is a danger of a public health or safety incident [209], although Regulation may provide a sufficient lawful basis to disclose information across multiple agencies in instances of communicable diseases and other risks to public health [227], particularly where there is no statutory function[7].

[7] Elements that relate to statutory functions of organisations, including the role of central digital functions in Wales, are explained in more detail in Chapters 5 and 6.

4.9 The public interest in the UK GDPR

It should be noted that the application of the public interest defence at common law bares no relevance to the lawful basis of processing of 'public interest' under the UK GDPR, although application of this lawful basis for processing may be appropriate depending on the circumstances.

4.10 Freedom of information and the exemption as applies to information held in confidence

While the author is also a subject matter expert in the subject of the operation of the Freedom of Information Act 2000, only the impact of the public interest defence to the information provided in confidence exemption is within the scope of this thesis.

4.10.1 Requests for information under the Freedom of Information Act 2000: the basics

The Freedom of Information Act 2000 enables a person to make a valid request for information as defined by the Act [228], to a public authority within the meaning of the Act [229]. Where a request is made the Act provides a general right for the requestor to be informed whether information is held by that Public Authority [230], known as 'the duty to confirm or deny [231]' and if so, to have the information communicated to them [232].

4.10.2 Exemption: information provided in confidence

Section 41(1) of the Freedom of Information Act 2000 provides an exemption for information where:

> '(a)it was obtained by the public authority from any other person (including another public authority), and

> (b)the disclosure of the information to the public (otherwise than under this Act) by the public authority holding it would constitute a breach of confidence actionable by that or any other person [233].'

This exemption is described as an 'absolute exemption in the Freedom of Information Act 2000 [234]. If information was obtained by the public authority from any other person [235], and disclosure of the information to the public, otherwise than in under the Freedom of Information Act 2000, the public authority would constitute an actional breach of confidence to the person holding it [236], the requirement to communicate the information to them does not apply [237].

Section 41(2) of the Freedom of Information Act 2000 states that:

> 'The duty to confirm or deny does not arise if, or to the extent that, the confirmation or denial that would have to be given to comply with section 1(1)(a) would (apart from this Act) constitute an actionable breach of confidence [238].'

This means that the duty to confirm or deny that information is held does not apply where this would constitute and actionable breach of confidence [238]. This is reaffirmed in relation to the effect of the exemptions as set out in Part 1 of the Act [239].

4.10.3 The relevance of the public interest test at common law as may apply to the exemption for information held in confidence

With exception of absolute exemptions, the Freedom of Information Act 2000 contains provision that in order for the public authority to be released from the obligation to disclose the information, the public interest in maintaining the exemption must outweigh the public interest in disclosing the information [240]. Similarly, with the exception of absolute exemptions, in order for the public authority to be able to refuse to confirm or deny that they hold information, the public interest in upholding the exemption on the duty to confirm or deny must outweigh

the public interest in disclosing whether information is held by the authority [241]. The effect of an absolute exemption therefore is that no other considerations relate to the exemption under the Freedom of Information Act 2000, the exemption is absolute.

Separately, the public interest test at common law as applies to information subject to the duty of confidence is relevant to deciding whether information should be disclosed. In the case of Derry City Council v. Information Commissioner [242], the application of the Section 41 exemption in relation to information provided in confidence failed on the basis of the public interest in disclosure as provided in the common law as relates to the duty of confidence [243]. This case is illustrative of the importance of understanding how defences to a disclosure under the duty of confidence, may be relevant to other areas of the law.

4.11 Summary of Chapter 4: Public Interest

The chapter provides an academic text systemising and explaining comprehensively existing knowledge in relation to the public interest defence as relates to the duty of confidence in the healthcare context.

The extent of what could be in the public interest may be quite wide [31], but this concept is untested, an obstacle in making decisions as to whether other disclosures would be in the public interest [32].

The following are some examples of things that have been said to be in the public interest:

- Serious crime or fraud [19].
- A minor criminal act that causes serious harm [28].
- Civil wrongs [20]
- Other misconduct or misdeeds that are not criminal or civil [20], including reporting cases of suspected malpractice to professional bodies [24].

- Activities contrary to public society and public welfare [20].
- Cases of serious corruption [23].
- No need to prove wrongdoing where the disclosure protects from harm to safety of health [29].
- It may be possible to rely on this to protect public health [22].'
- Disclosure of confidential health information may be made to the relevant parties where there is a danger to public safety *(e.g.* the responsible authorities [30].)

There is no public interest where there is a minor crime where there is no serious harm [25] such as smoking cannabis in private [26], or private acts of consensual sexual activity between adults, even where this consists of the offence of prostitution [27].

Table 5 (below) contains a summary of the key elements that should be considered when relying on the public interest defence:

Question	**Answer**
Is it in the public interest to make the disclosure of the information?	It is necessary to ensure that the information is truly in the public interest to disclose. There is a difference in identifying information that may be interesting to the public and that which is in the public interest [197]. Multiple minor public interest arguments do not add weight to the argument to override the duty [25]. It may be in the public interest to disclose acts that have been committed, or where an act may happen if the information is not disclosed[20], but only insofar as the disclosure is justified[20] and there is a pressing social need to disclose [17].

Question	Answer
What Can I disclose?	Maintaining the duty of confidence should always be an overriding consideration [33], and the argument in favour of disclosure must be significant enough in order to override the duty of confidence owed to an individual [25]. Where the public interest outweighs the duty of confidence, only information that there is pressing social need to make known should be disclosed [17]. The decision on what should be disclosed should be assessed in proportion to the public interest in disclosure [25].
Who can I disclose it to?	A disclosure of information must be limited to those parties who have a proper interest in knowing the information [20] and it is in the public interest to disclose to [36].
When can I disclose the information	The defence can only be relied upon at the time there is a public interest to disclosure [34]. The public interest may in some circumstances relate to a disclosure of information relating to past events, current events, or could be information that could impact events that could happen in the future if the information is not disclosed [35].
Can I evidence I was justified in making the disclosure?	The person disclosing any information must be able to defend the position on the basis that the public interest argument has some substance [33] unless the disclosure is to a regulatory body, and there is a possible professional conduct issue [38]. Speculation that there may be a substantial public interest is insufficient and a person disclosing may find themselves in breach of confidence should they disclose information [33].

Table 5: Public Interest Disclosures - Key Considerations

The next chapter explains how confidential information can be disclosed where it is permitted or required by statute. The chapter specifically considers the provisions of section 251 of the National Health Service Act 2006 and the current regulations that exist by virtue of these provisions.

5. Lawful disclosures – disclosures permitted or required by Statute

5.1 Section 251 of the National Health Service Act 2006

5.1.1 Introduction to section 251

The previous two chapters describe two defences to a breach of confidence at common law. This chapter focussed on a statutory mechanism to set aside the duty of confidence as relates to information generated in the National Health Service.

Section 251 of the National Health Service Act 2006 provides a mechanism by which patient information can be regulated. It is often stated that the purpose of section 251 is to enable patient information to be used without consent [244], While Regulations created under section 251 of the National Health Service Act 2006 can contain provisions to set aside the common law duty [245], this is one of many options contained in the legislation[8]. To understand how Section 251 operates however, it is necessary to look at the provisions to the extent that they can apply to any information to understand the types of Regulations that can be produced.

There are no academic texts that discuss the application of section 251 in any detail; therefore, it is proposed to discuss these provisions in the way that these apply to Wales. Further studies may be required in relation to these provisions and their operation in England, particularly where future amendments are made that apply only to England.

The historical context of these provisions will be explained in more detail when discussing the extant Regulations, which predate the current provisions under which they operate.

[8] Note that Section 261(2) includes the words 'may include' when providing particular provisions that may form part of the regulations.

5.1.2 Scope of Regulations issued under Section 251

It would appear that a court would likely conclude that the Regulations can only apply to information created within the NHS. In Lewis v. Secretary of State for Health and another [64], Mr Justice Foskett commented in obiter dictum on this issue as follows:

> 'I respectfully agree that there is nothing explicit in the Act and or Regulations confining the information concerned to NHS-generated information but, as I have said, the whole context would seem to suggest this. Had the matter been fundamental, I would doubtless have been invited to look more closely at the whole Act, and, perhaps, its legislative history and background. In the course of the relatively short argument, I have not been so invited and, accordingly, can express no view other than that which I have expressed [246].'

This observation was stated in obiter dictum and not as the ratio decidendi of the case. It is therefore not a binding precedent and therefore need not be followed by any other court. As per the judgement of Mr Justice Foskett, such a view would require a more detailed examination by the court where this was fundamental to a case [246].

Mr Justice Foskett made another statement in obiter dictum in clarifying whether Regulations could authorise use outside of the NHS in Lewis v. Secretary of State for Health and another [64]. He stated:

> 'If I was forced to conclude, on the arguments I have heard, whether the procedures afforded by the Act and the Regulations are available for the authorisation of the use of confidential patient information generated outside the NHS, I would have to conclude that it did not [247].'

Again, this is not a ratio decidendi, but more clearly indicative of the scope of the Regulations.

5.1.3 Amendments and devolution

5.1.3.1 Cities and Local Government Devolution Act 2016

Following the assent of the Cities and Local Government Devolution Act 2016 [248] provisions exist to create Regulation in relation to social care information. These amendments are reflected in the below text.

5.1.3.2 Devolution and the role of the Welsh Ministers

Functions under section 251 were transferred by Order to the Welsh Ministers by The Welsh Ministers (Transfer of Functions) Order 2018 [249]. The text in Section 251 of the National Health Service Act was not amended by legislation, however the implication of the transfer of any functions is that the reference to the Secretary of State should be read as if it directly refers to the Welsh Ministers to correctly reflect the operation of the legislation.

Article 1(5) of The Welsh Ministers (Transfer of Functions) Order 2018 provides:

> 'Any reference in this Order to a function of a Minister of the Crown under an enactment includes a reference to any functions of that Minister which are included in any scheme, Regulations, rules, Order, bye-laws or other instrument having effect under or in relation to that enactment, and the power to confer functions on that Minister by any such scheme, Regulations, rules, Order, bye-laws or other instrument has effect as a power to confer such functions on the Welsh Ministers [250].'

This means that any Regulation in existence under section 251 of the National Health Service Act 2006 is also devolved to the Welsh Ministers [250].

5.1.4 Powers to create Regulations under Section 251

Section 251(1) of the National Health Service Act creates a Henry VIII power that enables the Welsh Ministers to make Regulations. This section provides that the:

> 'Secretary of State may by Regulations make such provision for and in connection with requiring or regulating the processing of prescribed patient information for medical purposes as he considers necessary or expedient—
> (a) in the interests of improving patient care, or
> (b) in the public interest [251].'

This general provision contains wide powers to create Regulations that may require or regulate the processing of such patient information as may be prescribed for medical purposes. The test appears subjective in that the Welsh Ministers simply need to consider Regulations 'necessary or expedient' in achieving these purposes. The wording 'as he considers necessary [251]' suggests that the only the subjective view of the Welsh Ministers is required and there is no requirement to demonstrate this objectively.

5.1.5 Relevant definitions

5.1.5.1 Medical purposes

The definition of what is considered 'medical purposes' is set out explicitly in Section 251(12) of the National Health Service Act 2006. It provides that 'medical purposes' are those purposes of :

> '(a) preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of health and social care services, and
> (b) informing individuals about their physical or mental health or condition, the diagnosis of their condition or their care and treatment [252].'

The definition of medical purposes therefore has a wide scope of services. It is not only limited to the care of an individual but extends to activities such as health research.

The provision contained in Section 251(12) encompasses many direct care activities, whereas Section 251(4) provides that:

> 'Regulations under subsection (1) may not make provision requiring the processing of confidential patient information for any purpose if it would be reasonably practicable to achieve that purpose otherwise than pursuant to such Regulations, having regard to the cost of and the technology available for achieving that purpose [253].'

Clearly, medical research cannot be achieved without consent or an alternative lawful excuse, the likes of such which may include Regulations created under section 251, as it could be argued that this is not within the reasonable expectations of the patient. With regard to most other activities relating to the prescribing or administering of preventative medicine, medical diagnosis, the provision of care and treatment and the management of health and social care services, it could be argued that most of these activities would be in the remit of the direct care relationship anyway, and therefore could be reasonably practicable to achieve within the reasonable expectations of the patient. In the modern health service, it is also likely that bodies established in law to undertake functions will have an implied statutory duty to use information without consent [254].

Another point of note is that, in order to inform individuals about their physical or mental health or condition, the diagnosis of their condition or their care and treatment, there usually must be a relationship between the medical practitioner and the patient during the normal care relationship. This is where the technological aspect may be of relevance, as the cost of achieving effective communications, particularly if this is achieved on a mass scale, may be cost prohibitive, or technologically difficult if achieved without involving other bodies or agencies, and in

these circumstances, specific Regulations may be put in place to overcome these issues.

Section 251(6) explicitly excludes the creation of any Regulation for the sole provision of care. Section 251(6) says:

> 'Regulations under subsection (1) may not make provision for requiring the processing of confidential patient information solely or principally for the purpose of determining the care and treatment to be given to particular individuals [255].'

This narrows the scope of any Regulations that can be created. The use of Information in medical diagnosis and the provision of care and treatment can be justified under the common law as this is a use in the reasonable expectations of the patient. It could be suggested that the provision protects any interference in creating regulation that governs information exchange in direct care situations on an individual basis. This said, regulations could include situations where outside of the direct care relationship data is to be analysed for a variety of purposes including to create registries, to monitor medical devices and implants that may be faulty, or to detect and monitor disease or to deliver health screening or targeted treatments.

For illustrative purposes, a good example exists in the current Regulations in force under Section 251(1). The Health Service (Control of Patient Information) Regulations 2002, which permits the processing of Confidential Patient Information for the:

> '…the delivery, efficacy and safety of immunisation programmes [256].'

The Regulation enables information to be disclosed to another person outside the direct care relationship to compile immunisation priority lists to affect the most vulnerable without being in breach of confidence.

5.1.5.2 Patient information”

Section 251(10) provides that, for the purpose of section 251, “patient information” means:

> ‘(a) information (however recorded) which relates to the physical or mental health or condition of an individual, to the diagnosis of his condition or to his care or treatment, and
> (b) information (however recorded) which is to any extent derived, directly or indirectly, from such information, whether or not the identity of the individual in question is ascertainable from the information [257].’

Regulations under section 251 may therefore include information that is anonymised and is therefore not subject to the common law duty of confidence. It is difficult to imagine how such Regulations could apply to data that is truly anonymised, specifically as it could be obtained legitimately from any Public Body in the NHS by making a request pursuant to Section 1 of the Freedom of Information Act 2000. The effect of Henry VIII powers is however out of the scope of this thesis.

5.1.5.3 Confidential patient information

Interestingly, Section 251 of the National Health Service Act 2006 provides a definition of confidential patient information [258]. Section 251(11) states that:

> ‘For the purposes of this section, patient information is “confidential patient information” where—
> (a)the identity of the individual in question is ascertainable—
> (i)from that information, or
> (ii)from that information and other information, which is in the possession of, or is likely to come into the possession of, the person processing that information, and
> (b)that information was obtained or generated by a person who, in the circumstances, owed an obligation of confidence to that individual [258].’

The definition is of interest. Information may be generated or obtained by a person who owes an obligation of confidence to an individual, but the information that could be collected by that individual may include information that is not subject to the common law duty of confidence. The definition of confidential information in this context appears to apply to any information that is collected from any service user.

The definitions only apply to section 251 of the National Health Service Act 2006 and therefore do not influence the Common Law definitions [258].

5.1.5.4 Other definitions contained in Section 251

Other definitions are not relevant to the discussions contained in this chapter.

5.1.6 Specific provisions

5.1.6.1 Communications

Section 251(2) provides specific uses of the types of Regulations that may be made under Section 251(1). There is a stipulation that these may require [259]' and therefore these are specific clauses that may be included, they are permissive, they are not restrictive, nor exhaustive. Section 251(2)(a) provides that Regulations may make provision [260],:

> 'Prescribed communications of any nature which contain patient information to be disclosed by health service bodies or relevant social care bodies in prescribed circumstances—
> (i) to the person to whom the information relates,
> (ii) (where it relates to more than one person) to the person to whom it principally relates, or
> (iii)to a prescribed person on behalf of any such person as is mentioned in sub-paragraph (i) or (ii),in such manner as may be prescribed [259].'

This specifically referring to communications. It is necessary to explain this in more detail to understand the implications of such a provision on prospective Regulations.

The provision that enables Regulation to be put in place to use patient information to enable prescribed communications with the person to whom it relates [261] describes circumstances that, even where information subject to the duty of confidence was to be disclosed to those individuals, would *prima facie* not be in breach of confidence. The information relates to that person, and even if this information was confidential, there would be no disclosure. Given the wider scope of Regulations that may be created however, this may compliment an end-to-end process by which Regulations may determine acquisition and processing of data to make those communications.

When sending information to more than one person, but principally the information principally relates to one individual [262], there may be a duty of confidence owed. The information could potentially be confidential. An example of such an instance may be where a person in a household has a communicable disease, and the others may need to get tested, get treatment, or isolate. With some conditions, the public interest argument at common law may be difficult to demonstrate, and therefore Regulation may be put in place to determine how this can be achieved.

5.1.6.2 Disclosures or other processing

Section 251(2)(b) of the National Health Service Act relates to disclosures or other processing that may be regulated. Again, there is a stipulation that Regulations '...may in particular, make provision [260]' and therefore these are specific clauses that are specifical permissive, but are not restrictive, nor exhaustive.

As with the provisions relating to communications, it is necessary to explain this in more detail to understand the implications of such a provision on prospective Regulations.

Section 251(2)(b) provides that Regulations may require or authorise:

> 'The disclosure or other processing of prescribed patient information to or by persons of any prescribed description subject to compliance with any prescribed conditions (including conditions requiring prescribed undertakings to be obtained from such persons as to the processing of such information) [263].'

5.1.6.3 Provisions to set aside the duty of confidence

The Act provides a statutory provision that enables the Welsh Ministers to set aside the duty of confidence. Again, there is a stipulation that Regulations may, 'in particular, make provision [260]' and therefore these are specific clauses that are specifically permissive, but are not restrictive, nor exhaustive. This means that the Regulations need not specifically set aside a duty of confidence.

Section 251(2)(c) that:

> 'Where prescribed patient information is processed by a person in accordance with the Regulations, anything done by him in so processing the information must be taken to be lawfully done despite any obligation of confidence owed by him in respect of it [245].'

This general provision creates a specific right to set aside the duty of confidence. The current Regulations, the Health Service (Control of Patient Information) Regulations [264] makes use of this clause in setting aside any duty of confidence owed by stating:

> 'Anything done by a person that is necessary for the purpose of processing confidential patient information in accordance with these Regulations shall be taken to be lawfully done despite any obligation of confidence owed by that person in respect of it [265].'

5.1.6.4 Sanctions

Section 251(2)(d) makes provision that enables the Welsh Ministers to create sanctions for non-compliance with Regulations. With regard sanctions, the wording states that Regulations may, 'in particular, make provision[260]' for such sanctions, and therefore again, this clause permits sanctions to be included.

Section 251(2)(d) states that Regulations may provide for:

> '...creating offences punishable on summary conviction by a fine not exceeding level 5 on the standard scale or such other level as is prescribed or for creating other procedures for enforcing any provisions of the Regulations [266].'

Interestingly, the current Regulations impose a civil penalty of £5000 on anyone who does not comply with the Regulations [267], and this must be recovered by the Welsh Ministers as a civil debt [268]. This would be enforced by the Welsh Ministers based on their subjective view as to the seriousness of a breach [269]. The Regulations are discussed in more detail in this chapter.

5.1.6.5 Requirement to review Regulations

Section 251(5) provides that where Regulations provide for the processing of confidential patient information. The Secretary of State:

> '(a) must, at any time within the period of one month beginning on each anniversary of the making of such Regulations, consider whether any such provision could be included in Regulations made at that time without contravening subsection (4), and
> (b) if he determines that any such provision could not be so included, must make further Regulations varying or revoking the Regulations made under subsection (1) to such extent as he considers necessary in order for the Regulations to comply with that subsection. [270].'

This is a provision that positively requires Regulations to be reviewed with a view including additional provisions as may be necessary. As noted above, such provisions cannot contravene Section 251(4) in that they must not create an provision that requires the processing of confidential patient information, within the meaning of the Act, for any purpose if it would be reasonably practicable to achieve that purpose otherwise than pursuant to such Regulations, having regard to the cost of and the technology available for achieving that purpose.

It is difficult to know whether the current Regulations, the Health Service (Control of Patient Information) Regulations 2002, have been reviewed as required by this section. There is no requirement to publish this in the Regulations, and no set review process is in place. This nevertheless is a statutory requirement of the Secretary of State in England, and the Welsh Ministers in Wales.

5.1.6.6 Data protection implications

Section 251(7) provides that Regulations are not permitted to make:

> '...provision for or in connection with the processing of prescribed patient information in a manner inconsistent with any provision of the data protection legislation [271].'

This is self-explanatory. In terms of the duty of confidence however, section 251(8) makes clear that:

> *'Subsection (7) does not affect the operation of provisions made under subsection (2)(c)* [272]*.'*

This effectively means that even if provisions in the Regulations were contrary to the UK GDPR and/or Data Protection Act 2018, that there would be no breach of confidence by anyone relying on those provisions.

5.1.6.7 The requirement to consult

As a supplementary matter, Section 251(9) provides that:

> *'Before making any Regulations under this section the Secretary of State must, to such extent as he considers appropriate in the light of the requirements of section 252, consult such bodies appearing to him to represent the interests of those likely to be affected by the Regulations as he considers appropriate* [273].'

The requirement to consult is again a subjective matter, that can be assessed by the Welsh Ministers. There is no objective test required to ensure that certain bodies are consulted. This is unfortunate considering that Regulation may be made without full consultation of those bodies with interests in such Regulations, including professional bodies.

5.2 Current Regulations under section 251

5.2.1 Basic information

To date there are currently only one set of Regulations that exist under section 251(1) of the National Health Service Act 2006. These are the Health Service (Control of Patient Information) Regulations 2002. As the year of creation suggests, the Regulations themselves precede the current Parent Act.

The Regulations were originally created under section 60(1) of the Health and Social Care Act 2001. Many provisions in the Health and Social Care Act 2001, including Section 60, were consolidated into both the National Health Service Act 2006 and the National Health Service (Wales) Act 2006. Similar provisions to Section 60 of the Health and Social Care Act had been consolidated into Section 251 of the National Health Service Act 2006. The effect of the repeal of Section 60 by the National Health Service (Consequential Provisions) Act 2006 [273], did not affect the operation of the Regulations in the new legislation [274]

The Health Service (Control of Patient Information) Regulations consists of eight Regulations and a schedule of general provisions.

As the process for Regulation 5 approvals is well documented, with a procedure for applications being available on the Health Research Authority website [275], this will not be discussed in detail in this thesis.

With the exception of Regulation 5 approvals, however, not much academic discussion has taken place on the legal provisions contained within the Regulations, or how the Regulations could be applied. The below paragraphs intend to be an indication of the way in which the Regulations work. More in depth studies could add to this work in future and look at both the legal and social aspects of the Regulations in more detail.

5.2.2 Interpretation of the Regulations

Basic principles of statutory interpretation as stated in law will be applied in interpreting the Regulations in this chapter so as to explore the meaning.

5.2.3 Scope of the Regulations

As stated above, while there is nothing in the Act or the Regulations that specifies that the information is restricted to information generated by the NHS, in Lewis v. Secretary of State for Health and another [64], Mr Justice Foskett suggested that this appeared to be the case [246]. This statement was made in *obiter dictum* and not part of the *ratio decidendi* and therefore did not create a binding precedent. A binding precedent would only be created where the issue was central to the facts of the case, and the issue would be subject to a more detailed examination by the court [246]. It does however provide an indication that it is likely that powers contained within Section 251 and any Regulation created

pursuant to that section cannot apply to any information generated outside of the NHS [247].

Regulation 7(2) restricts the processing of confidential patient information under the Regulations to those persons who are either health professionals, or someone who owes an equivalent duty of confidentiality [276]. The reference to 'health professional' in this provision could be misleading. While it could be suggested that professionals have a professional duty to their patient's confidentiality. Where it comes to assessing the duty of confidence, the very form or even format of the information determines its sensitivity [33], and an actionable breach of confidence is not restricted to the processing body and extends to any person, even those acting of their own volition [87]. The second part of the Regulation therefore creates much wider possibilities for persons who may be able to process information. The limitations on the persons who can rely on the Regulations in each use case are explained in more detail in this chapter.

5.2.4 Overarching provisions

5.2.4.1 Setting aside the duty of confidence

The Health Service (Control of Patient Information) Regulations enable the setting aside of the duty of confidence by anyone relying on any specific provision contained therein, as enabled by the National Health Service Act [245]. Regulation 4 of the Health Service (Control of Patient Information) Regulations [264] provides:

> 'Anything done by a person that is necessary for the purpose of processing confidential patient information in accordance with these Regulations shall be taken to be lawfully done despite any obligation of confidence owed by that person in respect of it [265].'

The effect is clear from the wording of the Regulation, information does not cease to be confidential, but whatever is done in compliance with the Regulations is lawful.

There are three Regulations that enable the processing of personal information that may be subject to the duty of confidence, with other Regulations being applicable to those uses.

- Regulation 2 relates to the processing of confidential patient information for medical purposes for the diagnosis and treatment of neoplasia in prescribed circumstances.
- Regulation 3 relates to the processing of confidential patient information relating to communicable disease and other risks to public health in prescribed circumstances.
- Regulation 5 relates to the processing of confidential patient information in prescribed circumstances.

5.2.4.2 Regulation 7: restrictions and exclusions

Regulation 7 applies a number of conditions on any information processed in accordance with the Regulations.

Regulation 7(1) provides an overarching requirement that where information is processed under the Regulations:

> 'He shall not process that information more than is necessary to achieve the purposes for which he is permitted to process that information under these Regulations [277].'

To those who are aware of other aspects of information law, this general principle may seem familiar. At the time the Regulations were created, the Data Protection Act 1998 was in force. The third principle of that Act provides that:

> ‘Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed [278].’

The UK GDPR, which provides an equivalent principle provides that, the processing of personal data must be

> ‘…adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation) [279].’

Similar to the provision in the Data Protection Act 1998, the UK GDPR principle effectively states that information should be adequate for its purpose, relevant to the requirements of the process, and not be more than is necessary for the processing in hand. In other words, while the information used must be adequate to the purpose, no more information than is necessary to achieve the purposes of the processing should be processed to achieve that purpose.

Removing identifiers

Regulation 7(1)(a) states that:

> ‘So far as it is practical to do so, remove from the information any particulars which identify the person to whom it relates which are not required for the purposes for which it is, or is to be, processed [280].’

This suggests that particulars that may identify the person are removed where practical. It is conceivable therefore that the more obvious identifiers that identify a person such as name and address could be removed, whereas other identifiers such as NHS number could remain to undertake exercises such as data linkage.

The theme of reducing the amount of confidential information processed is also emphasised in Regulation 7(1)(d). It provides that when relying on the Regulations, the person relying on the Regulations must:

> '...review at intervals not exceeding 12 months the need to process confidential patient information and the extent to which it is practicable to reduce the confidential patient information which is being processed [281].'

Interestingly, these provisions are complimented by another principle in the UK GDPR, that information be kept in an identifiable form for no longer than is necessary [282]. Regulation 7 does not however say that the information must be anonymised.

Security

Two of the provisions under Article 7(1) are security focused. Regulation 7(1)(b) stipulates that when processing data under the Regulations a person relying on the Regulations must:

> 'Not allow any person access to that information other than a person who, by virtue of his contract of employment or otherwise, is involved in processing the information for one or more of those purposes and is aware of the purpose or purposes for which the information may be processed [283].'

Of note in this provision is the requirement to ensure that individuals engaged in the processing are aware of the purpose for which the information may be processed. While this appears to make it clear that when processing information that individuals must understand the precise nature of any processing, and any limitations, it could be suggested that the Regulations lack clarity in this regard.
Regulation 7(1)(c) provides that information must:

> '...ensure that appropriate technical and organisational measures are taken to prevent unauthorised processing of that information [284].'

Again, this is consistent with those provisions in the data protection legislation. At the time the Regulations were introduced, the seventh data protection principle of the Data Protection Act 1998, provided that:

> ‘Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data [285].’

The sixth principle of the UK GDPR provides a similar narrative. It provides that personal data must be:

> .‘...processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’) [286].’

Other provisions

Regulation 7(1)(e) creates a requirement in relation to being able to demonstrate compliance. It provides that:

> ‘On request by any person or body, make available information on the steps taken to comply with these Regulations [287]’.

It would appear from this provision that anyone can ask an organisation relying on the Regulations to demonstrate steps to comply with the Regulations. While the full set of provisions of The Freedom of Information Act 2000 did not come force until 2005 [288], this appears to have created a right of access to information relating to compliance with reliance on the Health Service (Control of Patient Information) Regulations 2002. While such information may now be subject to a request under the Section 1 of the Freedom of Information Act 2000, the requirement under the Regulations provides no process and no timescales for compliance with a request.

5.2.5 Regulation 2: medical purposes related to the diagnosis or treatment of neoplasia

5.2.5.1 Purpose

Regulation 2 relates specifically to the processing of confidential patient information relating to patients referred for diagnosis or the treatment of neoplasia [289], for medical purposes, despite any duty of confidence owed in respect of that information [265]. It can be noted that given it refers to neoplasia, this includes non-cancerous neoplasia. Given the Regulation refers to referral for diagnosis, obviously whether the neoplasia is cancerous or not will not be known at this stage,

Regulation 2(1) provides that:

> '…confidential patient information relating to patients referred for the diagnosis or treatment of neoplasia may be processed for medical purposes which comprise or include—
>
> (a) the surveillance and analysis of health and disease.
> (b) the monitoring and audit of health and health related care provision and outcomes where such provision has been made.
> (c) the planning and administration of the provision made for health and health related care.
> (d) medical research approved by research ethics committees.
> (e) the provision of information about individuals who have suffered from a particular disease or condition where—
> (i) that information supports an analysis of the risk of developing that disease or condition; and
> (ii) it is required for the counselling and support of a person who is concerned about the risk of developing that disease or condition [289].'

Given the observation that this Regulation has been largely unused within the current NHS, as identified below, it is not proposed to examine the provisions in Regulation 2(1) in any great detail. The provisions themselves are relatively self-explanatory in their regulatory form. It is however proposed that for completeness, some of the key features of the Regulation as a whole are identified,

The generality of this provision is of interest. While the confidential patient information must relate to cohort of patients referred for the diagnosis or treatment of neoplasia, the provision does not specify that the confidential patient information must relate to the neoplasia itself. This suggests that the analysis of se other health conditions that these patients may have would be lawful under this Regulation. For example, it may be useful to monitor the mortality of patients on chemotherapy where they contract certain conditions. The example is illustrative and does not intend to claim any authority in the medical use of cancer information.

5.2.5.2 Definition of 'processing' in Regulation 2

Regulation 2(2) provides a definition for processing. It states that:

> 'For the purposes of this Regulation, "processing" includes (in addition to the use, disclosure or obtaining of information) any operations, or set of operations, which are undertaken in order to establish or maintain databases for the purposes set out in paragraph (1), including—
>
> (a)the recording and holding of information.
> (b)the retrieval, alignment and combination of information.
> (c)the organisation, adaption or alteration of information.
> (d)the blocking, erasure and destruction of information [290].'

The term 'processing' exceeds the boundaries of what would be considered a breach of confidence in that it includes those data activities by which a breach of confidence would occur. There would only be a potential breach where there was a potential disclosure of information, as described previously in this thesis. This does not mean that the description of such processing activities is obsolete. It is suggested that the very fact that Regulation 2 is relied on in order to have a lawful basis to disclose information by one party to another, will engage the different processing activities set out in Regulation 2(2) in the regulatory regime. Where another lawful basis can be identified however, and Regulation 2 does not apply, the common law definitions will apply. Where the common

law does not apply, one use of such a provision in the use of information is to enable organisations to be able to demonstrate a clearer basis to use the data in demonstrating compliance with the data protection legislation.

5.2.5.3 Permissions to process

Regulation 2(3) provides that in order to process information relating to Welsh residents, individuals or classes of individuals doing the processing must have the approval of the Welsh Ministers [291] and have the authorisation off the person who holds that information [292]. The requirement that authorisation is sought from the persons holding the information raises an issue in the practical operation of the Regulation. Where bodies such as cancer registries are formed, without there being a requirement that NHS bodies submit data to the registry, it could be the case that some organisations decide that they will not submit information to the registry. Such a decision may be for no other reason than the costs of compiling the datasets, however this would threaten the integrity of the data in not having a full dataset. There is a provision in Regulation 2(4) that a notice can be issued to require that data be processed. This is set out in detail in the next heading.

5.2.5.4 Secretary of State Notices

Regulation 2(4) provides a mechanism by which the Welsh Ministers can require information to be processed under Regulation 2(1). It states:

> *'Where the Secretary of State considers that it is necessary in the public interest that confidential patient information is processed for a purpose specified in paragraph (1), he may give notice to any person who is approved and authorized under paragraph (3) to require that person to process that information for that purpose and any such notice may require that the information is processed forthwith or within such period as is specified in the notice* [293].'

As described above, Regulation 2(3) provides that in the absence of a notice of the type described in Regulation 2(4), in order to process information relating to Welsh residents, individuals or classes of individuals doing the processing must have the approval of the Welsh Ministers [291] and have the authorisation off the person who holds that information [292]. Where the Welsh Ministers consider 'that it is necessary in the public interest that confidential patient information is processed' under this Regulation, these party who holds the data may be required to make data available to another person. It can be noted that time periods can also be stipulated in the notice. With the exception of certain events that may require cohorts of data to be collected, it is difficult to see that the Welsh Ministers could ever justify that there is an ongoing public interest to provide data. It could even be suggested that where registries exist that they should have a statutory footing, or bodies are directed in some other way. In Wales, it is within the gift of the Welsh Ministers to direct Health Boards [294] and NHS Trusts [295] to exercise functions to contribute toward such a registry.

5.2.5.5 Reporting and audit

Regulation 2(5) creates an obligation for bodies that have been approved to process data under the Regulation, to provide the Welsh Ministers with information to assist in the investigation and audit of the processing that has taken place, and any annual review of the Regulations [296].

5.2.5.6 Regulation 7: application to Regulation 2

For completeness, it is important to reference the provisions of Regulation 7, as described above, as there is a requirement that the safeguards contained therein comply with this Regulation.

5.2.5.7 General commentary on Regulation 2

Many cancer registries in the United Kingdom collect data as part of a collaborative exercise between each of the participating home nations, with certain statutory bodies taking the lead.

In Wales, cancer registration and surveillance forms part of the statutory functions of Public Health Wales, with some additional activity relying on approvals under Regulation 5 [80]. The author is aware that similar arrangements exist in the NHS in England, but the complexities of the NHS in England are outside of the scope of this thesis.

While Regulation 2 is no longer relied upon by any cancer registry that currently operates, the provisions remain in force and could technically be relied upon.

5.2.6 Regulation 3: communicable disease and other risks to public health

5.2.6.1 Purpose

Regulation 3 specifically relates to the processing of confidential patient information that relates to communicable diseases and other risks to public health [297] despite any duty of confidence owed in respect of that information [265].

Regulation 3(1) provides that:

> '...confidential patient information may be processed with a view to—
> (a) diagnosing communicable diseases and other risks to public health.
> (b) recognising trends in such diseases and risks.
> (c) controlling and preventing the spread of such diseases and risks.
> (d) monitoring and managing—
> (i) outbreaks of communicable disease.

(ii) incidents of exposure to communicable disease.
(iii) the delivery, efficacy and safety of immunisation programmes.
(iv) adverse reactions to vaccines and medicines.
(v) risks of infection acquired from food or the environment (including water supplies).
(vi) the giving of information to persons about the diagnosis of communicable disease and risks of acquiring such disease [298]'

5.2.6.2 Definition of processing

With regard the definition of 'processing' Regulation 3(2) provides:

> 'For the purposes of this Regulation, "processing" includes any operations, or set of operations set out in Regulation 2(2) which are undertaken for the purposes set out in paragraph (1) [299].'

The definition of processing as applies to Regulation 2(1) in relation to neoplasia therefore applies to processing under Regulation 3(1).

In other words, the use of the word processing in Regulation 3(2) means:

> '…(in addition to the use, disclosure or obtaining of information) any operations, or set of operations, which are undertaken in order to establish or maintain databases for the purposes set out in paragraph (1), including—
> (a)the recording and holding of information.
> (b)the retrieval, alignment and combination of information.
> (c)the organisation, adaption or alteration of information.
> (d)the blocking, erasure and destruction of information [290].'

As the same definition of processing applies to this paragraph, the same observations can be made in relation to its applications. For example, the definition of 'processing' is much wider than those activities which would otherwise be considered a breach of confidence to include activities where no disclosure is made, and the information is used internally. As stated above, it could be suggested that such provisions could enable organisations to have clearer basis to use the data in demonstrating compliance with the data protection legislation, but the principles of the common law duty of confidence may not apply in some circumstances.

Where the common law does not apply, one use of such a provision in the use of information is to enable organisations to be able to demonstrate a clearer basis to use the data in demonstrating compliance with the data protection legislation.

5.2.6.3 Bodies who can rely on Regulation 3

Unlike Regulation 2(3) which specifies that information relating to neoplasia can only be processed by persons approved by the Welsh Ministers [291] and have the authorisation off the person who holds that information [292], Regulation 3(4) provides that processing can be carried out by 'persons employed or engaged for the purposes of the health service [217] and 'other persons employed or engaged by a Government Department or other public authority in communicable disease surveillance [218]'. This provides autonomy in using information.

It should be noted at this point that Section 251(4) of the National Health Service (Wales) Act provides that:

> 'Regulations under subsection (1) may not make provision requiring the processing of confidential patient information for any purpose if it would be reasonably practicable to achieve that purpose otherwise than pursuant to such Regulations, having regard to the cost of and the technology available for achieving that purpose [253].'

Given this clause, within the principles of statutory interpretation, it should be assumed that the application of the Regulations should be interpreted with this limitation in mind [300]. In other words that the Regulations apply to enable processing be carried out by 'persons employed or engaged for the purposes of the health service [217]' and 'other persons employed or engaged by a Government Department or other public authority in communicable disease surveillance [218]', unless it is 'reasonably practicable to achieve that purpose otherwise than pursuant to such Regulations, having regard to the cost of and the

technology available for achieving that purpose [253] in which case that lawful basis should apply.

5.2.6.4 The provisions

5.2.6.4.1 Diagnosing communicable diseases and other risks to public health

This includes any activity that relates to the diagnosis of communicable diseases. This could include the communication of information to other bodies where communicable identifying factors that could identify possible infections. The term 'other risks to public health' indicates that the provision relates to other diseases, infections or anything that could risk the spread of diseases, although there is no further guidance provided by the Regulations.

A key observation is the use of the word 'diagnosing', There is no definition to the word 'diagnosing' in the Regulations. The Parent Act provides that Regulation cannot solely apply to the healthcare of a patient [255]. As a principle of statutory interpretation, any Regulation produced pursuant to an Act of Parliament will usually be interpreted in light of provisions expressly excluded within the scope of the Act of Parliament [301]. Where such Regulations are expressly inconsistent with the Parent Act that a Regulation will be ultra vires [302]. In these circumstances however, it could be said that such a Regulation could be relied upon where there is one purpose and that does not relate solely to patient care, or a number of purposes that do not solely relate to patient care. This suggests therefore that the word 'diagnosis' must be used more broadly. An example of this could be targeting information to try and detect possible incidents of communicable disease to deal with public health issues, and not the actual one to one interaction by healthcare professionals to diagnose and treat that individual.

5.2.6.4.2 Recognising trends in such diseases and risks

The section contained in this provision is clear. This involves the use of information to identify patterns in disease, or in any risk. The use of the word 'risk', or how it can be applied is again not defined, and it could be interpreted as meaning any risk that relates to communicable diseases or to public health. This could include the direct risk of spreading the disease, the risk to how the service could be impacted by the spread of disease, or even a mortality risk presented by exposure to a specific public health situation. Again, no guidance or case law exists to provide any guidance on the implementation of this provision, and therefore the general application is assumed.

5.2.6.4.3 Controlling and preventing the spread of such diseases and risks

It could be assumed that this heading contains authority to process confidential patient information for a wide variety of purposes that relate to controlling the spread of diseases, preventing the spread of disease, and dealing with any risks associated with these activities. The definition of what is meant by the word 'risk' is not defined and it could be assumed in the widest definition of the word that this could relate to managing any risks that may present themselves when controlling or preventing the spread of disease. Again, no guidance or case law exists to provide any guidance on the implementation of this provision, and therefore the general application is assumed.

5.3.6.4.4 Monitoring and managing specific public health related activities

Article 3(1)(d) contains provisions that enable confidential patient information to be used to monitor and manage a number of activities set out in the Regulations.

For clarity, these are:

> ‘(i) outbreaks of communicable disease.
> (ii) incidents of exposure to communicable disease.
> (iii) the delivery, efficacy and safety of immunisation programmes.
> (iv) adverse reactions to vaccines and medicines.
> (v) risks of infection acquired from food or the environment (including water supplies).
> (vi) the giving of information to persons about the diagnosis of communicable disease and risks of acquiring such disease [303]’

There are numerous information exchanges that could come under these headings organisationally. Given there is no definition of managing and monitoring, the interpretation of such a provision could be argues as best defined with a wide interpretation of the types of activities, as a restrictive interpretation would defeat the object of the Regulations [304].

Information sharing mechanisms between those bodies provided in Regulation 3 would be lawful at common law where they are set up to monitor or manage outbreaks of communicable disease [305] and those incidents where individuals have been exposed to communicable disease [306]. It is conceivable that this will include diagnostic activity, such using details from tests for those diseases, and activities to identify those who may have been in contact with someone who has been found to have a communicable disease. An example of the latter relates to contact tracing as was widely known to have been utilised during the Covid-19 pandemic.

Information sharing for the purpose of monitoring and managing the delivery, efficacy and safety of immunisation programmes [307] would also be lawful at common law under the Regulations. Such activities that could be included under these Regulations include the type of information that may be required to comply with good practice, For example, ‘The Green Book’ [308] as relates to immunisations, provides a number of stipulations relating to the way immunisations are delivered,

including the priority levels by which immunisations are delivered in the event of a vaccination campaign. It may be necessary to obtain or disclose information on a wide variety of health conditions in order to identify those persons.

The Regulations enable bodies to lawfully disclose information for the purpose of monitoring and managing adverse reactions to vaccines and medicines [309]. More information under this head is currently provided in Chapter 9 of 'The Green Book', but this essentially means that where a body is included in the scope of the Regulations, information can lawfully be obtained or disclosed for this purpose.

The Regulations also include provision for the lawful sharing of confidential patient information for the purposes of monitoring and managing risks of infection acquired from food or the environment (including water supplies) [310]. It is conceivable that certain bodies or agencies within the scope of the Regulations may possess data in relation to persons who have had or are suspected to have an infection from food or water that they have consumed, or as an example, fumes they may have inhaled.

As an example of water contamination by legionella, certain types of poisoning from food or water sources could need to be monitored, and where there may be long term cases, those cases may need to be supported before their condition worsens.

The final situation by which confidential patient information may be disclosed relates to the monitoring and managing the giving of information to persons about the diagnosis of communicable disease and risks of acquiring such disease [311]. It could be suggested that this more specifically could be the type of communication that is targeted to certain people in society who may be more at risk from severe health issues if they contracted a communicable disease. Arguably there could be a situation where a body engaged in the health service for example is

responsible for making such a communication separately from any activity covered by any of the other Regulations. In the absence of another lawful basis, this Regulation could be used to utilise lawful disclosure of any information they need to satisfy their purpose as set out by other health bodies, or guidance such as 'The Green Book',

5.2.6.5 Secretary of State Notices

Similarly to Regulation 2(4), Regulation 3(4) provides a mechanism by which the Welsh Ministers can require information to be processed under Regulation 3(1). It states:

> 'Where the Secretary of State considers that it is necessary to process patient information for a purpose specified in paragraph (1), he may give notice to any body or person specified in paragraph (2) to require that person or body to process that information for that purpose and any such notice may require that the information is processed forthwith or within such period as is specified in the notice [312].'

This Regulation contains an error that has not been rectified. The 'persons or bodies' are specified in Regulation 3(3) and not 'Paragraph 2'. As a principle of statutory interpretation, regardless of the error, the courts are prepared to correct obvious mistakes in any instrument where obvious as to the correct meaning [313], and therefore this Regulation will be treated as correct for the purpose of this thesis.

It is suggested that the test is a subjective test in that the Welsh Ministers must consider that the processing of patient information is necessary for any of the processing set out in Regulation 3(1) [312]. This could include one or more purposes as the Welsh Ministers decide in the circumstances.

It is important to note that only those 'persons employed or engaged for the purposes of the health service' [217] and 'other persons employed or engaged by a Government Department or other public authority in communicable disease surveillance' [218] can be served a notice under this Regulation [312].

It can be noted that time periods can also be stipulated in the notice. With the exception of certain events that may require cohorts of data to be collected, as observed in relation to Regulation 2, it is difficult to see that the Welsh Ministers could ever justify that there is an ongoing public interest to provide data. It could be suggested that where registries exist that they should have a statutory footing, or bodies are directed in some other way. In Wales, it is within the gift of the Welsh Ministers to direct Health Boards [294] and NHS Trusts [295] to exercise functions to contribute toward such a registry.

5.2.6.6 Reporting and audit

As in the case of Regulation 2 [296], Regulation 3(5) creates an obligation for bodies that have been approved to process data under Regulation, to provide the Welsh Ministers with information to assist in the investigation and audit of the processing that has taken place, and any annual review of the Regulations [296].

5.2.6.7 Regulation 7: application to Regulation 3

For completeness, it is important to reference the provisions of Regulation 7, as described above, as there is a requirement that the safeguards contained therein comply with this Regulation.

5.2.7 Regulation 5:

Regulation 5 provides that:

> '(1) Subject to Regulation 7, confidential patient information may be processed for medical purposes in the circumstances set out in the Schedule to these Regulations provided that the processing has been approved—
> (a) in the case of medical research, by [the Health Research Authority], and
> (b) in any other case, by the Secretary of State.

> (2) The Health Research Authority may not give an approval under paragraph (1)(a) unless a research ethics committee has approved the medical research concerned.
> (3) The Health Research Authority shall put in place and operate a system for reviewing decisions it makes under paragraph (1)(a) [80].'

As stated above, the process described by Regulation 5 is a well-established process. The Schedule to the Regulations defines 'medical purposes' for the purposes of Regulation 5 [315]. While it is not proposed to discuss Regulation 5 or the Schedule to the Regulations in any detail in this thesis, it is interesting to note that the effect of the Parent Act means that its application is nevertheless limited. Section 251(4) of the National Health Service (Wales) Act provides that:

> 'Regulations under subsection (1) may not make provision requiring the processing of confidential patient information for any purpose if it would be reasonably practicable to achieve that purpose otherwise than pursuant to such Regulations, having regard to the cost of and the technology available for achieving that purpose [253].'

As established by the principle of statutory interpretation, the Regulations should be interpreted with this limitation in mind [300]. Operationally this means that Regulations under Section 251(4) cannot make provision where it is reasonably practicable to do so without the Regulation unless cost and technological reasons prevent this [253]. Therefore, where is practical to achieve the purpose without the Regulations, the Regulations will not apply [300].

In 2014, The Law Commission laid a report titled 'The Law Commission: Data Sharing between Public Bodies, A Scoping Report' [15] before parliament. The report identified that organisations often interpreted statutory functions in the narrowest way, inhibiting effective data sharing [316] and that information sharing was impeded because organisations who held the data questioned their statutory power and sought a more prescriptive legal gateway [317]. A researcher at some point in the future may be interested in exploring whether any of the approvals made under

Regulation 5 were granted in circumstances where the requesting body had a lawful basis to use the data anyway, such as in line with a statutory function. In such circumstances, despite any approval made by the Secretary of State, Regulation 5 could not apply in the circumstances [253]. Given the existing lawful basis, there would be no breach either.

Legal gateways, including statutory functions are explained in more detail in the next chapter.

5.3 Summary of Chapter 5

This chapter represents the first comprehensive academic text of the powers to the Secretary of State for Health in England and the Welsh Ministers under section 251 of the National Health Services Act 2006. The Chapter also describes in full the regulations currently in force.

> Section 251(1) of the National Health Services Act 2006 allows for the creation of Regulations requiring or regulating the processing of prescribed patient information for medical purposes in the interests of improving patient care, or in the public interest [251].'

Table 6 (below) summarised the definitions of 'Medical Purposes', 'Patient Information' and 'Confidential Patient Information' as applies to Section 251 of the National Health Services Act 2006

Medical Purposes	Providing preventative medicine [99]	Providing medical diagnosis [99]	Providing of care and treatment [99] (but not solely for this purpose [255])
	Medical research [99]	The management of health and social care services [99]	
	Informing about their physical or mental health or condition [100].	Informing about the diagnosis of their condition [100]	Informing about their care and treatment [100].

<table>
<tr><td rowspan="2">Patient Information</td><td>Physical or mental health [101].</td><td>Condition of an individual [101]</td><td rowspan="2">Derived, directly or indirectly, from such information, including where the individual cannot be identified [102]</td></tr>
<tr><td>Diagnosis of his condition [101].</td><td>His care or treatment [101].</td></tr>
<tr><td>Confidential Patient Information</td><td colspan="3">Where an individual can be identified:
From the information, or from that information and other information, which is in the possession of, or is likely to come into the possession of, the person processing that information, and
The information was obtained or created by a person who owed a duty of confidence to the individual [258].'</td></tr>
</table>

Table 6: Definitions contained in Section 251 of the NHS Act 2006

Functions under Section 251 in relation to Wales were transferred to the Welsh Ministers [249] along with the extant regulations [250]. Such Regulations can only apply to information created within the NHS [247]' and in social care [248]

Table 7 (below) summarises the scope of the provisions in the regulations.

Regulations created under s251 can contain provisions	**Regulations created under s 251 cannot contain provisions**
As relate to medical purposes in the interests of improving patient care or in the public interest [251].'	Where it's reasonably practical to process confidential information for any purpose without needing to rely on the regulations, having regard to the cost of and the technology available for achieving that purpose [253].
To set aside the common law duty [245],	
To create criminal offences including those on summary conviction punishable by a fine not exceeding level 5 on the standard scale [266].	
In relation to making prescribed communications of patient information to the person it relates to, the person it principally relates to (where there is more than one person) or to another person on behalf of that person [259].	For the sole provision of care or treatment [255].
Requiring or authorising disclosure of prescribed patient information of any description subject to conditions, including undertakings on how the information is processed [263].	

Table 7: Regulations Under s.251 - Scope of Provisions

The Welsh Ministers must:

- Consult parties affected when creating or amending Regulations [109].
- Review the Regulations within a month of the anniversary of the regulations to establish whether additional provisions need to be made [270] unless this is practical to do so by means [253].
- Vary or revoke the Regulations to the extent they consider necessary [270].

While Regulation must not provide for processing that is inconsistent with the data protection legislation [271], in the event that information was to be shared in line with regulations, there would be no breach of confidence [272].

6. Lawful disclosures - statutory functions

6.1 Legal gateways – general information

6.1.1 Introduction

In the previous chapter mechanisms for creating regulation under the provisions of Section 251 of the National Health Services Act 2006 was discussed. This chapter looks at the role of lawful disclosures where there is a legal gateway, including where an organisation needs the information to undertake a statutory function.

The first part of this chapter considers the various statutory gateways by which information subject to the duty of confidence can be disclosed lawfully. This is an overview of the general types of power that can be used in these circumstances, and a more in-depth analysis of how statutory gateways for the lawful use of information in Wales follows. For completeness, non-statutory powers as relate to the royal prerogative, and other crown powers are described, but these are out of scope of this thesis. It is conceivable that this could be considered in more detail in another scholarly research project as these powers have also never been specifically defined.

6.1.2 Statutory gateways

6.1.2.1 Express statutory gateways

An express statutory function can either expressly state that an organisation undertakes specific functions or exist in the form of powers that enable that organisation to require that another person supply it with data.

Organisations such as Digital Health and Care Wales have express statutory functions relating to information systems and data [450] and can therefore lawfully have data disclosed to fulfil those functions.

In the National Health Service in Wales, organisations created by the Welsh Ministers do not have any express statutory powers to require that confidential patient data is shared. In the England and Wales legal jurisdiction, however. NHS England who have responsibilities for data and digital functions in England have specific provisions in legislation that provide mechanisms for a number of activities, including provisions for the Secretary of State to direct it specifically to establish information systems [319], and powers to require and request provision of information [320].

6.1.2.2 Implied statutory gateways

The second type of statutory gateway are those information exchanges that are necessary in order for organisations to undertake broad statutory functions. Section 12(1) of the Interpretation Act 1978 provides:

> '(1) Where an Act confers a power or imposes a duty it is implied, unless the contrary intention appears, that the power may be exercised, or the duty is to be performed, from time to time as occasion requires [321].'

This provision relates to statutory provisions. This provision clarifies that, unless restricted by other provisions, powers may be implied based on the occasion in performing that duty. This suggests a broad approach to implying powers, and the courts take a view that such powers are interpreted in the broadest sense, to the extent that they do not conflict with any express power [113]

Section 12(2) of the Interpretation Act 1978 provides:

> '(2) Where an Act confers a power or imposes a duty on the holder of an office as such, it is implied, unless the contrary intention appears, that the power may be exercised, or the duty is to be performed, by the holder for the time being of the office [322].'

This is similar to the powers contained in Section 12(1) of the Interpretation Act 1978, with the exception that this provision applies to individuals while performing functions in office as relates to an Act of Parliament. An example of such a power is the Welsh Ministers powers to issue directions to a Special Health Authority under Section 23(1) of the National Health Services (Wales) Act 2006.

It is apparent that the common law also takes this approach in the interpretation of broader functions [323]. The case of Woolgar v. Chief Constable of the Sussex Police and another [323] related to the death of a patient in a nursing home. The matron had been arrested and interviewed by the police, but they were not charged with any offence. When the Central Council for Nursing, Midwifery and Health Visiting (the UKCC), the nursing regulatory body investigated the incident, the matron refused to consent to the disclosure of information. The police therefore indicated that it would review the tape-recorded interviews and decide whether to disclose the information based on the information contained on the tapes. She sought an injunction to prevent disclosure. It was held that where a public body was conducting an inquiry in line with its statutory powers, the police were entitled to disclose such information as would be relevant to those powers, although in any case, there was a clear public interest to disclose the information which outweighed the public interest in not disclosing the information [211].

An example as to how implied statutory gateways can operate is illustrated by the case of R (on the application of W and others) v. Secretary of State for Health (British Medical Association intervening) [106]. The case related to the charging of overseas visitors for NHS healthcare. While the information was not confidential information, the

principal of allowing information on implied statutory authority is the same. It had been argued that there was no express statutory authority to allow for the transfer of information from NHS organisations on the instruction of the Secretary of State for Health (England) to the Home Office. It was held however that the Secretary of State had implied powers under the National Health Service Act 2006, such as those that were in accordance with his general obligation under section 1(1) "to continue the promotion in England of a comprehensive health service designed to secure improvement (a) in the physical and mental health of the people of England, and (b) in the prevention, diagnosis and treatment of illness". And in connection with section 1(2): "to provide or secure the provision of services in accordance with this Act" [324]. The Act further recognised that that the Secretary of State had general powers under section 2(1) in "providing such services as he considers appropriate for the purpose of discharging any duty imposed on him by this Act," and that they may "do anything else which is calculated to facilitate, or is conducive or incidental to, the discharge of such a duty", including where this relates to ensuring any information necessary to fulfil that function is conveyed [254].

Equivalent legislation in Wales and how this can operate is discussed in the next part of this chapter.

6.1.2.3 Express gateways and implied terms

Where there are express clauses in Statutes permitting of requiring uses of information the courts are reluctant to apply any implied uses of information [325]. As a general principle therefore statutory power that could be inferred in broad terms cannot be used to override any express statutory provisions [106].

In the case of the express statutory provisions and processes in the Health and Social Care Act 2012 such as the power to require and request the provision of information [320], while non conflicting acts may be

acceptable where expressed elsewhere in Statute, any activity that conflicts with those provisions cannot be used to trump the provisions [106].

Another point of note is that a statutory body cannot argue that there is an implied statutory gateway where there is an express prohibition of disclosure [326]. Interestingly many prohibitions relate to specific documents and not necessarily the information that is created independent of them. For example, The Abortion Regulations 1991 [327], as created in compliance with the Abortion Act 1967, prohibit disclosure of the notice or any information provided to the Chief Medical Officer except in prescribed circumstances [328]. It stands to reason that a healthcare organisation that carried out the termination of pregnancy will have records both to support the persons healthcare, and to supply to the Chief Medical Officer. Disclosure of the certificate, or correspondence with the Chief Medical Officer could not in such circumstances be overridden by an implied statutory power. Although in the circumstances of the treatment, the general administrative records and health records would not apply to this restriction [326].

6.1.3 Powers deriving from Government

As described above, the powers described under this heading are stated for completeness and are out of scope of this thesis. Crown powers could be discussed at length; however, two powers are described in this section for awareness. These are the Royal Prerogative and RAM Powers.

6.1.3.1 Royal Prerogative Powers

The Royal Prerogative can be concisely defined as:

> ‘The remaining portion of the Crown's original authority, and is therefore, as already pointed out, the name for the residue of discretionary power left at any moment in the hands of the Crown,

> whether such power be in fact exercised by the King himself or by his Ministers [329].'

While it is a common law power [330] it carries a unique position in that the Royal Prerogative cannot be challenged in the courts [331] and therefore it effectively trumps the common law. The Crown cannot be bound by Statute unless the specific Act of Parliament removes the prerogative power without ambiguity [332], therefore Statute would need to expressly make provision to that affect.

If confidential patient information was required by prerogative power, it could not be obtained in breach of confidence, and this could not be subject to ordinary proceedings for such a claim [331]. Examples of the Royal Prerogative will include those that relate to the making of treaties, the defence of the realm, the prerogative of mercy, the grant of honours, the dissolution of Parliament and the appointment of ministers [333].

While technically, information held by a NHS organisation could be subject to prerogative powers in rare circumstances, this in unlikely given the types of power that these consist of. Prerogative powers are in any case out of scope of this thesis but mentioned for completeness as there may be a use of data that is required that falls within scope of the Royal Prerogative.

6.1.3.2 The Ram Doctrine

The suggestion that such a power could exist stems 2003 when legal advice received in 1945 was disclosed to parliament in answer to a Parliamentary question [334]. The effect of the doctrine is that any Minister for the Crown may, as an agent to the Crown, exercise powers that the Crown has unless Statute prohibits him or her from doing so [334]. Whether or not the doctrine has any effect in law however is untested, with the House of Lords' Constitution Committee doubting the effect of the advice and expressing the opinion that the doctrine is not a source of law [335] and does not accurately reflect the current law [336].

This however remains untested to its full extent. It could be that government may attempt to utilise the doctrine to justify disclosure of confidential information. This is however outside the scope of this thesis.

6.1.3.3 Information sharing and uncertainty of the law in practice

It is important to note at this stage that regardless of statutory or other gateways, some people are concerned with sharing information, even when they can do so lawfully.

In 2013, Dame Fiona Caldicott, National Data Guardian, undertook a review entitled 'Information: To share or not to share? The Information Governance Review' [337]. Recognising issues in the sharing of important information, she formulated a seventh Caldicott Principle as follows:

> 'The duty to share information can be as important as the duty to protect patient confidentiality [338].'

As discussed at the end of the previous chapter, In 2014, The Law Commission's report reported to parliament [15] that organisations often interpreted statutory functions in the narrowest way, inhibiting effective data sharing [316]. The Law Commission recognised that there are a lack of provisions requiring organisations to share [339] and this often impedes legitimate data sharing because organisations who held the data questioned their statutory power and sought a more prescriptive legal gateway [317].

There have been no legal developments in this area to date, and the author of this thesis is familiar with the same issues to those recognised by the Law Commission at the time of writing. In Wales, no guidance exists on the statutory gateways relating to organisational functions, and there is no other legal research in this area. The following paragraphs will therefore explore this in some detail.

6.2 The National Health Service in Wales

6.2.1 Introduction

To date, there is no comprehensive description as to how the NHS in Wales in constructed, or how statutory responsibilities can provide a legal gateway in order to process data that is subject to the common law duty of confidence in relation to these functions. This section of the thesis sets out the key considerations as relates to NHS organisations.

6.2.2 The general duty and powers of Welsh Ministers

The Welsh Ministers are responsible for the National Health Service in Wales. The legislation that is currently applicable to the establishment of the National Health Service in Wales is the National Health Service (Wales) Act 2006.

Section 1 of the National Health Service (Wales) Act 2006 states:

> '(1) The Welsh Ministers must continue the promotion in Wales of a comprehensive health service designed to secure improvement—
> (a) in the physical and mental health of the people of Wales, and
> (b) in the prevention, diagnosis and treatment of illness.
> (2) The Welsh Ministers must for that purpose provide or secure the provision of services in accordance with this Act [340].'

The Welsh Ministers have a general power in relation to fulfilling its functions as stated in Section 2 of the Act which provides:

> '(1) The Welsh Ministers may—
> (a) provide such services as they consider appropriate for the purpose of discharging any duty imposed on them by this Act, and
> (b) do anything else which is calculated to facilitate, or is conducive or incidental to, the discharge of such a duty.'

While there is no case law as relates to these sections of the operation of the National Health Service (Wales) Act 2006, there is case law that

explains similar provisions in the National Health Service Act 2006 as relates to England, as discussed above.

In R (W and others) v. Secretary of State for Health (British Medical Association intervening) [106] it was held however that the Secretary of State had implied powers to authorising the sharing of information under the National Health Service Act 2006, such as those that were in accordance with his general obligation under section 1(1) “to continue the promotion in England of a comprehensive health service designed to secure improvement (a) in the physical and mental health of the people of England, and (b) in the prevention, diagnosis and treatment of illness”. And in connection with section 1(2): “to provide or secure the provision of services in accordance with this Act” [324]. Furthermore the case recognised that the Secretary of State had general powers under section 2(1) in “providing such services as he considers appropriate for the purpose of discharging any duty imposed on him by this Act,” and that they may “do anything else which is calculated to facilitate, or is conducive or incidental to, the discharge of such a duty”, including where this relates to ensuring any information necessary to fulfil that function is conveyed [254].

It is therefore clear that the Welsh Ministers, in an identical set of provisions, also have implied powers to share information under the National Health Service (Wales) Act 2006 to “continue the promotion in Wales of a comprehensive health service designed to secure improvement in the physical and mental health of the people of Wales, and in the prevention, diagnosis and treatment of illness”, and to “provide or secure the provision of services in accordance with this Act [340].” In addition, The Welsh Ministers can share such information that they see fit in providing “such services as they consider appropriate for the purpose of discharging any duty imposed on them by this Act [341]”, and in the wider context ”do anything else which is calculated to facilitate, or is conducive or incidental to, the discharge of such a duty [342]”.

It is important to note that Section 1(2) of these provisions in the National Health Service (Wales) Act 2006 state that the Welsh Ministers must provide or secure the provision of services in accordance with the National Health Service (Wales) Act [343]. This suggests that services which are secured outside of the Act cannot rely on the implied power provided under section 1(2).

Furthermore, of the general power under Section 2(1) in providing such services as they consider appropriate in discharging a duty under the Act, it could be suggested that the general power under Section 1(2)(b) will be limited to those duties as set out in the Act.

6.2.3 The NHS structure in Wales: background context

In order to fulfil its functions, the Welsh Government can create a number of NHS organisations under the Act, namely National Health Service Trusts [344], Health Boards [345], and Special Health Authorities [346]. An Establishment Order can contain specific functions that relate to organisations, and these can confer functions that will inevitably involve the use and/or disclosure of health information.

Many NHS organisations in NHS Wales predate the National Health Service Wales Act 2006 and are therefore formed under different primary legislation. Any new organisations would be created in line with the National Health Service Wales Act 2006.

For contextual purposes the structure and organisation of the National Health Service in Wales is defined below. It should be noted however, that with the exception of the functions of Digital Health and Care Wales, which shall be used as an example as to how legislation can permit the disclosure of confidential personal data from those creating bodies, only certain key legislation is cited in relation to those bodies. The complexity of Regulation surrounding the functions of provided by organisations is outside of the scope of this thesis.

6.2.3.1 Local Health Boards

The Local Health Boards in Wales have a number of duties relating to the provision of functions that relate to the delivery of healthcare services in their area of Wales.

To understand the current NHS organisation structure, it is useful to understand the historic context of the organisations. In 2003, twenty-two Local Health Boards were established by Order [347], pursuant to powers contained in the National Health Service Act 1977 [348]. Twenty one of those Local Health Boards were abolished [349] in 2009 [350], leaving just Powys in its preexisting form [349]. In place of the twenty-one Local Health Boards, six new Local Health Boards were created to deliver health services in these areas [278].

In 2019, a boundary change resulted in the principal local government area of Bridgend transferring from Abertawe Bro Morgannwg University Local Health Board to Cwm Taf University Local Health Board [351]. They were renamed Cwm Taf Morgannwg University Local Health Board [352], and Swansea Bay University Local Health Board [353] to account for this change.

The Local Health Boards in Wales as of the 30th of October 2024 are therefore:

- Aneurin Bevan University Health Board [354]
- Betsi Cadwaladr University Health Board [354]
- Cardiff and Vale University Health Board [354]
- Cwm Taf Morgannwg University Health Board [354]
- Hywel Dda University Health Board [354]
- Swansea Bay University Health Board [354]
- Powys Local Health Board [347]

Except where referred to in the case study, this information is supplied to provide an understanding of the organisational roles and responsibilities in Wales, and it is not proposed to examine these powers in any more depth that currently specified.

6.2.3.2 NHS Trusts in Wales

There are currently three National Health Service Trusts in Wales.

The Velindre University National Health Service Trust was established by Order in 1993 [355] pursuant to powers conferred by the National Health Service and Community Care Act 1990 [356]. The Velindre University National Health Service Trust performs a number of functions, including the operation of Velindre Hospital, a hospital primarily operating for the management of cancer services [357], the operation of the Welsh Blood Service in Wales [358], the management and provision of prescribing and dispensing services [359], the NHS Wales Shared Services Partnership [360] and management of the Wales Infected Blood Support Scheme in accordance with directions issued by the Welsh Ministers [361].

The Welsh Ambulances Services National Health Service Trust was established by Order in 1998 [362] pursuant to powers conferred by the National Health Service and Community Care Act 1990 [356]. The main functions of the organisation include managing ambulance and associated transport services [363], and to manage other services in relation to care as are carried out in relation to these functions [364].

The Public Health Wales National Health Service Trust was established by Order in 2009 [365] pursuant to powers conferred by the National Health Service (Wales) Act 2006 [366]. Public Health Wales National Health Service Trust undertake a number of functions including, but not limited to health protection, health surveillance, healthcare improvement,

microbiological laboratory services [367], campaigns relating to health awareness and improvement [368], health research in certain circumstances [368], and certain screening services [369]. The Public Health Wales National Health Service Trust has provision in its Establishment Order to collect, analyse and disseminate information relating to the health of people of Wales, particular including cancer incidence, mortality and survival; and prevalence of congenital anomalies [370].

As with the section on Health Boards, except where these are referred to in the case study, this information is supplied to provide an understanding of the organisational roles and responsibilities in Wales, and it is not proposed to examine these powers in any more depth that currently specified.

6.2.3.3 Special Health Authorities

There are currently two Special Health Authorities in Wales, both established by Order pursuant to powers conferred by the National Health Services (Wales) Act 2006 [81], these are:

Health Education and Improvement Wales (HEIW) was established in 2017 [371] by Order [372]. The functions of HEIW relate to the planning, commissioning and delivery of education and training related to the provision of health services to both those already employed in the health service, or those who are considering becoming employed in the health service [373]

Digital Health and Care Wales was established in 2020 [374] by Order [375]. The functions of Digital Health and Care Wales include the design, management, development and delivery of digital platforms (article 3).

The functions of Digital Health and Care Wales include are provided in directions relating to:

'(a) the provision, design, management, development and delivery of digital platforms, systems and services; [376]
(b) the collection, analysis, use and dissemination of health service data; [377]
(c) the provision of advice and guidance to the Welsh Ministers about improving digital platforms, systems and services; [378]
(d) supporting bodies and persons identified in directions given by the Welsh Ministers to DHCW in relation to matters relevant to digital platforms, systems and services; [379]
(e) any other matter so as to secure the provision or promotion of services under the Act [380].'

Further detail on the operation of Digital Health and Care Wales and how data subject to the duty of confidence can be disclosed to it is set out below.

As with the section as relates to Health Boards and National Health Service Trusts, except where these are referred to in the case study, this information is supplied to provide an understanding of the organisational roles and responsibilities in Wales, and it is not proposed to examine these powers in any more depth that currently specified.

6.2.4 The NHS in Wales, and the use of Information subject to the duty of confidence in relation to statutory functions

Where an organisation has a lawful statutory function to undertake a particular task such as collecting or receiving data or disclosing data in its own right or on behalf of another body, the collection, use or disclosure of data in satisfying those functions will be lawful at common law [381].

In Smith Kline & French Laboratories Ltd v. Licensing Authority (Generics (UK) Ltd and another intervening) [381] therefore, it was found that when a licencing authority was exercising its general functions, the confidential information could be used for purposes that were consistent with those duties. The case particularly illustrates that where

organisations have responsibilities set out in law, that a wider view of the use of information is taken [381].

The generic functions of organisations can enable flexibility in undertaking statutory duties, although as noted at the end of the previous chapter, and earlier in this chapter, research by the Law Commission found that the narrow interpretation of statutory functions inhibits effective data sharing [316]. In having general functions, there can be a lack of provision in legislation that requires organisations to share [339], resulting organisations being reluctant to share and seeking more robust legal gateways [317].

It could be suggested that the rigid rules that are contained in guidance to ensure that the health service is protected from inadvertent unlawful disclosures could be partly to blame for the inhibition in sharing [10], with the courts commenting on this where a rare case is put before them [12]. It could further be suggested that more prescriptive statutory provisions as to how data is handled in other areas of the public services, such as those under the Health and Social Care Act 2012 in relation to NHS England, further complicate understanding of how statutory functions allow data sharing, given the more generic approach that can be applied where there are no specific statutory provisions [381].

6.2.5 Welsh Ministers powers to direct bodies established under the Act

6.2.5.1 The general position

The National Health Service Wales Act provides a mechanism for Welsh Ministers to Direct Local Health Boards [382], National Health Service Trusts [387], and Special Health Authorities [388] [389] in relation to its functions. Other powers to issue directions exist in this Act, in relation to specific services.

Where such a direction has been made, and functions are conferred on one or more NHS bodies, the collecting or receiving data in connection with this function will be lawful at common law [381]. It follows that specific data acquisitions could be included in such a direction where it is consistent with the general power of the Welsh Ministers under Section 1 and/or Section 2 of the National Health Service (Wales) Act 2006 as appropriate to the use case.

6.2.5.2 Directions conferred on Local Health Boards

There are many provisions by which directions can be given to Local Health Boards in the National Health Service Act 2006 alone, and the functions conferred by doing so may result in information being shared to satisfy those functions. This thesis however looks at more general functions that may be conferred under Section 12 and 13 of the National Health Service (Wales) Act 2006.

Section 12(1) of the National Health Service (Wales) Act 2006 provides that:

> '(1) The Welsh Ministers may direct a Local Health Board to exercise in relation to its area—
> (a) functions which were transferred to the National Assembly for Wales by the Health Authorities (Transfer of Functions, Staff, Property, Rights and Liabilities and Abolition) (Wales) Order 2003 (S.I. 2003/813 (W.98)),
> (b) such other of their functions relating to the health service as are specified in the direction [294].'

The Health Authorities (Transfer of Functions, Staff, Property, Rights and Liabilities and Abolition) (Wales) Order 2003 [383] abolished the Health Authorities in Wales [384] and transferred the functions to the National Assembly to Wales [385]. The extent of such functions is not within the scope of this thesis, but it should be noted that given the increased powers of the Welsh Parliament, particularly since the introduction of

legislation such as the Wales Act 2017, the reliance on such a provision may have superseded.

In any case, notwithstanding the provision in Section 12(1)(a) of the National Health Service (Wales) Act 2012, a more permissive clause contained in Section 12(3) which provides:

> "The Welsh Ministers may give directions to a Local Health Board about its exercise of any functions [386]".

This could apply to any function, including the Welsh Ministers responsibility to 'continue the promotion in Wales of a comprehensive health service designed to secure improvement in the physical and mental health of the people of Wales, and in the prevention, diagnosis and treatment of illness', and to 'provide or secure the provision of services in accordance with this Act' [340]. In addition, given the Welsh Ministers can do anything that they see fit in providing 'such services as they consider appropriate for the purpose of discharging any duty imposed on them by this Act' [341], and 'do anything else which is calculated to facilitate, or is conducive or incidental to, the discharge of such a duty' [342].

Section 13 of the National Health Service (Wales) Act 2006 relates to directions that relate to the functions of Local Health Boards [387] and the exercise of those functions by another body. The Welsh Ministers may direct that certain Local Health Board functions are undertaken by another Local Health Board [388], a Special Health Authority [389], or jointly with [390] NHS England [391], integrated care boards [392], NHS trusts [393], and other Local Health Boards [394].

Further discussion on directions that may be issued to Local Health Boards are out of scope of this thesis.

6.2.5.3 Directions conferred on National Health Service Trusts

Section 19 of the National Health Service (Wales) Act 2006 provides that:

> '(1) The Welsh Ministers may give directions to an NHS trust about its exercise of any functions.
> (2) The Welsh Ministers may not give directions under this section in respect of matters concerning xenotransplantation, surrogacy agreements, embryology or human genetics.
> (3) Nothing in provision made by or under this or any other Act affects the generality of subsection (1) [395].'

The operation of this section is straightforward. The Welsh Ministers may issue a direction of a very general nature as a vehicle to delivering functions. Directions could confer functions under Section 1(1) as relates to continuing the promotion of a comprehensive health service and in connection with section 1(2) in providing and securing the provision of services in accordance with the National Health Service (Wales) Act 2006 [324]. Functions could also be conferred pursuant to section 2(1) in providing such services considers appropriate in discharging duties or is conducive or incidental to, the discharge of such a duty [254]. The use of any information in accordance with functions could be implied, or alternatively explicit information sharing functions could be included in directions. The use of information subject to the duty of confidence would be lawful in these circumstances [254].

6.2.5.4 Directions conferred on Special Health Authorities

Section 23 of the National Health Service (Wales) Act 2006 provides that:

> '(1) The Welsh Ministers may give directions to a Special Health Authority about its exercise of any functions.
> (2) The Welsh Ministers may not give directions under this section in respect of matters concerning xenotransplantation, surrogacy agreements, embryology or human genetics.
> (3) Nothing in provision made by or under this or any other Act affects the generality of subsection (1) [396].'

As with National Health Service Trusts, the operation of this section is straightforward. The Welsh ministers can provide directions to a Statutory Health Authority without needing to create a statutory provision. As with National Health Service Trusts, the same provision as relate to the generality of provisions applies. Again, a direction could be used as a vehicle to deliver functions, including those functions under Section 1 and 2 of the National Health Service (Wales) Act 2006 [106].

6.2.5.5 Use of directions to direct a Special Health Authority to exercise the functions of the Welsh Ministers

Section 24 of the National Health Service (Wales) Act 2006 provides a mechanism for the Welsh Ministers to direct a Special Health Authority to undertake any of the functions of the Welsh Ministers as relates to the Health Service. It states that:

> '(1) The Welsh Ministers may direct a Special Health Authority to exercise any of the functions of the Welsh Ministers relating to the health service which are specified in the directions.
> (2) Subsection (1) does not apply to the functions of the Welsh Ministers in relation to pilot schemes.
> (3) The functions which may be specified in directions include functions under enactments relating to mental health and care homes [397].'

For completeness, it is important to note that the functions of the Welsh Ministers in relation to pilot schemes are mostly set out Schedule 6 of the National Health Service Act 2006 and are in relation to the procedural elements in approving and forming pilot schemes and this is, in any case out of scope of this thesis.

Sections 24(1) are however of interest. In enabling the Welsh Ministers to delegate responsibility to a Special Health Authority, this could potentially enable the Welsh Ministers direct that Special Health Authorities issue directions within his power. Alternatively, this could mean that any responsibilities of the Welsh Ministers with regard Regulations within their power, such as in approving the disclosure of patient information under

Regulation 5 of the Health Service (Control of Patient Information) Regulations 2002. There is case law that reinforces this approach. Where a general statutory power exists that this can be potentially limitless, providing the delegation is in scope of the area to which the provision relates [398], which in the case of Section 24(1) is clearly the health service.

In Dory v. Sheffield Health Authority [399] this is referred to as 'devolution' of the power [400]. Where powers are explicitly granted in an appropriate instrument to further devolve powers, this has been referred to as a 'chain of devolution [401]'. The effect of devolution is that a public body will effectively act as a government department in exercising those functions [402].

Only where there is doubt as to whether a minister can delegate authority will the courts interpret provisions narrowly [403]. In other circumstances, they will accept such provisions, despite sometimes expressing concern at the broad nature of such clauses [403].

6.2.5.6 Formality of directions under the National Health Service (Wales) Act 2006

There are different types of directions that can be issued under the National Health Service Act 2006. This detail under this heading is, however, only concerned with directions discussed above in relation to:

- Directions issued by the Welsh Ministers under Section 12 as relate to the functions that may be conferred on Health Boards.
- Directions issued by the Welsh Ministers under Section 13 as relate to functions conferred on the Health Boards
- Directions issued by the Welsh Ministers under Section 19 as relate to functions conferred on the NHS Trusts in Wales
- Directions issued by the Welsh Ministers under Section 23 as relate to functions conferred on Special Health Authorities

- Directions issued by the Welsh Ministers under Section 24 as relate to Special Health Authorities exercising the functions of the Welsh Ministers.

Section 204(3) of the National Health Service (Wales) Act 2006 provides that:

> 'A direction under this Act by the Welsh Ministers must be given—
> (a) (subject to paragraphs (b) and (c)), by an instrument in writing,
> (b)in the case of a direction under—
> (i)section 12(1)(a),
> (ii)section 24 about a function under section 4, 145 or 146, or
> (iii)section 147(2),by Regulations,
> (c)in the case of—
> (i)any other direction under section 12,
> (ii)any other direction under section 24, or
> (iii)a direction under section 13, 19, 23, 45, 52(4), 60 or 66(4),by Regulations or an instrument in writing [404].'

The general position therefore that, subject to the other provisions listed, that a Direction must be made by an instrument in writing [405]. In the absence of more prescriptive requirements in the legislation, this may just be a letter or other document from the Welsh Ministers directing the appropriate authority that they are directed to perform certain tasks.

Under Section 204(3)(b) however, there is a requirement that such directions need to be included in Regulations in certain cases. For completeness, the full set of provisions are explained. These are:

- Directions under Section 12(1)(a) as relate to those functions that transferred to the national Assembly for Wales on abolition of the old health authorities [406].
- Directions under section 24 on Special Health Authorities where these relate to:
  - High Security Psychiatric Services where these are created under section 4 of the National Health Service (Wales) Act 2006 [407]

- The requirement that a NHS body, statutory health body, service provider or NHS contractor produce documents to the Welsh Ministers as per Section 145 and 146 of the National Health Service (Wales) Act 2006 [407]
- Directing Special Health Authorities that senior officers of the Authority exercise the delegated functions on behalf of the Special Health Authority in accordance with Section 147(2) [407].

Section 204(3)(c) of the National Health Service (Wales) Act 2006 provides that all other directions under 12, and 24, and directions under Sections 13, 19, 23 may be made by Regulations or an instrument in writing. Arguably, while making a direction by an instrument in writing may appear the easier option, this section is permissive of the incorporation of a direction in Regulations if required, even if this is not mandatory. It could be submitted that where any Regulations are produced for particular functions, this could prove useful in consolidating provisions into one document to provide clarity on functions.

6.2.5.7 Amending or revoking directions

Section 204(1) of the National Health Service (Wales) Act 2006 provides:

> 'Where under or by virtue of any provision of this Act—
> (a)an Order may be made, or
> (b)directions may be given
> that provision includes power to vary or revoke the Order or directions by subsequent Order or by subsequent directions [408].'

This section of the Act therefore permits variation or revocation of any direction issued under the National Health Service (Wales) Act 2006. By a variation, such an instrument may change the purposes contained within the direction, or in the case of more detailed directions this could change a process by which an activity takes place. Revoking directions would have the inevitable effect of ceasing those functions that have been conferred on organisations.

6.2.5.8 Conferring functions already exercised by other bodies

Section 31 of the National Health Service (Wales) Act 2006 provides that where functions subject to the directions are currently exercised by any person or body, they should not be precluded from the Direction, except where specifically prescribed [409]. As an example of how this would operate, it could be that a Special Health Authority is being directed under Section 23 of the National Health Service (Wales) Act 2006 being directed to undertake a Local Health Board function, such as managing appointments for immunisations. The Local Health Board must in such circumstances not precluded from such a direction to the Special Health Authority.

6.2.6 Statutory disclosures to NHS England to Undertake a function on behalf of Wales

6.2.6.1 Scope

For the purpose of this thesis, the mechanisms under the Health and Social Care Act 2012 by which information subject to the duty of confidence can be transferred to NHS England in order for services to be conducted by them on behalf of NHS Wales organisations is in scope. The operation of the arrangements in practice is out of scope of this thesis.

6.2.6.2 'Section 255 requests'

Section 255(1) of the Health and Social Care Act 2012 creates a statutory mechanism by which any person, including an authority exercising functions devolved authority, can request that NHS England establish and operate a system for the collection or analysis of information on their behalf [410].

NHS bodies in Wales can therefore request that NHS England operates such an information system, providing that it is *necessary* or *expedient* for the exercise of functions, or carrying out of activities, in connection with the provision of health care or adult social care [411]. Prior to submitting a request to NHS England, there is a requirement that NHS England is consulted on the proposed request [412].

Devolved authorities cannot require that NHS England undertake to undertake functions[9], and as such any work undertaken is done with the discretion of NHS England. NHS England are obliged to ensure that in exercising that discretion [413], to consider whether complying with the request would unreasonably interfere with its functions [414], and may take into account the extent to which the requestor has considered the code of practice prepared and published by NHS England in accordance with the requirements of the legislation [415] or any advice and guidance given by NHS England in connection with the request [416].

Where the Section 255 request is to establish and create a system to collect information that either identifies any individual to whom that information relates and they are not a provider of health care or adult social care [417] or enables their identity to be ascertained [418], the request is known as a confidential collection request. It should be noted however that the word 'confidential' in this regard does not have the same meaning as in the common law duty of confidence, although that information may include information that is subject to the duty of confidence.

From the perspective of a request from a public authority in Wales, confidential collection requests can only be made where the person making the request can require the information to be disclosed to them or NHS England [419], or in any other case, where the information can be lawfully disclosed to NHS England or the requestor themselves [420].

[9] Those mandatory requests are set out in the legislation. See for example Health and Social Care Act 2012, Section 255(4)

6.2.6.3 Dissemination

It is not proposed to consider the statutory powers of NHS England in relation to dissemination of information in detail, but it is useful to be aware that such powers exist. Section 261 of the Health and Social Care Act 2012 contains provisions by which NHS England may disseminate information on behalf of another person, such as a NHS Wales organisation.

NHS England can use its discretion to publish any information it receives in complying with a s255 request [421] in certain circumstances [422] where the dissemination is for purposes connected with the provision of health care or adult social care [423], or the promotion of health [424]. It can also use its discretion in making information available to any person to who the information could have been lawfully disclosed to by the person supplying NHS England [425],

The person making the section 255 request may request that NHS England do not disseminate information in line with its statutory functions [426], however this is merely a request not to publish [427].

The person making the section 255 request can also request that NHS England disseminate information in line with its discretionary power [428] or in line with any other power of dissemination it may have at the current time or in the future [429]. In such circumstances, a request may stipulate the persons to who the information is to be disseminated, and the form, manner and timing of dissemination [427].

6.2.6.4 Publication

The general position is that NHS England must publish any information that it collects when it complies with a request under section 255 [430].

There are safeguards such as where the information identifies individuals [431], or where the data does not comply with specific data standards [432]. This and other provisions in this regard are outside of the scope of this thesis.

6.2.7 Impact of the Human Rights Act 1998

The Human Rights Act 1998 relates to 'Convention Rights', defined as those rights set out in the Convention for the Protection of Human Rights and Fundamental Freedoms, agreed by the Council of Europe at Rome on 4th November 1950 [433]. It is not proposed to consider the application of the Human Rights Act 1998 in any detail in this thesis. The application of the Human Rights Act 1998 on the functions of a Public Authority is out of scope.

For completeness however, it is important to acknowledge that when exercising statutory powers, as a general principle, if a Public Authority acts in a way that is incompatible with a Convention Right [434] or omits to act in a way that is compatible with a convention right [435], they may be acting unlawfully subject to the provisions of the Human Rights Act 1998.

For the purposes of the Human Rights Act 1998, any person who undertakes functions of a public nature [436] is subject to the Act. This definition is far ranging, extending beyond statutory bodies to those undertaking functions of a public nature. Where a person undertakes tasks of a private nature, they will not be subject to the obligations of the Human Rights Act 1998 [437]. The Human Rights Act provides little guidance, but it is clear that functions will very much depend on the types of arrangements in place [438]. For example, a General Medical Practice operating in providing NHS services in line with the statutory General Medical Service Contract [439] will clearly be a Public Authority, however a private contractor who has via a procurement process been

selected by a public authority to undertake work will not be acting as a public authority [438].

Despite any statutory gateway, consideration of the rights and freedoms protected by the Human Rights Act 1998 is therefore essential. These include Article 8: Right to respect for private and family life, and Article 10: Freedom of Expression. These rights are often subject to a balancing act to determine whether the individual's right to privacy is outweighed by the right of freedom of expression of the other person [35]. The scope of this exercise is out of scope of this thesis.

One final point of note is that the protections of the Human Rights Act 1998 may not be absolute, and exceptions are included within the terms of certain articles. For example, Article 8(2) provides that:

> 'There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others [440].'

It can also be noted Section 6(2) of the Human Rights Act 1998 provides that a Public Authority will not have been acting unlawfully if:

> '(a) as the result of one or more provisions of primary legislation, the authority could not have acted differently; or
> (b) in the case of one or more provisions of, or made under, primary legislation which cannot be read or given effect in a way which is compatible with the Convention rights, the authority was acting so as to give effect to or enforce those provisions [441].'

6.3 Summary of Chapter 6

The chapter provides an academic text systemising and explaining comprehensively existing knowledge in relation to the public law, and how this enables data to be shared or obtained lawfully where there is a duty of confidence. The chapter also represents the first comprehensive academic text of the basic statutory functions in place in NHS Wales and how these can enable data to be shared or obtained lawfully by NHS statutory bodies where there is a duty of confidence.

Data Sharing and Statutory Functions

Information subject to the duty of confidence can be shared lawfully in order to fulfil:

- An express statutory function. Examples of such functions include the functions of Digital Health and Care Wales in relation to data and digital systems [1] [2]
- An implied statutory function both conferred by Act of Parliament [3] or by secondary legislation (including directions) [5] to the extent that they do not conflict with any express power [4]

At common law:

- The courts accept that Ministers duties and powers can be interpreted in the widest form, and this will include requiring disclosure of information to fulfil a duty conferred on them [8].
- Organisations can treat their own broad statutory functions in their widest form, and can lawfully obtain or disclose data to fulfil those functions [6] to the extent that they do not conflict with any express power [4]

The courts are unlikely to imply functions where:

- Where an organisation is subject to prescriptive functions and those functions that may be implied conflict with these functions [11]

- Where those functions that may be implied conflict with another express statutory provision [8].
- There is an express prohibition of disclosure [13] (e.g. To receive a copy of the notice provided to the Chief Medical Officer as prohibited by The Abortion Regulations 1991 [14])

On reviewing the operation of statutory functions in practice, The Law Commission produced a report [26] that recognised that:

- Organisations often interpreted statutory functions in the narrowest way, inhibiting effective data sharing [27].
- There are a lack of provisions requiring organisations to share [28] and this often impedes legitimate data sharing because organisations who held the data questioned their statutory power and sought a more prescriptive legal gateway [29].

'Information: To share or not to share? The Information Governance Review' [24] recognised these issues in the NHS and created a seventh Caldicott Principle that specifies that 'The duty to share information can be as important as the duty to protect patient confidentiality [25].'

The structure of NHS Wales and statutory powers

The Welsh Ministers:

- Are responsible for the promotion in Wales of a comprehensive health service designed to secure improvement in the physical and mental health of the people of Wales, and in the prevention, diagnosis and treatment of illness [30].'
- Have a general power to provide such services as they consider appropriate for the purpose of discharging any duty imposed on them and do anything else which is calculated to facilitate, or is conducive or incidental to, the discharge of their duty.

The duties imposed on Welsh ministers creates an implied power to authorise the sharing of information in order to achieve these aims [10].

Structure of NHS Wales

The Welsh Government can create a number of NHS organisations including:

- National Health Service Trusts [34]
- Local Health Boards [35], and
- Special Health Authorities [36].

The current Local Health Boards in Wales are

- Aneurin Bevan University Health Board [45]
- Betsi Cadwaladr University Health Board [45]
- Cardiff and Vale University Health Board [45]
- Cwm Taf Morgannwg University Health Board [45]
- Hywel Dda University Health Board [45]
- Swansea Bay University Health Board [45]
- Powys Local Health Board [37]

Local Health Boards can be directed by the Welsh Ministers to undertake specific functions in relation to their geographic area [77]:

- By creating regulations, where these relate to the functions that were transferred from the Health Authorities to the Welsh Ministers [101]
- By regulation or an instrument in writing [27] where these relate to any other function [81].

Welsh Ministers have the power to vary or revoke directions [103].

The current National Health Service Trusts in Wales are:

- The Velindre University National Health Service Trust [47].
- The Welsh Ambulances Services National Health Service Trust [53]
- Public Health Wales National Health Service Trust [56]

The Welsh Ministers can direct National Health Service Trusts to undertake any functions [32]:

- On any matter except xenotransplantation, surrogacy agreements, embryology or human genetics [33].
- By any instrument (e.g. a letter) or regulation [27]

Directions can be generic in nature [34] . The Welsh Ministers have the power to vary or revoke directions [103].

The two Special Health Authorities in Wales are:

- Health Education and Improvement Wales (HEIW) [63]
- Digital Health and Care Wales [66]

The Welsh Ministers can directions a Special Health Authority to undertake any functions [35]:

- On any matter except xenotransplantation, surrogacy agreements, embryology or human genetics [37].
- By any instrument (e.g. a letter) or regulation [27].

Directions can be generic in nature [36] and can take the form of either a regulation or an instrument in writing

The Welsh Ministers may also direct a Special Health Authority to exercise any of the functions of the Welsh Ministers relating to the health service [39]. In such circumstances:

- Directions can in most circumstances take the form of either a regulation or an instrument in writing [27], however there are exceptions whereby certain provisions may only be made by regulation [102].
- Where a body is directed to perform the functions of Ministers of the Crown, this is referred to as ‘devolution’ of power [95] and the Authority acts as a government department when exercising those functions [97].

Welsh Ministers have the power to vary or revoke directions [103].

The effect of statutory functions

Where each of these bodies has a statutory function to undertake a particular task the sharing of information with that body to undertake that task will be lawful at common law [73].

Lawful use of data by NHS England - 'Section 255 requests'

Section 255 of the Health and Social Care Act 2012:

- Creates a statutory mechanism by which any person can request that NHS England establish and operate a system for the collection or analysis of information on their behalf [105].
- It must be necessary or expedient for the exercise of functions, or carrying out of activities, in connection with the provision of health care or adult social care [106].
- NHS England is consulted on the proposed request before the request is made [107].
- Non mandatory requests, such as those undertake by devolved authorities are only accepted at the discretion of NHS England [108], who must consider:
- Whether the request would unreasonably interfere with its functions [109]; and
- May take into account the extent to which the requestor has considered NHS England's Code of Practice [110]; or
- Any advice and guidance given by NHS England in connection with the request [111].

'A Confidential Collection Request' is the term used to describe a request where the information collected identifies any individual that is not providing health or adult social care (i.e. a service user) [112] or enables their identity to be ascertained [113]. Public Authorities in Wales can only make a confidential collection request where:

- Where the person making the request can require the information to be disclosed to them or NHS England [114]
- Where the information can be lawfully disclosed to NHS England or the requestor [115].

NHS England can use its discretion:

- To publish any information it receives in complying with a s255 request [116] in certain circumstances [117] where he dissemination is for purposes connected with:
    - The provision of health care or adult social care [118], or
    - The promotion of health [119].
- To make information available to any person to who the information could have been lawfully disclosed to by the person supplying NHS England [120],

Any person making a section 255 request may request that NHS England:

- Disseminate information in line with its discretionary power [123] or any other power of dissemination it has or may have [124] stipulating the recipients manner and timing of the dissemination [122].
- Do not disseminate information in line with its statutory functions [121] as relate to publication [122].

The Human Rights Act 1998

The Human Rights Act:

- Applies to bodies undertaking tasks of a public nature regardless of whether these are bodies created by statute [131]
- Does not apply to bodies undertaking tasks of a private nature [132].
- Whether a function is public or private will depend on the types of arrangements in place [133].

When exercising statutory powers, a body may be acting unlawfully if they:

- Act in a way that is incompatible with a Convention Right [129] or
- Omits to act in a way that is compatible with a convention right [130]

Insofar as the Duty of Confidence is concerned, two human rights usually apply, namely:

- Article 8: Right to respect for private and family life, and
- Article 10: Freedom of Expression.

Rights are subject to a balancing act to determine whether the individual's right to privacy is outweighed by the right of freedom of expression of the other person [135].

A Public Authority is not acting unlawfully where:

- They act in accordance with the law and is necessary in a democratic society in the interests of:
    - National security, public safety or the economic well-being of the country,
    - For the prevention of disorder or crime,
    - For the protection of health or morals, or
    - For the protection of the rights and freedoms of others [136].'
- Primary legislation prevents them from acting in any other way [28] or
- The Public Authority is acting in accordance with secondary legislation and that the provisions of that legislation cannot be interpreted in a way which is compatible with the Convention rights [29]

7. Central digital functions in Wales: A case study

7.1 Digital Health and Care Wales

7.1.1 Introduction

This section expands on the information contained in chapters 5 and 6 to explain how data can be lawfully disclosed to Digital Health and Care Wales as the central digital and data body in Wales. It is not proposed to analyse the historical origins of organisations in any more detail than is relevant to those provisions that are in place.

7.1.2 Establishment of Digital Health and Care Wales

7.1.2.1 The Establishment Order

In accordance with the powers granted to Welsh Ministers by Section 22 of the National Health Service (Wales) Act 2006, the Welsh Ministers, by Order, created a Special Health Authority known as Digital Health and Care Wales [375]. The new body was established on the 30th of December 2020 [442]. The staff, property and liabilities of the NHS Wales Informatics Service, a department of Velindre NHS Trust, termed a 'hosted organisation', but in reality, not established by any instrument were transferred by a separate instrument with effect of the 1st of April 2021. The staff from this department were transferred on the 1st of April 2021 [443].

Digital Health and Care Wales have a number of core functions set out in its Establishment Order.

Article 3 of the Establishment Order states:

> 'DHCW is to exercise such functions as the Welsh Ministers may direct in connection with—
> (a) The provision, design, management, development and delivery of digital platforms, systems and services.
> (b) The collection, analysis, use and dissemination of health service data.
> (c) The provision of advice and guidance to the Welsh Ministers about improving digital platforms, systems and services.
> (d) Supporting bodies and persons identified in directions given by the Welsh Ministers to DHCW in relation to matters relevant to digital platforms, systems and services.
> (e) Any other matter so as to secure the provision or promotion of services under the Act [444].'

Interestingly, as with the Establishment Order for Health Education Improvement Wales, the Order doesn't specify that the list of activities in Article 3 are functions of Digital Health and Care Wales. It states that the list of activities are the types of function that the Welsh Ministers may direct it to undertake [444].

As this is in the Establishment Order however, it could be inferred that these are functional responsibilities of the organisation on the day it was established [254]. In any case the functions of an organisation are not limited by the text of the Establishment Order and the Welsh Ministers can direct Digital Health and Care Wales as to the exercise of any of any of its functions [445], or those functions of the Welsh Ministers relating to the health service [446].

7.1.2.2 Digital Health and Care Wales: directions

The first two directions issued to Digital Health and Care Wales provide an interesting backdrop to the core functions of the organisation.

The Digital Health and Care Wales Directions 2020 [447] provides some dialogue on the preparatory functions that needed to be in place on the establishment of the organisation [448].

The second set of directions that were issued to Digital Health and Care Wales were The Digital Health and Care Wales (No.2) Directions 2021 [449]. These outline the functions of Digital Health and Care Wales as a Special Health Authority.

Paragraph 3 of The Digital Health and Care Wales (No.2) Directions 2021 provide directions to Digital Health and Care Wales as follows:

> '(1) In order to secure the provision or promotion of effective digital platforms, systems and services the Welsh Ministers direct DHCW to—
> (a) design, develop and deliver, either directly or by entering into arrangements with others, digital platforms, systems and services.
> (b) support and assist others in the design, development and delivery of digital platforms, systems and services.
> (c) support the development and implementation of common standards for digital platforms, systems and services.
> (d) advise and assist the Welsh Ministers in relation to the security of digital platforms, systems, services and health service data.
> (e) support the development of the digital workforce through education, training and promotion of professional standards.
>
> (2) DHCW may do anything which is calculated to facilitate, or is conducive or incidental to, the discharge of its functions [450].

Paragraph 2 of The Digital Health and Care Wales (No.2) Directions 2021 defines "digital platforms, systems and services" as meaning:

> '...hardware, software and other arrangements for the digital collection, storage, processing, analysis, use and dissemination of health service data [451].'

"Health service data" is further defined as meaning:

> '...data processed for or in connection with the provision or promotion of services under the Act [451].'

Paragraph 2 also specifies that references to 'the Act' refers to the National Health Service (Wales) Act 2006 [451].

For completeness, it is also worth noting that the term '*digital workforce' refers to:*

> '…those who are employed or engaged, or considering becoming employed or engaged, in the design, development, or delivery of digital platforms, systems and services [451].'

The first observation that can be made is how general the directions are for the functions to be undertaken Digital Health and Care Wales. Directions made under Section 254 of the Health and Social Care Act are much more detailed and relate to separate services[10]. The Health and Social Care Act 2012 as applies to NHS England is very specific that a description of the service must be included in the Direction [452]. There are also other procedural provisions contained within the Act [453].

Section 23(1) of the Nation Health Service (Wales) Act 2006 however simply provides in Section 23(1) that:

> 'The Welsh Ministers may give directions to a Special Health Authority about its exercise of any functions [454].'

Unlike the directions that are made to NHS England in relation to digital services and the use of data under Section 254 of the Health and Social Care Act that require directions in a granular form [452] with certain procedural requirements to be followed [453], Section 23(3) of the National Health Service (Wales) Act 2006 provides:

> 'Nothing in provision made by or under this or any other Act affects the generality of subsection (1) [455].'

This is a significantly different approach, and it could be suggested that this provides more flexibility and less bureaucracy in ensuring data is

[10] See for example an A to Z of Secretary of State Directions listed on the NHS England Website: https://digital.nhs.uk/about-nhs-digital/corporate-information-and-documents/directions-and-data-provision-notices/secretary-of-state-directions/secretary-of-state-directions-a-z last visited 5/10/2024

made available to respond to the needs of the health service in a timely manner.

Paragraph 3(2) of The Digital Health and Care Wales (No.2) Directions 2021 further emphasised that the wide scope of functions to be undertaken by Digital Health and Care Wales in stating:

> 'DHCW may do anything which is calculated to facilitate, or is conducive or incidental to, the discharge of its functions [456].'

This provides significant autonomy in relation to the way Digital Health and Care Wales can conduct itself in performing these functions. The general nature of this autonomy permitted by the Parent Act [455].

7.1.3 The duty of confidence and the functions of Digital Health and Care Wales

7.1.3.1 The basics

The purpose of defining the operation of the National Health Service in Wales, and particularly Digital Health and Care Wales as a central body for digital functions is to clarify how the bodies operate, and to demonstrate the lawfulness of data sharing despite the duty of confidence.

It has already been established that Digital Health and Care Wales has a very broad set of functions, and a significant amount of autonomy in the way that the functions are exercised. Where an organisation is acting in line with its general functions, even where data is not referenced, that organisation can lawfully have information disclosed to it [381].

7.1.3.2 Functions and the duty of confidence

The author of this thesis is employed by Digital Health and Care Wales in the field of information governance and has an in-depth professional knowledge of the digital platforms, systems and services provided by the organisation. Some of the information that follows is not published in the level of detail provided and therefore no reference sources can be included in this regard to provide any person reading with further information. More general information is however provided on the website of Digital Health and Care Wales in a form that can be understood by the public[11].

The two functions that are to be considered in this case study are the role of Digital Health and Care Wales in:

- Creating information systems; and
- Collecting and disseminating data.

Other functions undertaken by Digital Health and Care Wales, while forming part of its purpose, and where processing data that is subject to the duty of confidence, will not be considered. A separate and detailed study of these functions would be useful as a separate exercise.

Other regulatory or statutory considerations are also out of scope, and the common law duty of confidence is the only element of the law that will be considered in this section.

It could be argued that there is artificial to distinguish between the creation of information systems and the collection and dissemination of data and therefore the provisions are considered on the whole.

[11] The Digital Health and Care Wales website is available at: https://dhcw.nhs.wales

Both the collection of data in systems that hold records of the patients interactions with the health service and those collections of specific datasets in DHCW have a clear basis as a function of Digital Health and Care Wales under Paragraph 3 of The Digital Health and Care Wales (No.2) Directions 2021 [448]. The systems that are designed and developed to provide front line care to patients throughout Wales, also have a clear basis under the same directions.

Paragraph 3(1)(a) provides that, "In order to secure the provision or promotion of effective digital platforms, systems and services [227]" the Welsh Ministers direct Digital Health and Care Wales to:

> 'Design, develop and deliver, either directly or by entering into arrangements with others, digital platforms, systems and services [457].'

Bearing in mind the definition of digital platforms, systems and services in paragraph 2, this is not limited to the work that Digital Health and Care Wales undertakes. The organisation has a function to support and assist others in establishing digital platforms, systems and services to:

> 'Support and assist others in the design, development and delivery of digital platforms, systems and services [458].'

The first observation to be made in assessing the scope of these provisions relates to the definition of "digital platforms, systems and services". This is defined as relating to:

> '...hardware, software and other arrangements for the digital collection, storage, processing, analysis, use and dissemination of health service data [459].'

This has a very wide scope and could include almost anything that Digital Health and Care Wales may decide to do.

Arguable any functions that fall outside of the direct provision or promotion of digital platforms, systems and services, but could be seen

as necessary for any reason could be construed as an implied function [381]. An example of this is the National Intelligent Integrated Audit System, that provides automated audit functionality to detect potential confidentiality breaches by staff accessing patient records.

Notwithstanding the more obvious functions that may be implied by the directions, Digital Health and Care Wales nevertheless has significant autonomy in undertaking any function as provided by Paragraph 3(2) of The Digital Health and Care Wales (No.2) Directions 2021 which provides that:

> 'DHCW may do anything which is calculated to facilitate, or is conducive or incidental to, the discharge of its functions [460].'

It is clear that the creation of any digital service in relation to the health service, including clinical systems is within scope of Digital Health and Care Wales. With regard repositories of data, Information services to include maintaining a central repository of data is within scope of the function of 'services' that are secured [459]. Such services can be delivered by Digital Health and Care Wales, or by a third party. Where data is being collected in line with this purpose however, it is important to note that such a collection is to secure the provision or promotion of digital platforms, systems, and services [227].

Paragraph 3(3) of The Digital Health and Care Wales (No.2) Directions 2021 permits Digital Health and Care Wales to advise and make recommendations in relation to any of its functions [461]. This suggests the need for proactive engagement with Welsh Government in relation to operational tasks.

Paragraph 3(4) provides that:

> 'In exercising its functions, DHCW must not disclose information if disclosure of the information is prohibited by any enactment or other rule of law [462].'

The use of the word ‘prohibited’ could need further clarification. The word ‘prohibited’ could suggest that disclosure needs to be expressly prohibited by an enactment or other rule of law. Another approach would be to consider that the word ‘prohibited’ would relate to any circumstance in which disclosure would be unlawful. There is no case law on this, however, the Parent Act, the National Health Service (Wales) Act 2006, does provide some guidance.

Section 140(6), as relates to disclosures of documentation, and information held by or on behalf of Welsh Ministers, provisions outside of the scope of this thesis, provides that:

> ‘Information to which this section applies may be disclosed in accordance with subsection (3) despite any obligation of confidence that would otherwise prohibit or restrict the disclosure [463].’

The use of the word ‘prohibit’ in this context in the National Health Service (Wales) Act 2006 suggests that the obligation of confidence itself prohibits disclosure of information. In the case of paragraph 3(4) therefore, it is inferred that the word ‘prohibited’ refers to the act of an unlawful disclosure, and not having a specific restriction on sharing specific information.

Arguably, acting lawfully is an obligation placed on every person, including legal persons such as a Special Health Authority. It therefore stands to reason that Digital Health and Care Wales should not disclose information where a disclosure is unlawful. Of course, such a prohibition would not apply where Digital Health and Care Wales has a lawful excuse, or another body has a lawful reason to receive the information, such as receiving the information in accordance with its statutory functions.

Obligations in relation to service improvement by Digital Health and Care Wales under Paragraph 4 of The Digital Health and Care Wales (No.2) Directions 2021 are out of scope of this thesis.

7.1.4 Difficulties with the established model

7.1.4.1 Issues Obtaining Data from statutory NHS organisations to perform core functions

As outlined above, Digital Health and Care Wales [1] has a clear remit in its establishment order [2] and has express functions set out in directions [5], that can be legitimately applied in the most general sense [11] with autonomy [6]. In law, when performing these functions, Digital Health and Care Wales can lawfully have information disclosed to it [13]. The only prohibition relates to any disclosure by Digital Health and Care Wales where this is prohibited by law [21].

While this *prima facie* appears not to be a problematic position, misunderstandings as to how information subject to the duty of confidence can be disclosed to Digital Health and Care Wales will continue to be an issue [16] particularly where there is no clear statutory requirement to disclose data. NHS England, for example have powers that enable them to require that data be provided to it to undertake its statutory functions.

Section 259 of the Health and Social Care Act 2012 enables NHS England to require [464] that any health and social care body [465] or any person other than a public service body providing services on behalf of a public body in health or adult social care in England [466] to provide it with any information that they consider 'necessary or expedient for NHS England to have' in relation to functions carried out under the relevant chapter of the Health and Social Care Act 2012 [467]. They can also request of any other person to provide it with information [468].

The approach to confidentiality taken by the health professions, impose specific approaches to confidentiality that extend beyond the scope of

the common law requirements [16]. These are often imposed upon a healthcare professional acting in their clinical capacity [17] and not upon the organisation acting in line with their statutory function.

While relationships with Health Boards and NHS Trusts in Wales may enable constructive discussions to take place to ensure that data is shared for the mutual benefit of patients, in the event a Health Board or NHS Trust refused to share on the basis that they were unsure of the law, this could delay, or even result in programmes or projects set up to benefit patients being closed down before achieving their aim, having also accumulated costs.

7.1.4.2 Issues obtaining data from primary care contractors such as GPs

Where data is stored in the systems of those providing NHS services such as in GP surgeries, or in community pharmacies, despite any lawful excuse that Digital Health and Care Wales may have to receive that data, there is no direct provision in legislation that requires that this be provided to Digital Health and Care Wales. In any case, it may be impractical in communicating with each primary care contractor.

There are however options to require data be provided. The examples provided relate to General Practice information.

The operation of GP services in Wales is, at time of writing, regulated by The National Health Service (General Medical Services Contracts) (Wales) Regulations 2023 [439].

Paragraph 85 of Schedule 3 to the Regulations provides that:

> '(1) Subject to sub-paragraph (2), the contractor must, at the request of the Local Health Board, produce to the Local Health Board or to a person authorised in writing by the Local Health

Board, or allow the Local Health Board or a person authorised in writing by it, to access—

(a) any information which is reasonably required by the Local Health Board for the purposes of or in connection with the contract, and
(b) any other information which is reasonably required in connection with the Local Health Board functions.

(2) The contractor is not required to comply with any request made in accordance with sub-paragraph (1) unless it has been made by the Local Health Board in accordance with directions relating to the provision of information by contractors given to it by the Welsh Ministers under section 12(3) of the Act.

(3) The contractor must produce the information requested, or, as the case may be, allow the Local Health Board access to that information—
(a)by a date agreed as reasonable between the contractor and the Local Health Board, or
(b)in the absence of such agreement, within 28 days beginning with the date the request is made [470].'

To mandate a collection of data from general practice therefore the following steps must be undertaken:

Step one: The Welsh Ministers must direct the Local Health Board in accordance with the provisions of Section 12(3) of the National Health Services (Wales) Act 2006 to request from GPs that information required, and to authorise DHCW access to the information [471].

Step two: The Local Health Board must then write to the GPs to require them to provide information required in connection with general Local Health Board functions and authorising it to be disclosed to Digital Health and Care Wales [472].

Step three: The information must be provided within in 28 days of the request [473] or at a data agreed as reasonable between the contractor and Local Health Board [474]. As a side note, it may be difficult for Local Health Boards to agree with every

GP practice on a date to supply information, given the number of GP practices, and therefore it may be easier not to specify a date and receive the data in the twenty-eight-day limit. This said, the provision of agreeing a date with contractors is a useful provision should a GP practice seek more time.

From the information above, it can be observed that this process is only practical for the extraction of data requests on an ad hoc basis. While it is possible that such a process could be utilised on a regular basis to acquire datasets, this is very bureaucratic.

The next section looks at how it may be possible for Digital Health and Care Wales to lawfully require data in line with existing enactments as apply to Wales.

7.1.5 Solutions to data provision for Digital Health and Care Wales

7.1.5.1 Introduction

It is not proposed to explore the legislative competence of the Welsh Parliament in this thesis to create statutory provision. This section explores the existing powers available to the Welsh Ministers, and how they could be utilised to streamline data provision to Digital Health and Care Wales.

While there may be other options, two methods by which information could be required from Local Health Boards, National Health Service Trusts, and other NHS organisations will be considered. The first relates to General Practice, and in particular amendments that could be made to The National Health Service (General Medical Services Contracts) (Wales) Regulations 2023 or included in any Regulations that replace them. The second relates to the Welsh Ministers existing powers in making

directions in conjunction with the power to make Regulations for medical purposes under section 251 of the National Health Service Act 2006.

7.1.5.2 Utilising provision in the 'GMS Contact Regulations'

In relation to General Medical Services, a requirement for GP practices to provide data to Digital Health and Care Wales could be provided for in an update to, or replacement of The National Health Service (General Medical Services Contracts) (Wales) Regulations 2023 [439].

The National Health Service (General Medical Services Contracts) Regulations 2015 [475] as applies to general practice in England, provides a similar clause to that in National Health Service (General Medical Services Contracts) (Wales) Regulations 2023 [439] as enables Local Health Boards to require data [470]. In the English Regulations there is a provision to enable NHS England to centrally require information be supplied [476]. As previously noted, this approach is very bureaucratic. A more convenient option would be to identify the appropriate flow of data required for specific functions and to provide data is supplied to fulfil those functions. There is a precedent for this. Paragraph 79 of Schedule 3 of the in The National Health Service (General Medical Services Contracts) (Wales) Regulations 2023 [439] provides for the automated retrieval of information from the GP system as follows:

> '(1) Subject to paragraph (2), a contractor must, in any case where there is a change to the information included in a patient's medical record, enable the automated retrieval of summary information from the Welsh GP Record (WGPR) and the NHS Wales App, when the change occurs, using approved systems provided to it by the Local Health Board.
>
> (2) The enabling of automated retrieval of summary information from the WGPR must be for clinical use [477].'

It could be argued that in having a lawful basis to hold GP data in the exercise of its functions, that once received, it could be used for other purposes that form part of Digital Health and Care Wales's functions [12].

This however may not be an appropriate solution to the issue from the perspective of the Welsh Government, or in terms of what the GP community may consider appropriate.

7.1.5.3 Creating Regulations giving Digital Health and Care Wales autonomy

The second method is more complex. In the previous chapter the potential to create Regulation under the provisions of section 251(1) of the National Health Service Act 2006 was discussed, and in particular in relation to any patient information [257], including Confidential Patient Information [258]. Section 251(1) of the National Health Service (Wales) Act 2006 provides that the:

> 'Secretary of State may by Regulations make such provision for and in connection with requiring or regulating the processing of prescribed patient information for medical purposes as he considers necessary or expedient—
> (a) in the interests of improving patient care, or
> (b) in the public interest [251].'

While there are many different types of activities that can be regulated, such as, for example, communication's [259], only the issue as relates to data provision of data to Digital Health and Care Wales will be considered in this section.

Regulations under Section 251(1) of the National Health Service Act 2006 can require the provision of data for medical purposes as defined by Section 251(12) of the Act [252] or for the management or planning of health and social care services. Prescribed conditions could be put in place on this type of disclosure [263], such as the implementation of safeguards, or a privacy committee to assure patients and the public.

Under the Regulations, the Welsh Ministers must consider subjectively that the provisions contained in the Regulations are "necessary or

expedient [251]" in the interests of improving patient care [478], or in the public interest [479]. This is something for consideration by the Welsh Ministers, but it could be argued that an affirmative conclusion could be made in this regard given the importance of data in relation to the strategic benefits of a national NHS.

There is also a requirement that Regulations should only make provision where this is reasonably practical in the circumstances [253]. Given the complexity of the National Health Service, providing instructions by specific directions every time a data set was required could be a bureaucratic process, involving a lot of people, and significant cost. While a statutory function can mean that there is no breach of confidence, for the purpose of the UK GDPR, each organisation is Controller of this data, and another organisation, while having a statutory function would not have access to data. Such Regulations could therefore be justified in that acquiring this data is not reasonably practicable in the circumstances [253].

Regulations under Section 251(1) must not solely be created for the purpose of providing care and treatment for individuals. A body such as Digital Health and Care Wales that undertakes digital and data functions would not determine "the care and treatment to be given to particular individuals [255]", and while information may be used to determine care and treatment of care and treatment, it would not be *solely* used for this purpose [255]. It can be noted at this point that the functionality required to enable the Welsh GP record to be viewed in healthcare settings is a provision already in place, and the access to the data enabled in law by The National Health Service (General Medical Services Contracts) (Wales) Regulations 2023 [477].

There are two options in the use of this Regulation. The first would be that those functions are directly conferred on Digital Health and Care Wales in the Regulations. The second option would be for the Welsh Ministers to retain the power, and then to direct Digital Health and Care Wales to

undertake these functions by Direction, under Section 24(1) of the National Health Service (Wales) Act 2006 which enables the Welsh Ministers to direct a Special Health Authority to exercise the functions of the Welsh Ministers in relation to the Health Service [446].

It should be noted that creation of new Regulations would not replace any existing Regulations produced under Section 251. If a revamp of the existing framework was however proposed, it could be an option to consolidate the provisions in a new set of Regulations.

7.1.5.4 Provisions to set aside the duty of confidence

While Digital Health and Care Wales do have general legal powers to receive the information lawfully, in the interests of certainty, and to protect organisations from inadvertent breaches of confidence the power to set aside the duty of confidence could be implemented in the Regulations [245]. A similar clause to that contained in Regulation 4 of the extant Health Service (Control of Patient Information) Regulations [265] could be used. Another benefit in taking this approach would be that if by complying with the provisions this did in any way operate inconsistently with the data protection Regulations [271], the setting aside of the duty of confidence would not be affected [272].

7.1.5.5 Consultation

Any Regulations created under Section 251(1) must be fully consulted upon [480]. While the legal obligation rests on the Welsh Ministers to subjectively decide who should be consulted [480], it could be suggested that appropriate bodies should include those organisations, contractors or people affected by the Regulations, and professional bodies.

7.1.5.6 Other matters relating to potential Regulation

It is not proposed to discuss the merits or options that could be available to create sanctions under Section 251(2)(d) of the National Health Service (Wales) Act 2006. It could be suggested however that sanctions will ensure compliance with any Regulations passed.

Any Regulations created under Section 251(1) must be reviewed by the Welsh Ministers in line with the requirements of Section 251(5) within one month on the anniversary of the Regulations coming into force [481], As part of this process, the Welsh Ministers must consider whether any other provision can be included in Regulations [481], and vary the Regulations of make new Regulations to reflect these new provisions [482].

7.2 Disclosures by Digital Health and Care Wales

While this chapter discusses the statutory powers of Digital Health and Care Wales and how data can be acquired, it is important to note that data can also be disclosed to other bodies where they have statutory functions [381]. Where bodies are not formed by a legal instrument that creates powers however, the mechanisms set out in other parts of this thesis will still apply. For example, data can be disclosed:

- With the consent of a person to whom the data relates
- Where it is in the public interest to do so
- Where there is a statutory provision that compels disclosure
- Where there is provision that data can be disclosed in other legislation, such as there being an approval to process data under Regulation 5 of the Control of Patient Information Regulations.

7.3 Embedding the principles in working practices in Digital Health and Care Wales

Following the submission of this thesis, a plan of action is to put in place to provide robust processes and guidance in place to ensure that Digital Health and Care Wales. The work to be undertaken will build on existing good practice in the organisation which has been continuously improved utilising knowledge gained through the research.

7.4 Summary of Chapter 7

This chapter represents the first comprehensive academic text of the powers of Digital Health and Care Wales and how data can be lawfully used in line with those powers.

The establishment and statutory powers of Digital Health and Care Wales can be summarised as follows:

- Digital Health and Care Wales was established on the 30th of December 2020 [442] as a Special Health Authority by Order [375] under powers provided to Welsh Ministers under the National Health Service (Wales) Act 2006 [2]
- Functional responsibilities inferred [254] by the Establishment Order [444].
- Functions of a Special Health Authority can be set out in Directions [454], and accordingly directions were issued [450] to *setting out its functions* [8].
- General directions made under Section 23 of the National Health Service (Wales) Act 2006 are lawful [455].
- 'DHCW may do anything which is calculated to facilitate, or is conducive or incidental to, the discharge of its functions [456].'
- 'In exercising its functions, DHCW must not disclose information if disclosure of the information is prohibited by any enactment or other rule of law [462].'

Table 8 (below) sets out the main functions of Digital Health and Care Wales.

Design, develop and deliver digital platforms, systems and services [457]	To support and assist others in the design, development and delivery of digital platforms, systems and services [458]	To support the development and implementation of common standards for digital platforms, systems and services [14].
To advise and assist the Welsh Ministers in relation to the security of digital platforms, systems, services and health service data [15].	To support the development of the digital workforce through education, training and promotion of professional standards [16]	

Table 8: DHCW - Main Functions

The term 'digital platforms, systems and services' relate to *'...hardware, software and other arrangements for the digital collection, storage, processing, analysis, use and dissemination of health service data* [459].'

The following issues exist in ensuring that data can be obtained by Digital Health and Care Wales:

- Unlike powers that NHS England have to require data [19] no equivalent function exists in relation to Digital Health and Care Wales.
- GP information can only be requested by the Local Health Board [470]. No provision exists for Digital Health and Care Wales. This can create a *convoluted* process where:
    - The Welsh Ministers direct the Local Health Board [21] to request information [471].
    - The Local Health Board must write to the GPs to require them to provide information to Digital Health and Care Wales [472].

A solution to the issue of obtaining data may include:

- As relates to general practice, making modifications to include provision in the National Health Service (General Medical Services Contracts) (Wales) Regulations 2023 [439] for Digital Health and Care Wales to acquire data. Similar provision exists in The National Health Service (General Medical Services Contracts) Regulations 2015 [475] in England to enable NHS England to centrally require information be supplied [476]. On an ad hoc basis this could be bureaucratic, but similar provisions to retrieve GP information routinely, as used for the NHS Wales App may be more efficient [477].
- As relates to more general data functions, there is an option to create Regulation under the provisions of section 251 of the National Health Service Act 2006 to require the provision of data for medical purposes as defined by Section 251(12) of the Act [252] or for the management or planning of health and social care services. Setting aside the duty of confidence as permitted by the Act [245], so providing other bodies with certainty. New regulation could then:
    - Be directly conferred on Digital Health and Care Wales in those Regulations; or
    - Conferred on Digital Health and Care Wales by direction to undertake the functions on its behalf [446].

The next chapter acts as a conclusion to this thesis.

8. Conclusion and future work

8.1 Contribution to knowledge

The purpose of undertaking the research originated from internal discussions relating to the lack of clarity around the law as relates to the duty of confidence and the resulting whether disclosures could be made lawfully. The author is employed in a senior information governance role in the organisation and had observed that across the NHS in Wales there were often misconceptions as to what constituted law and what constituted good practice.

As explained in the previous chapter, the research undertaken for this Ph.D. has already been used within the service and will be utilised to provide further advice and guidance in the service. This research provides the following contributions to knowledge:

- Chapter 2 provides a basic set of principles relevant to the NHS, that will contribute to a better understanding as to whether information is confidential.
- Chapter 3 provides an academic text systemising and explaining comprehensively existing knowledge in relation to the defence of consent as relates to the duty of confidence in the healthcare context.
- Chapter 4 provides an academic text systemising and explaining comprehensively existing knowledge in relation to the public interest defence as relates to the duty of confidence in the healthcare context.
- Chapter 5 represents the first comprehensive academic text of the powers to the Secretary of State for Health in England and the Welsh Ministers under section 251 of the National Health Services Wales Act 2006. The Chapter also describes the regulations currently in force.
- Chapter 6 provides an academic text systemising and explaining comprehensively existing knowledge in relation to the public law,

and how this enables data to be shared or obtained lawfully where there is a duty of confidence. The chapter also represents the first comprehensive academic text of the basic statutory functions in place in NHS Wales and how these can enable data to be shared or obtained lawfully by NHS statutory bodies where there is a duty of confidence.

- Chapter 7 represents the first comprehensive academic text of the powers of Digital Health and Care Wales and how data can be lawfully used in line with those powers.

This work thus makes a significant contribution to knowledge by addressing each of these issues.

8.2 Information contained in this thesis

This thesis has set out the relevant information within the provided scope as follows:

- **Common law duty of confidence**

  The thesis defines the common law duty of confidence to the extent set out at the beginning of the research project by:

  - Defining the duty of confidence as relates the confidential information that relates to individuals, with references to health data where appropriate.
  - Setting out the elements as relate to a potential breach of confidence in the following areas:
    - **Quality of confidence:** A description of the relevant factors that relate to establishing the quality of confidence including:
      - The format of information
      - The effect of trivial confidences
      - The effect of information entering the public domain

        - The effect of anonymisation
        - The effect of death on confidential information
        - Other incidental information that is of note, and relevant to the subject is included for completeness.
    - **Imparted in circumstances importing an obligation of confidence':** An explanation as to when information is considered to have been imparted in circumstances importing an obligation of confidence with reference to the case law, and other factors, including relationships.
    - **Breach of confidence:** Defining what is meant by a breach of confidence and explaining the circumstances by which a breach of confidence may arise. Where there are breaches of the duty of confidence in relation to personal information, an explanation has been included as to how this will also result in a breach of the UK GDPR.

- **Defences: consent**

  The thesis defines consent to the extent set out at the beginning of the research project by:

  - Defining valid consent as set out in general common law principles, acknowledging the lack of case law in relation to the duty of confidence.
  - Setting out the components for consent including:

    - **Knowledge:**
        - The expectations as relate to knowledge and the concepts applied in relation to any express and complied consent.
        - The concept of reasonable expectations
        - The impact of a misrepresentation on knowledge.
        - An overview of key principles as relates to capacity, including at high level, and overview of the Mental Capacity Act 2005, and the law that creates

considerations at common law in relation to adults and children.

- **Freely given consent:**
  - The definition of freely given consent, describing how relationships can affect freely given consent.
  - An explanation on the effect of undue influence on whether consent has been freely given.
- **Signifying consent:**
  - The ways in which consent can be signified is explained in the thesis.

- An explanation of the relevance of consent at common law, and how the two regimes operate in practice.

- **Defences: public interest**

The chapter defines what is meant by a public interest disclosure by:

- Illustrating where the public interest defences has been applied.
- Set out the basic principle of the public interest test.
- Explains the relevance of the timing of a disclosure and the parties to that disclosure.
- Sets out how the public interest test applies in the public sector,
- Explains why the public interest test is relevant to any request for information under the Freedom of Information Act 2000.

- **Defences: lawful disclosures – disclosures permitted or required by Statute**

Lawful disclosures in law are explained, with a particular focus on disclosures enabled by Section 251 of the National Health Service Act 2006. In particular this thesis:

- Defines the purpose of Section 251 of the National Health Service Act 2006.

- Explains the provisions that devolve functions to the Welsh Ministers.
- Explains the powers conferred by the Act.
- Describes current Regulation under the Act, and in particular:
    - Explains the scope of the Regulations
    - Explains the effect on the common law duty of confidence
    - Provides a high-level description of the operation and effect of Regulation 2 as relates to collections of information as relates to neoplasia,
    - Provides a high-level description of the law and effect of Regulation 3 as relates to communicable diseases and other risks to public health, with a high-level overview of their use, considering the provisions contained in the Regulation, and the effect of a notice to process information.
    - Outlines of the purpose of Regulation 5, and how it operates.

- **Lawful disclosures: statutory functions**

The chapter describes those statutory gateways that exist, and in particular it:

- Describes the types of statutory gateway that may exist that enable confidential information to be acquired or disclosed in certain circumstances.
- Explains other gateways that may be available that derive from government, but only to the extent as to explain their existence.
- Describes how the statutory bodies in Wales were formed and are organised at a high level. The specific functions of Health Boards and NHS Trusts in Wales, or the Functions of Health Education Improvement Wales, are not considered.
- Describes The Welsh Ministers powers to direct NHS organisations and in particular:
    - The statutory provisions that relate to specific directions

    - The format of directions
    - The amendment or revocation of directions
  - Explains the mechanisms available to enable NHS England to create an information system on behalf of any other person.
  - Highlights the impact of the Human Rights Act 1998 on statutory functions of a public authority.

- **Central digital functions in Wales: A case study**

  The thesis explains how Digital Health and Care Wales:
  - Is established in law
  - Can use of information subject to the duty of confidence as a result of its functions and directions.
  - The role of Digital Health and Care Wales
  - Is able to data disclosed to it lawfully despite the duty of confidence as a result of its functions.

  The thesis also explores the difficulties that Digital Health and Care Wales encounters within the current established model, with reference to the powers enjoyed by NHS England. Potential solutions are identified that could be applied with Digital Health Wales existing in its current form.

8.3 Application of the research to date

The author is a Principal Information Governance Lead at Digital Health and Care Wales. The research has been timely as the organisation was formed during the period of research, and therefore principles established as part of the research have been used frequently to:

- Advise Welsh Government officials as to the necessary action that may be required to ensure Digital Health and Care Wales can receive information subject to the duty of confidence lawfully, in line with common law principles.

- Advise colleagues in the NHS in England how the law as applies to bodies in Wales can be used to processes information subject to the duty of confidence lawfully.
- Provide internal advice during the Covid-19 pandemic around disclosures of information by application of statutory functions.
- Provide internal advice within NHS Wales as to the lawfulness of disclosures of data subject to the duty of confidence.

8.4 Future research

This thesis sets out many key areas as relate to the common law duty of confidence. It intends to demystify the law in the area to enable the lawful sharing of information. The thesis intentionally looks specifically at the law in these areas. Further research could include:

- A comparison of legal principles with those ethical principles set out by professional bodies, to include research to explain those circumstances where ethical principles may apply.
- Establishing whether existing approvals under Regulation 5 of the Health Service (Control of Patient Information) Regulations 2002 had a lawful basis at common law, with the effect that the approval was not within scope of Regulation 5 and therefore rendering the approval ultra vires.
- Examining in which type of situation the duty of confidence could be set aside by crown powers such as the Royal Prerogative.
- A study on how the law compares to sociolegal principles of confidentiality, not discussed by this thesis, but the texts of which the author is aware of and many of which he has read.

As part of further work, a guidance document for information governance professionals in Wales would be a useful document. Such guidance could apply the principles of the common law duty of confidence together with other good practice guidance and apply this in a way that is appropriate to the organisations that form the National Health Service in Wales,

establishing good practice guidance and robust processes to ensure that information is only used in appropriate circumstances.

References

[1] L. Edelstein, The Hippocratic Oath, text, translation and interpretation, Baltimore, John Hopkins Press, 1943.

[2] General Medical Council, Good Medical Practice, Manchester, 2024, p. 11.

[3] Hunter v. Mann [1974] 1 QB 767.

[4] Cited in Albert v. Strange [1849] 1 Mac. & G.25 at para 46.

[5] HM Law Commission, "Law Commission, Breach of Confidence (Law Comm CP No 58, 1974)".

[6] Albert v. Strange [1849] 1 Mac. & G.25.

[7] Morison v. Moat (1861) 68 E.R. 492.

[8] Albert v. Strange [1849] 1 Mac. & G.25 at p44.

[9] United Kingdom General Data Protection Regulation, Article 5(1)(a).

[10] A. M. W. P. Moodie, "'Confidentiality, Codes and Courts. An Examination of the Significance of Professional Guidelines on Medical Ethics in Determining the Legal Limits of Accountability," Ango-American Law Review, vol. 29, no. 1, pp. 39-66, 2000.

[11] O. L. &. S. P. Quick, "Confidentiality and public interest disclosure: A framework to evaluate UK healthcare professional regulatory guidance," Medical Law International, vol. 22(1), pp. 3-32, at 24, 2022.

[12] R v. Department of Health ex parte Source Informatics (CA) [2001] Q.B. 424 at 440.

[13] Kennedy v. The Charity Commission [2014] 2 All ER 847.

[14] Kennedy v. The Charity Commission [2014] 2 All ER 847 at 855-856.

[15] The Law Commission,, Data Sharing between Public Bodies: A Scoping Report (Law Com No 351, 2014).

[16] The Law Commission, "The Law Commission,, Data Sharing between Public Bodies: A Scoping Report (Law Com No 351, 2014),, Para 5.21".

[17] "The Law Commission,, Data Sharing between Public Bodies: A Scoping Report (Law Com No 351, 2014), Para 1.54".

[18] Interpretation Act 1978, Section 6.

[19] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

[20] Data Protection Act 2018.

[21] United Kingdom General Data Protection Regulation.

[22] Coco v. A.N. Clark (Engineers) Limited [1968] F.S.R. 415.

[23] United Kingdom General Data Protection Regulation, Article 4(1).

[24] United Kingdom General Data Protection Regulation, Article 4(2).

[25] United Kingdom General Data Protection Regulation, Article 77.

[26] British Medical Association, Ethics Toolkit: Confidentiality, London: British Medical Association, 2024.

[27] General Medical Council, Confidentiality: good practice in handling patient information, Manchester: General medical Council, 2021.

[28] A.G. v. Guardian Newspapers [1988] 2 W.L.R. 805.

[29] Health and Social Care Act 2012, Section 256(1).

[30] Saltman Engineering Co. Ltd. v. Campbell Engineering Co. Ltd. (1948) 65 R.P.C. 203 at 215.

[31] Venables v. MGN and Thompson v. MGN [2001] Fam. 430, at 461.

[32] Seager v. Copydex Ltd. [1967] 1 W.L.R. 923.

[33] D v. L [2003] EWCA Civ 1169 at 24.

[34] D v. L [2003] EWCA Civ 1169.

[35] Campbell v. M.G.N. [2004] UKHL 22.

[36] Campbell v. M.G.N. [2004] UKHL 22 at 5.

[37] W v. Egdell [1990] 1 Ch 359.

[38] Coco v. A.N. Clark (Engineers) Limited [1968] F.S.R. 415 at 422.

[39] Campbell v. M.G.N. [2004] UKHL 22 at 157.

[40] W v. Egdell [1990] 1 Ch 359 at 419.

[41] Saltman Engineering Co. Ltd. v. Campbell Engineering Co. Ltd. (1948) 65 R.P.C. 203.

[42] Stephens v. Avery [1988] Ch. 449 at 454.

[43] A.G. v. Guardian Newspapers [1988] 2 W.L.R. 805 at 868.

[44] O. Mustad and Son v. Dosen [1964] 1 W.L.R. 109.

[45] O. Mustad and Son v. Dosen [1964] 1 W.L.R. 109 at 111.

[46] Ashworth Hospital Authority v. Mirror Group Newspapers Ltd 67 BMLR 175.

[47] Schering Chemicals Ltd. v. Falkman Ltd. [1982] 1 Q.B. 1.

[48] Schering Chemicals Ltd. v. Falkman Ltd. [1982] 1 Q.B. 1 at 5.

[49] Seager v. Copydex Ltd. [1967] 1 W.L.R. 923 at 931 - 932.

[50] A v. B Plc and Another [2001] (QB) 1 W.L.R. 2341 at 2354.

[51] Barrymore and another v. News Group Newspapers Ltd and another (1997) IP&T Digest 49.

[52] A v. B Plc and Another [2001] (QB) 1 W.L.R. 2341 at 2355.

[53] Stephens v. Avery [1988] Ch. 449.

[54] A v. B Plc and Another [2001] (QB) 1 W.L.R. 2341.

[55] Seager v. Copydex Ltd. [1967] 1 W.L.R. 923 at 931.

[56] R v. D [1984] A.C. 778 at 806.

[57] R v. Department of Health ex parte Source Informatics (CA) [2001] Q.B. 424 at 439.

[58] H (a Healthworker) v. Associated Newspapers Ltd. [2002] EWCA civ 195, at 48.

[59] United Kingdom General Data Protection Regulation, Article 4(5).

[60] H (a Healthworker) v. Associated Newspapers Ltd. [2002] EWCA civ 195, at 59.

[61] H (a Healthworker) v. Associated Newspapers Ltd. [2002] EWCA civ 195.

[62] H (a Healthworker) v. Associated Newspapers Ltd. [2002] EWCA civ 195, at 9.

[63] Lewis v. The Secretary of State for Health [2008] EWHC 2196 (QB) at 19.

[64] Lewis v. The Secretary of State for Health [2008] EWHC 2196 (QB).

[65] Bluck v. Information Commissioner and Epsom & St Helier University NHS Trust [2006] UKIT EA 2006 0090..

[66] Lewis v. The Secretary of State for Health [2008] EWHC 2196 (QB) at 18.

[67] Attorney General v. Jonathan Cape Ltd [1975] 3 WLR 606.

[68] Attorney General v. Jonathan Cape Ltd [1975] 3 WLR 606 at 616.

[69] Lewis v. The Secretary of State for Health [2008] EWHC 2196 (QB), 30.

[70] Coco v. A.N. Clark (Engineers) Limited [1968] F.S.R. 415 at 420.

[71] Coco v. A.N. Clark (Engineers) Limited [1968] F.S.R. 415 at 421.

[72] Coco v. A.N. Clark (Engineers) Limited [1968] F.S.R. 415 at 419.

[73] Peter Pan Manufacturing Corporation v. Corsets Silhouette Ltd [l964] 1 WLR. 96.

[74] Fraser v. Thames Television Ltd [l984] Q.B. 44.

[75] United Kingdom General Data Protection Regulation, Article 28.

[76] Tweddle v. Atkinson [1861] EWHC QB J57.

[77] Donoghue v. Stevenson (1932) AC 562 at 580.

[78] Venables v. MGN and Thompson v. MGN [2001] Fam. 430.

[79] Health Protection (Notification) (Wales) Regulations 2010, SI 2010/1546, Regulation 2(1).

[80] The Health Service (Control of Patient Information) Regulations 2002, SI 2002/1438, Regulation 5(1).

[81] National Health Service (Wales) Act 2006, Section 22(1).

[82] X v. Y and others [1988] 2 All ER 648.

[83] X v. Y and others [1988] 2 All ER 648 at 650.

[84] Dubai Aluminium v. Salaam [2003] 2 AC 366.

[85] Dubai Aluminium v. Salaam [2003] 2 AC 366 at 401.

[86] Various Claimants v. Wm Morrison Supermarkets plc [2020] AC 989.

[87] Various Claimants v. Wm Morrison Supermarkets plc [2020] AC 989 at 1018.

[88] Taranto v. Cornelius [2001] All ER 227.

[89] R v. Department of Health ex parte Source Informatics (CA) [2001] Q.B. 424.

[90] R v. Department of Health ex parte Source Informatics (CA) [2001] Q.B. 424 at 444.

[91] Attorney General v. Guardian (no 2) [1990] 1 A.C. 109.

[92] Sports Direct International plc v. Rangers International Football Club plc [2016] EWHC 85 (Ch) at 26.

[93] Warren v. DSG Retail Ltd [2022] 1 All ER (Comm) 1191 at 1198.

[94] Warren v. DSG Retail Ltd [2022] 1 All ER (Comm) 1191 at 1198.

[95] United Kingdom General Data Protection Regulation, Article 5(1)(f).

[96] Smith and Others v. Talktalk Telecom Group Plc [2022] EWHC 1311 (QB).

[97] Printers and Finishers Ltd v. Holloway and Others [1964] 3 All ER 731 at 736.

[98] Murray v. Express Newspapers Ltd [2007] EWHC 1908 at 72.

[99] Freeman v. The Home Office (No 2) [1984] 1 Q.B. 524 at 527.

[100] Re Caughey ex p. Ford (1876) 1 Ch.D 521 at 528.

[101] R (on the application of Stevens) v. Plymouth City Council [2002] EWCA Civ 388.

[102] Re Caughey ex p. Ford (1876) 1 Ch.D 521 at 521.

[103] Bell v. Alfred Franks & Bartlett Co. Ltd. and Another [1980] 1 W.L.R. 340 at 350.

[104] Re Caughey ex p. Ford (1876) 1 Ch.D 521.

[105] Chatterton v. Gerson [1981] 1 All ER 257.

[106] R (W and others) v. Secretary of State for Health (British Medical Association intervening) [2015] EWCA Civ 1034.

[107] Montgomery v. Lanarkshire Health Board [2015] UKSC 11.

[108] St George's Healthcare NHS Trust v. S; R v. Collins and others ex parte S, [1998] 3 All ER 673.

[109] Marland v. Director of Public Prosecutions [2023] EWHC 1046 (Admin).

[110] Murray v. Express Newspapers plc, [2008] EWCA Civ 446.

[111] Murray v. Express Newspapers plc, [2008] EWCA Civ 446 at 24.

[112] R (W and others) v. Secretary of State for Health (British Medical Association intervening) [2015] EWCA Civ 1034 at 42.

[113] Rex (Piffs Elm Ltd) v. Commission for Local Administration in England [2024] KB 107 at 146.

[114] Nettleship v. Weston [1971] 3 All ER 581 at 587.

[115] National Data Guardian, "Letter from the National Data Guardian to the Information Commissioner," 21 08 2018. [Online]. Available: https://assets.publishing.service.gov.uk/media/5d5e5d3aed915d08d9cf7239/21.08.18_-_NDG_to_ICO.pdf. [Accessed 01 07 2024].

[116] Freeman v. The Home Office (No 2) [1984] 1 Q.B. 524 at 556.

[117] United Kingdom General Data Protection Regulation, Article 13.

[118] United Kingdom General Data Protection Regulation, Article 14.

[119] Chatterton v. Gerson [1981] 1 All ER 257 at 265.

[120] Smith v. Austin Lifts Ltd [1959] 1 All ER 81.

[121] Morris v. Murray [1991] 2 QB 6.

[122] Morris v. Murray [1991] 2 QB 6 at 28.

[123] Smith v. Austin Lifts Ltd [1959] 1 All ER 81 at 81.

[124] Abbas v. Kenney [1996] 31 BMLR 157 at 163.

[125] Freeman v. The Home Office (No 2) [1984] 1 Q.B. 524.

[126] R v. Tabassum [2000] All ER (D) 649.

[127] Mental Capacity Act 2005, Section 2(1).

[128] Mental Capacity Act 2005, Section 2(2).

[129] Mental Capacity Act 2005, Section 2(4).

[130] Mental Capacity Act 2005, Section 3(1)(a).

[131] Mental Capacity Act 2005, Section 3(1)(b).

[132] S. 3. Mental Capacity Act 2005.

[133] Mental Capacity Act 2005, Section 3(1)(d).

[134] Mental Capacity Act 2005, Section 2(5).

[135] Mental Capacity Act 2005, Section 1(1) ('the principles').

[136] Mental Capacity Act 2005, Section 2(3)(a).

[137] Mental Capacity Act 2005, Section 2(3)(b).

[138] Mental Capacity Act 2005, Section 3(2).

[139] Mental Capacity Act 2005, Section 1(3) ('the principles').

[140] Mental Capacity Act 2005, Section 3(3).

[141] Mental Capacity Act 2005, Section 3(4)(a).

[142] Mental Capacity Act 2005, Section 3(4)(b).

[143] Mental Capacity Act 2005, Section 1(4) (The principles).

[144] Mental Capacity Act 2005, Section 3(3)(1)(c).

[145] Mental Capacity Act 2005.

[146] Re L (Vulnerable Adults: Court's Jurisdiction) (No 2) (CA) [2012] 3 WLR 1439.

[147] Re L (Vulnerable Adults: Court's Jurisdiction) (No 2) (CA) [2012] 3 WLR 1439 at 1440.

[148] Gillick v. West Norfolk and Wisbech Area Health Authority [1986] 1 A.C. 112.

[149] Gillick v. West Norfolk and Wisbech Area Health Authority [1986] 1 A.C. 112 at 185.

[150] Banks v. Goodfellow [1861-73] All ER Rep 47.

[151] Children's Act 1989.

[152] Children's Act 1989, Section 105(1).

[153] Family Law Reform Act 1969.

[154] Family Law Reform Act 1969, Section 8(1).

[155] Family Law Reform Act 1969, Section 8(3).

[156] Gillick v. West Norfolk and Wisbech Area Health Authority [1986] 1 A.C. 112 at 170.

[157] Hewer v. Bryant [1970] 1 Q.B. 357 at 369.

[158] Gillick v. West Norfolk and Wisbech Area Health Authority [1986] 1 A.C. 112 at 171.

[159] Gillick v. West Norfolk and Wisbech Area Health Authority [1986] 1 A.C. 112 at 185.

[160] Bowater v. Rowley Regis Corp [1944] KB 476.

[161] United Kingdom General Data Protection Regulation, Article 6(1)(a).

[162] United Kingdom General Data Protection Regulation, Article 7(4).

[163] Information Commissioners Office, Guide to the GDPR, Wilmslow, 2022, p. 96.

[164] Royal Bank of Scotland plc v. Etridge (No 2) [2002] 2 AC 773 at 8.

[165] Bank of Credit Internacional SA v. Aboody [1990] 1 QB 923 at 969–970.

[166] Royal Bank of Scotland plc v. Etridge (No 2) [2002] 2 AC 773.

[167] Re T (adult: refusal of medical treatment) [1992] 4 All ER 649 at 662.

[168] Re T (adult: refusal of medical treatment) [1992] 4 All ER 649.

[169] Powell v. Powell [1900] 1 Ch. 243 at 246.

[170] Powell v. Powell [1900] 1 Ch. 243.

[171] Allcard v. Skinner (1887) 36 Ch D 145 at 182–183, CA.

[172] Bell v. Alfred Franks & Bartlett Co. Ltd. and Another [1980] 1 W.L.R. 340.

[173] Taylor v. Shropshire Health Authority [1998] Lloyd's Rep Med 395.

[174] Taylor v. Shropshire Health Authority [1998] Lloyd's Rep Med 395 at 398.

[175] Winterbotham v. Shahrak [2024] EWHC 2633 (KB).

[176] Sunderland v. Barclays Bank Ltd (1938) 5 LDAB 163.

[177] Re F (mental patient: sterilisation) [1989] 2 All ER 545 at 546.

[178] Re F (mental patient: sterilisation) [1989] 2 All ER 545.

[179] United Kingdom General Data Protection Regulation, Article 4(11).

[180] United Kingdom General Data Protection Regulation, Article 9(1).

[181] United Kingdom General Data Protection Regulation, Article 9(2).

[182] United Kingdom General Data Protection Regulation, Article 9(2)(a).

[183] Data Protection Act 2018, Sections 3(2), 3(3) and 3(5).

[184] United Kingdom General Data Protection Regulation, Article 7(2).

[185] United Kingdom General Data Protection Regulation, Recital 42.

[186] United Kingdom General Data Protection Regulation, Recital 43.

[187] United Kingdom General Data Protection Regulation, Article 7(3).

[188] United Kingdom General Data Protection Regulation, Article 6(1).

[189] United Kingdom General Data Protection Regulation, Recital 32.

[190] United Kingdom General Data Protection Regulation, Article 7(1).

[191] United Kingdom General Data Protection Regulation, Article 6(1)(e).

[192] United Kingdom General Data Protection Regulation, Article 6(1)(c).

[193] United Kingdom General Data Protection Regulation, Article 9(2)(h).

[194] United Kingdom General Data Protection Regulation, Article 9(2)(i).

[195] Attorney General v. Guardian (no 2) [1990] 1 A.C. 109 at 282.

[196] “Confidentiality NHS Code of Practice, Supplementary Guidance: Public Interest Disclosures, Department of Health, London, 2010, page 10, Pargraph 18”.

[197] British Steel Corporation v. Granada Television Ltd [1981] A.C. 1096 at 1168.

[198] British Steel Corporation v. Granada Television Ltd [1981] A.C. 1096.

[199] Lion Laboratories Ltd. v. Evans and Others [1985] 1 Q.B. 526.

[200] Lion Laboratories Ltd. v. Evans and Others [1985] 1 Q.B. 526 at 537.

[201] R v. Chief Constable of North Wales Police, ex p Thorpe [1999] QB 396 at 428.

[202] Gartside v. Outram (1857) 26 L.J.Ch. 113.

[203] Gartside v. Outram (1857) 26 L.J.Ch. 113 at 114.

[204] Initial Services Ltd v. Putterill [1968] 1 QB 396.

[205] Initial Services Ltd v. Putterill [1968] 1 QB 396 at 405.

[206] Fraser v. Evans and Others [1969] 1 Q.B. 349.

[207] Fraser v. Evans and Others [1969] 1 Q.B. 349 at 360.

[208] Malone v. Metropolitan Police Commissioner [1979] Ch. 344.

[209] Malone v. Metropolitan Police Commissioner [1979] Ch. 344 at 362.

[210] Jockey Club v. Buffham [2002] EWHC 1866 (QB).

[211] Woolgar v. Chief Constable of the Sussex Police and another [1999] 3 All ER 604 at 614-615.

[212] Mosley v. News Group Newspapers Ltd [2008] EWHC 1777 (QB) at 111.

[213] Mosley v. News Group Newspapers Ltd [2008] EWHC 1777 (QB).

[214] Mosley v. News Group Newspapers Ltd [2008] EWHC 1777 (QB) at 232.

[215] Mosley v. News Group Newspapers Ltd [2008] EWHC 1777 (QB) at 116.

[216] The Health Service (Control of Patient Information) Regulations 2002, SI 2002/1438, Regulation 3(1).

[217] The Health Service (Control of Patient Information) Regulations 2002, SI 2002/1438, Regulation 3(3)(b).

[218] The Health Service (Control of Patient Information) Regulations 2002, SI 2002/1438, Regulation 3(3)(c).

[219] W v. Egdell [1990] 1 Ch 359, at 424.

[220] A B v. C D 1851 D 177.

[221] Schering Chemicals Ltd. v. Falkman Ltd. [1982] 1 Q.B. 1 at 27.

[222] Francome and another v. Mirror Group Newspapers Ltd and others [1984] 2 All ER 408.

[223] Francome and another v. Mirror Group Newspapers Ltd and others [1984] 2 All ER 408 at 413.

[224] Francome and another v. Mirror Group Newspapers Ltd and others [1984] 2 All ER 408 at 414.

[225] Re a Company's Application [1989] 2 All ER 248.

[226] Re a Company's Application [1989] 2 All ER 248 at 252.

[227] The Digital Health and Care Wales Directions 2020 (WG20-72), Paragraph 3(1).

[228] Freedom of Information Act 2000, Section 8.

[229] Freedom of Information Act 2000, Section 3 and Schedule 1.

[230] Freedom of Information Act 2000, Section 1(1)(a).

[231] Freedom of Information Act 2000, Section 1(6).

[232] Freedom of Information Act 2000, Section 1(1)(b).

[233] Freedom of Information Act 2000, Section 41(1).

[234] Freedom of Information Act 2000, Section 2(3).

[235] Freedom of Information Act 2000, Section 41(1)(a).

[236] Freedom of Information Act 2000, Section 41(1)(b).

[237] Freedom of Information Act 2000, Section 2(2)(a).

[238] Freedom of Information Act 2000, Section 41(2).

[239] Freedom of Information Act 2000, Section 2(1).

[240] Freedom of Information Act 2000, Section 2(2)(b).

[241] Freedom of Information Act 2000, Section 2(1)(a).

[242] Derry CIty Council v. Information Commissioner [2006] UKIT EA 2006 0014.

[243] Derry CIty Council v. Information Commissioner [2006] UKIT EA 2006 0014, Paragraph 35(n).

[244] Health Research Authority, "CAG Guidance," 24th August 2024. [Online]. Available: https://www.hra.nhs.uk/about-us/committees-and-services/confidentiality-advisory-group/guidance-cag-applicants/.

[245] National Health Service Act 2006, Section 251(2)(c).

[246] Lewis v. The Secretary of State for Health [2008] EWHC 2196 (QB) at 48.

[247] Lewis v. The Secretary of State for Health [2008] EWHC 2196 (QB) at 49.

[248] Cities and Local Government Devolution Act 2016.

[249] The Welsh Ministers (Transfer of Functions) Order 2018, S.I. 2018/644, Article 1(1) and Article 43(1).

[250] The Welsh Ministers (Transfer of Functions) Order 2018, S.I. 2018/644, Article 1(5).

[251] National Health Service Act, Section 251(1).

[252] National Health Service Act 2006, Section 251(12).

[253] National Health Service Act 2006, Section 251(4).

[254] R (W and others) v. Secretary of State for Health (British Medical Association intervening) [2015] EWCA Civ 1034 at 68.

[255] National Health Service Act 2006, Section 251(6).

[256] The Health Service (Control of Patient Information) Regulations 2002, SI 2002/1438, Regulation 3(1)(d)(iii).

[257] National Health Service Act 2006, Section 251(10).

[258] National Health Service Act 2006, Section 251(11).

[259] National Health Service Act 2006, Section 251(2)(a).

[260] National Health Service Act 2006, Section 251(2).

[261] National Health Service Act 2006, Section 251(2)(a)(i).

[262] National Health Service Act 2006, Section 251(2)(a)(ii).

[263] National Health Service Act 2006, Section 251(2)(b).

[264] The Health Service (Control of Patient Information) Regulations 2002, SI 2002/1438.

[265] The Health Service (Control of Patient Information) Regulations 2002, SI 2002/1438, Regulation 4.

[266] National Health Service Act 2006, Section 251(2)(d).

[267] The Health Service (Control of Patient Information) Regulations 2002, SI 2002/1438, Regulation 8(1).

[268] The Health Service (Control of Patient Information) Regulations 2002, SI 2002/1438, Regulation 8(3).

[269] The Health Service (Control of Patient Information) Regulations 2002, SI 2002/1438, Regulation 8(2).

[270] National Health Service Act 2006, Section 251(5).

[271] National Health Service Act 2006, Section 251(7).

[272] National Health Service Act 2006, Section 251(8).

[273] National Health Service (Consequential Provisions) Act 2006, Section 6 and Schedule 4.

[274] National Health Service (Consequential Provisions) Act 2006, Section 4, and Schedule 2, Part 1.

[275] Health Research Authority, “The Health Service (Control of Patient Information) Regulations 2002: regulation 5 decision procedure for research applications,” 20 10 2019. [Online]. Available: https://www.hra.nhs.uk/about-us/committees-and-services/confidentiality-advisory-group/guidance-confidentiality-advisory-group-applicants/health-service-control-patient-information-regulations-2002-regulation-5-decision-procedure-research-applications/#:~. [Accessed 01 09 2024].

[276] The Health Service (Control of Patient Information) Regulations 2002 (SI 2002/1438), Regulation 7(2).

[277] The Health Service (Control of Patient Information) Regulations 2002 (SI 2002/1438), Regulation 7(1).

[278] The Local Health Boards (Establishment and Dissolution) (Wales) Order 2009, SI 2009/778 (W. 66), Article 3 and Schedule 1.

[279] United Kingdom General Data Protection Regulation, Article 5(1)(c).

[280] The Health Service (Control of Patient Information) Regulations 2002 (SI 2002/1438), Regulation 7(1)(a).

[281] The Health Service (Control of Patient Information) Regulations 2002 (SI 2002/1438), Regulation 7(1)(d).

[282] United Kingdom General Data Protection Regulation, Article 5(1)(e).

[283] The Health Service (Control of Patient Information) Regulations 2002 (SI 2002/1438), Regulation 7(1)(b).

[284] The Health Service (Control of Patient Information) Regulations 2002 (SI 2002/1438), Regulation 7(1)(c).

[285] Data Protection Act 1998, Schedule 1, Paragraph 7.

[286] United Kingdom General Data Protection Regulation, Article 5(1)(f).

[287] The Health Service (Control of Patient Information) Regulations 2002 (SI 2002/1438), Regulation 7(1)(e).

[288] The Freedom of Information Act 2000 (Commencement No. 5) Order 2004, SI 2004/3122, Article 2.

[289] The Health Service (Control of Patient Information) Regulations 2002, SI 2002/1438, Regulation 2(1).

[290] The Health Service (Control of Patient Information) Regulations 2002, SI 2002/1438, Regulation 2(2).

[291] The Health Service (Control of Patient Information) Regulations 2002 (SI 2002/1438), Regulation 2(3)(a).

[292] The Health Service (Control of Patient Information) Regulations 2002, SI 2002/1438, Regulation 2(3)(b).

[293] The Health Service (Control of Patient Information) Regulations 2002, SI 2002/1438, Regulation 2(4).

[294] National Health Service (Wales) Act 2006, Section 12(1).

[295] National Health Service (Wales) Act 2006, Section 19(1).

[296] The Health Service (Control of Patient Information) Regulations 2002, SI 2002/1438, Regulation 2(5).

[297] The Health Service (Control of Patient Information) Regulations 2002, SI 2002/1438, Regulation 3.

[298] The Health Service (Control of Patient Information) Regulations 2002, SI 2002/1438, Regulation 3(1).

[299] The Health Service (Control of Patient Information) Regulations 2002, SI 2002/1438, Regulation 3(2).

[300] Blashill v. Chambers (1884) 14 QBD 479 at 485, 490.

[301] MacFisheries (Wholesale and Retail) Ltd v. Coventry Corpn [1957] 3 All ER 299.

[302] Utah Construction and Engineering Pty Ltd v. Pataky [1965] 3 All ER 650 at 651.

[303] The Health Service (Control of Patient Information) Regulations 2002, SI 2002/1438, Regulation 3(1)(d).

[304] South West Water Authority v. Rumble's [1985] AC 609 at 619.

[305] The Health Service (Control of Patient Information) Regulations 2002, SI 2002/1438, Regulation 3(1)(d)(i).

[306] The Health Service (Control of Patient Information) Regulations 2002, SI 2002/1438, Regulation 3(1)(d)(ii).

[307] The Health Service (Control of Patient Information) Regulations 2002, SI 2002/1438, Regulation 3(1)(d)(iii).

[308] Ramsay, M. (Ed.). (2020). Immunisation against infectious disease. UK Health Security Agency.

[309] The Health Service (Control of Patient Information) Regulations 2002, SI 2002/1438, Regulation 3(1)(d)(iv).

[310] The Health Service (Control of Patient Information) Regulations 2002, SI 2002/1438, Regulation 3(1)(d)(v).

[311] The Health Service (Control of Patient Information) Regulations 2002, SI 2002/1438, Regulation 3(1)(d)(vi).

[312] The Health Service (Control of Patient Information) Regulations 2002, SI 2002/1438, Regulation 3(4).

[313] R (on the application of the Confederation of Passenger Transport UK) v. Humber Bridge Board 4 All ER 533.

[314] The Health Service (Control of Patient Information) Regulations 2002, SI 2002/1438, Regulation 2(5).

[315] The Health Service (Control of Patient Information) Regulations 2002, SI 2002/1438, Schedule.

[316] The Law Commission,, Data Sharing between Public Bodies: A Scoping Report (Law Com No 351, 2014), Paragraph 1.106.

[317] The Law Commission,, Data Sharing between Public Bodies: A Scoping Report (Law Com No 351, 2014), Paragraph 7.33.

[318] The Health Service (Control of Patient Information) Regulations 2002, SI 2002/1438.

[319] Health and Social Care Act 2012, Section 254.

[320] Health and Social Care Act 2012, Section 259.

[321] Interpretation Act 1978, Section 12(1).

[322] Interpretation Act 1978, Section 12(2).

[323] Woolgar v. Chief Constable of the Sussex Police and another [1999] 3 All ER 604.

[324] R (W and others) v. Secretary of State for Health (British Medical Association intervening) [2015] EWCA Civ 1034 at 62.

[325] Marcel v. Commissioner of Police for the Metropolis [1991] 2 WLR 1118.

[326] Tchenguiz v. Director of the Serious Fraud Office [2013] EWHC 2128 (QB).

[327] The Abortion Regulations 1991, SI 1991/499.

[328] The Abortion Regulations 1991, SI 1991/499, Regulation 5.

[329] Dicey, AV, Introduction to the Study of the Law of the Constitution (8th edn, 1915) p 421, cited in A.G. v. De Keyser's Royal Hotel Ltd [1920] All ER Rep 80 at 86.

[330] Attorney-General (on behalf of His Majesty) v. De Keyser's Royal Hotel, Ltd [1920] All ER Rep 80 at 106.

[331] Council of Civil Service Unions and others v. Minister for the Civil Service [1984] 3 All ER 935 at 942.

[332] Attorney-General (on behalf of His Majesty) v. De Keyser's Royal Hotel, Ltd [1920] All ER Rep 80 at 92.

[333] Council of Civil Service Unions and others v. Minister for the Civil Service [1984] 3 All ER 935 at 956.

[334] Hansard, HL deb 25 02 2003, vol , col 645, col WA 13.

[335] Select Committee on the Constitution, The Pre-emption of Parliament, 2014 (HL 2012-13, 165), Para 52.

[336] Select Committee on the Constitution, The Pre-emption of Parliament, 2014 (HL 2012-13, 165), Para 53-54.

[337] F. Caldicott, “Information: To Share Or Not To Share? The Information Governance Review, Department of Health, 2013”.

[338] F. Caldicott, “Information: To Share Or Not To Share? The Information Governance Review, Department of Health, 2013, Page 21”.

[339] The Law Commission,, Data Sharing between Public Bodies: A Scoping Report (Law Com No 351, 2014),, Paragraph 1.108.

[340] National Health Service (Wales) Act 2006, Section 1.

[341] National Health Service (Wales) Act 2006, Section 2(1)(a).

[342] National Health Service (Wales) Act 2006, Section 2(1)(b).

[343] National Health Service (Wales) Act 2006, Section 1(2).

[344] National Health Service (Wales) Act 2006, Section 18.

[345] National Health Service (Wales) Act 2006, Section 11.

[346] National Health Service (Wales) Act 2006, Section 22.

[347] The Local Health Boards (Establishment) (Wales) Order 2003, SI 2003/148 (W. 18), Article 3 and Schedule.

[348] National Health Service Act 1977, Section16BA.

[349] The Local Health Boards (Establishment and Dissolution) (Wales) Order 2009, SI 2009/778 (W. 66), Article 7.

[350] The Local Health Boards (Establishment and Dissolution) (Wales) Order 2009, SI 2009/778 (W. 66), Article 1(2).

[351] The Local Health Boards (Area Change) (Wales) (Miscellaneous Amendments) Order 2019, SI 2019/349 (W. 83), Article 3(1).

[352] The Local Health Boards (Area Change) (Wales) (Miscellaneous Amendments) Order 2019, SI 2019/349 (W. 83), Article 3(2).

[353] The Local Health Boards (Area Change) (Wales) (Miscellaneous Amendments) Order 2019, SI 2019/349 (W. 83), Article 3(3).

[354] The Local Health Boards (Establishment and Dissolution) (Wales) Order 2009, SI 2009/778 (W. 66), Article 3 and Schedule 1.

[355] Velindre National Health Service Trust (Establishment) Order 1993, SI 1993/2838, Article 2.

[356] National Health Service and Community Care Act 1990, Section 5(1).

[357] Velindre National Health Service Trust (Establishment) Order 1993, SI 1993/2838, Article 3(2)(a).

[358] Velindre National Health Service Trust (Establishment) Order 1993, SI 1993/2838, Article 3(2)(b).

[359] Velindre National Health Service Trust (Establishment) Order 1993, SI 1993/2838, Article 3(2)(c).

[360] Velindre National Health Service Trust (Establishment) Order 1993, SI 1993/2838, Article 3(2)(d).

[361] Velindre National Health Service Trust (Establishment) Order 1993, SI 1993/2838, Article 3(2)(f).

[362] Welsh Ambulance Services National Health Service Trust (Establishment) Order 1998, SI 1998/678, Article 2.

[363] Welsh Ambulance Services National Health Service Trust (Establishment) Order 1998, SI 1998/678, Article 3(2)(a).

[364] Welsh Ambulance Services National Health Service Trust (Establishment) Order 1998, SI 1998/678, Article 3(2)(b).

[365] Public Health Wales National Health Service Trust (Establishment) Order 2009 (SI 2009/2058), Article 2.

[366] National Health Service (Wales) Act 2006, Section 18(1).

[367] Public Health Wales National Health Service Trust (Establishment) Order 2009 (SI 2009/2058), Article 3(2)(a).

[368] Public Health Wales National Health Service Trust (Establishment) Order 2009 (SI 2009/2058), Article 3(2)(b).

[369] Public Health Wales National Health Service Trust (Establishment) Order 2009 (SI 2009/2058), Article 3(2)(d).

[370] Public Health Wales National Health Service Trust (Establishment) Order 2009 (SI 2009/2058), Article 3(2)(c).

[371] The Health Education and Improvement Wales (Establishment and Constitution) Order 2017, SI 2017/913 (W. 224), Article 2.

[372] The Health Education and Improvement Wales (Establishment and Constitution) Order 2017, SI 2017/913 (W. 224).

[373] The Health Education and Improvement Wales (Establishment and Constitution) Order 2017, SI 2017/913 (W. 224), Article 3(1)(a).

[374] The Digital Health and Care Wales (Establishment and Membership) Order 2020, SI 2020/1451 (W. 313), Article 2.

[375] The Digital Health and Care Wales (Establishment and Membership) Order 2020, SI 2020/1451 (W. 313).

[376] The Digital Health and Care Wales (Establishment and Membership) Order 2020, SI 2020/1451 (W. 313), Article 3(a).

[377] The Digital Health and Care Wales (Establishment and Membership) Order 2020, SI 2020/1451 (W. 313), Article 3(b).

[378] The Digital Health and Care Wales (Establishment and Membership) Order 2020, SI 2020/1451 (W. 313), Article 3(c).

[379] The Digital Health and Care Wales (Establishment and Membership) Order 2020, SI 2020/1451 (W. 313), Article 3(d).

[380] The Digital Health and Care Wales (Establishment and Membership) Order 2020, SI 2020/1451 (W. 313), Article 3(e).

[381] Smith Kline & French Laboratories Ltd v. Licensing Authority (Generics (UK) Ltd and another intervening) [1989] 1 All ER 578.

[382] National Health Service (Wales) Act 2006, Section 12.

[383] The Health Authorities (Transfer of Functions, Staff, Property, Rights and Liabilities and Abolition) (Wales) Order 2003, S.I. 2003/813 (W.98).

[384] The Health Authorities (Transfer of Functions, Staff, Property, Rights and Liabilities and Abolition) (Wales) Order 2003, S.I. 2003/813 (W.98), Article 7.

[385] The Health Authorities (Transfer of Functions, Staff, Property, Rights and Liabilities and Abolition) (Wales) Order 2003 (S.I. 2003/813 (W.98)), Article 3.

[386] National Health Service (Wales) Act 2006, Section 12(3).

[387] National Health Service (Wales) Act 2006, Section 13(1).

[388] National Health Service (Wales) Act 2006, Section 13(2)(a).

[389] National Health Service (Wales) Act 2006, Section 13(2)(b).

[390] National Health Service (Wales) Act 2006, Section 13(2)(c).

[391] National Health Service (Wales) Act 2006, Section 13(2)(a), Section 13(3)(aa).

[392] National Health Service (Wales) Act 2006, Section 13(2)(a), Section 13(3)(ab).

[393] National Health Service (Wales) Act 2006, Section 13(2)(a), Section 13(3)(b).

[394] National Health Service (Wales) Act 2006, Section 13(2)(a), Section 13(3)(c).

[395] National Health Service (Wales) Act 2006, Section 19.

[396] National Health Service (Wales) Act 2006, Section 23.

[397] National Health Service (Wales) Act 2006, Section 24.

[398] Richmond Waterworks Co and Southwark and Vauxhall Waterworks Co v. Richmond (Surrey) Vestry (1876) 3 ChD 82 at 98.

[399] Dory v. Sheffield Health Authority 11 BMLR 93.

[400] Dory v. Sheffield Health Authority 11 BMLR 93 at 102-103.

[401] Dory v. Sheffield Health Authority 11 BMLR 93 at 102.

[402] Dory v. Sheffield Health Authority 11 BMLR 93 at 104.

[403] R (Brown (formerly Bajinya) v. Governor of Belmarsh Prison [2007] EWHC 498 (Admin) at 20.

[404] National Health Service (Wales) Act 2006, Section 204(3).

[405] National Health Service (Wales) Act 2006, Section 204(3)(a).

[406] National Health Service (Wales) Act 2006, Section 204(3)(b)(i).

[407] National Health Service (Wales) Act 2006, Section 204(3)(b)(ii).

[408] National Health Service (Wales) Act 2006, Section 204(1).

[409] National Health Service (Wales) Act 2006, Section 31(2).

[410] Health and Social Care Act 2012, Section 255(1).

[411] Health and Social Care Act 2012, Section 255(2).

[412] Health and Social Care Act 2012, Section 257(4).

[413] Health and Social Care Act 2012, Section 255(7).

[414] Health and Social Care Act 2012, Section 255(8)(a).

[415] Health and Social Care Act 2012, Section 255(8)(b)(i), referring to the Code of Practice issued Health and Social Care Act 2012, Section 263.

[416] Health and Social Care Act 2012, Section 255(8)(b)(i), referring to advice and guidance as may be provided under the Health and Social Care Act 2012, Section 265.

[417] Health and Social Care Act 2012, Section 256(1)(a).

[418] Health and Social Care Act 2012, Section 256(1)(b).

[419] Health and Social Care Act 2012, Section 256(2)(b).

[420] Health and Social Care Act 2012, Section 256(2)(c).

[421] Health and Social Care Act 2012, Section 251(1)(a).

[422] Health and Social Care Act 2012, Section 261(2).

[423] Health and Social Care Act 2012, Section 261(1A)(a).

[424] Health and Social Care Act 2012, Section 261(1A)(b).

[425] Health and Social Care Act 2012, Section 261(4).

[426] Health and Social Care Act 2012, Section 262(5).

[427] Health and Social Care Act 2012, Section 261(7).

[428] Health and Social Care Act 2012, Section 262(4)(a).

[429] Health and Social Care Act 2012, Section 262(4)(b).

[430] Health and Social Care Act 2012, Section 260(1).

[431] Health and Social Care Act 2012, Section 260 (2)(a), Section 260(2)(b).

[432] Health and Social Care Act 2012, Section 260(2)(c).

[433] Human Rights Act 1998, Section 21(1).

[434] Human Rights Act 1998, Section 6(1).

[435] Human Rights Act 1998, Section 6(6).

[436] Human Rights Act 1998, Section 6(3)(b).

[437] Human Rights Act 1998, Section 6(5).

[438] YL v. Birmingham City Council and others [2007] 3 All ER 957.

[439] The National Health Service (General Medical Services Contracts) (Wales) Regulations 2023, SI 2023/953 (W. 155).

[440] Human Rights Act 1998, Section 8(2).

[441] Human Rights Act 1998, Section 6(2).

[442] The Digital Health and Care Wales (Establishment and Membership) Order 2020, SI 2020/1451 (W. 313), Article 1(2).

[443] The Digital Health and Care Wales (Transfer of Staff, Property, Rights and Liabilities) Order 2021, SI 2021/233 (W. 59), Article 1(2).

[444] The Digital Health and Care Wales (Establishment and Membership) Order 2020, SI 2020/1451 (W. 313), Article 3.

[445] National Health Service (Wales) Act 2006, Section 23(1).

[446] National Health Service (Wales) Act 2006, Section 24(1).

[447] The Digital Health and Care Wales Directions 2020 (WG20-72).

[448] The Digital Health and Care Wales Directions 2020 (WG20-72), Paragraph 3.

[449] The Digital Health and Care Wales (No.2) Directions 2021 (WG21-30).

[450] The Digital Health and Care Wales (No.2) Directions 2021 (WG21-30), Paragraph 3(1) and (2).

[451] The Digital Health and Care Wales (No.2) Directions 2021 (WG21-30), Paragraph 2.

[452] Health and Social Care Act 2012, Section 254(1).

[453] Health and Social Care Act 2012, Section 254(2)-(7).

[454] National Health Service (Wales) Act 2006, Section 23(1).

[455] National Health Service (Wales) Act 2006, Section 23(3).

[456] The Digital Health and Care Wales (No.2) Directions 2021 (WG21-30), Paragraph 3(2).

[457] The Digital Health and Care Wales Directions 2020 (WG20-72), Paragraph 3(1)(a).

[458] The Digital Health and Care Wales Directions 2020 (WG20-72), Paragraph 3(1)(b).

[459] The Digital Health and Care Wales Directions 2020 (WG20-72), Paragraph 2.

[460] The Digital Health and Care Wales Directions 2020 (WG20-72), Paragraph 3(2).

[461] The Digital Health and Care Wales Directions 2020 (WG20-72), Paragraph 3(3).

[462] The Digital Health and Care Wales Directions 2020 (WG20-72), Paragraph 3(1).

[463] National Health Service (Wales) Act 2006, Section 140(6).

[464] Health and Social Care Act 2012, Section 269(1).

[465] Health and Social Care Act 2012, Section 259(2)(a).

[466] Health and Social Care Act 2012, Section 259(2)(b).

[467] Health and Social Care Act 2012, Section 259(1)(a).

[468] Health and Social Care Act 2012, Section 259(1)(b).

[469] Health and Social Care Act 2012, Section 259(3)-(11).

[470] The National Health Service (General Medical Services Contracts) (Wales) Regulations 2023, SI 2023/953 (W. 155), Schedule 3, Paragraph 85.

[471] The National Health Service (General Medical Services Contracts) (Wales) Regulations 2023, SI 2023/953 (W. 155), Schedule 3, Paragraph 85(2).

[472] The National Health Service (General Medical Services Contracts) (Wales) Regulations 2023, SI 2023/953 (W. 155), Schedule 3, Paragraph 85(1).

[473] The National Health Service (General Medical Services Contracts) (Wales) Regulations 2023, SI 2023/953 (W. 155), Schedule 3, Paragraph 85(3)(b).

[474] The National Health Service (General Medical Services Contracts) (Wales) Regulations 2023, SI 2023/953 (W. 155), Schedule 3, Paragraph 85(3)(a).

[475] The National Health Service (General Medical Services Contracts) Regulations 2015, SI 2015/1862.

[476] The National Health Service (General Medical Services Contracts) Regulations 2015, SI 2015/1862, Regulation 74.

[477] The National Health Service (General Medical Services Contracts) (Wales) Regulations 2023, SI 2023/953 (W. 155), Schedule 3, Paragraph 79.

[478] National Health Service Act, Section 251(1)(a).

[479] National Health Service Act, Section 251(1)(b).

[480] National Health Service Act 2006, Section 251(9).

[481] National Health Service Act 2006, Section 251(5)(a).

[482] National Health Service Act 2006, Section 251(5)(b).

[483] The National Health Service (General Medical Services Contracts) (Wales) Regulations 2023, SI 2023/953 (W. 155), Schedule 3, Paragraph 85(1)(a).

[484] The National Health Service (General Medical Services Contracts) (Wales) Regulations 2023, SI 2023/953 (W. 155), Schedule 3, Paragraph 85(1)(b).

[485] The Law Commission,, Data Sharing between Public Bodies: A Scoping Report (Law Com No 351, 2014),, Paragraph 5.52.

[486] The Health Service (Control of Patient Information) Regulations 2002, SI 2002/1438, Regulation 3(1)(c).

[487] The Health Service (Control of Patient Information) Regulations 2002, SI 2002/1438, Regulation 3(1)(b).

[488] The Health Service (Control of Patient Information) Regulations 2002, SI 2002/1438, Regulation 3(1)(a).

[489] Data Protection Act 1998, Schedule 1, Paragraph 3.