Confidentiality Policy

Policy information

Policy number: 172

Classification:
Corporate

Supersedes:
Previous versions

Version number:
7

Date of Equality Impact Assessment:
20.06.2023

Approval information

Approved by:
Sustainable Resources Committee
Date of approval:
24.10.2023
Date made active:
26.10.2023
Review date:
24.10.2026

Summary of document:
This policy states our commitment to maintain the confidentiality, Privacy and security of all Classified information and outlines mechanisms for ensuring this takes place.

Scope:
This Policy deals with any information (held in any medium) collected or processed by Health Board staff that is subject to a classified status, as defined in the Health Board's Information Classification policy, that staff work with or come into contact with, however transitory, in the course of their work. Staff includes employees, temporary or agency staff, volunteers, locums and third party contractors.
To be read in conjunction with:
183- Information Security policy (opens in new tab)
201- Disciplinary policy (opens in new tab)
173- Freedom of Information Policy (opens in new tab)

All Records Management policies and Procedures

Owning group:
Information Governance Sub-committee (IGSC)*13/04/2023*

Executive Director job title:
Huw Thomas, Director of Finance

Reviews and updates:
1 – New Policy – 01.03.2011
2 – Amended – 28.04.02023
3 – Revised – 26.06.2018
4- Revised – 24.10.2023

Keywords
Confidential, Confidentiality

Glossary of terms

Contents

Introduction

Service users of health and social care are entitled to expect that the information they entrust to their providers of care will be held in the strictest confidence. This requirement has been a cornerstone of the trust that needs to exist between medical practitioner and patient. The trust which allows a patient to divulge intimate details secure in the knowledge that what they say will not be inappropriately divulged. It is not just information security that is important, patients also expect that the professionals involved in their care, will share that information appropriately, reliably, and effectively.

Policy Statement

The Hywel Dda Hywel Dda Health Board (HDdUHB) is committed to protecting the security and privacy of information, regardless of media type, in accordance with applicable laws and regulations. Information is a critical and valuable asset for the HDdUHB. Information security is the protection of information from a wide range of threats in order to ensure business continuity and minimise business risk. The objective of information security is to reduce the risk to the HDdUHB by protecting information, information systems and communications that deliver the information, from failures
of integrity, confidentiality, and availability, whether information is in storage, processing, or transmission. Information security is seen as an enabler to achieve HDdUHB business strategy and objectives and to avoid or reduce relevant risks.

This policy is intended to establish an organisational framework for the HDdUHB's policies related to information Governance and its security.

Scope

This Policy deals with any information (held in any medium) collected or processed by Health Board staff that is subject to a classified status, as defined in the Health Board's Information Classification policy that staff work with or come into contact with, however transitory, in the course of their work. Staff includes employees, temporary or agency staff, volunteers, locums and third party contractors.

Aims

There are a range of complex legal and professional obligations that limit, prohibit or set conditions in respect of the management, use and disclosure of information and, similarly, a range of statutes that permit or require information to be used or disclosed. The aim of this policy is to assist staff in carrying out their duties lawfully by identifying these statutory requirements and providing best practice guidance.

Objectives

This policy assists staff in understanding the interrelationship between the ethical considerations, professional principles and laws in relation to the using or sharing of confidential information and by assisting staff in addressing and understanding their duty under common law to maintain confidentiality and where that duty may be overridden. However, this document should not be seen as a substitute for professional legal advice.

Policy

The purpose of this Confidentiality Policy is to lay down the principles that must be observed by all who work within HDdUHB and have access to person-identifiable information or confidential information. All staff need to be aware of their responsibilities for safeguarding confidentiality and preserving information security.

All staff working in the NHS are bound by a legal duty of confidence to protect personal information they may come into contact with during the course of their work. This is not just a requirement of their contractual responsibilities but also a requirement within the common law duty of confidence and the Data Protection Act 2018, UK General Data Protection Regulation 2016, or any subsequent legislation to the same effect. It is also a requirement within the NHS Care Record Guarantee, produced to assure patients regarding the use of their information.

It is important that the Health Board protects and safeguards person-identifiable and confidential business information that it gathers, creates, processes, and discloses, in order to comply with the law, relevant NHS mandatory requirements and to provide assurance to patients and the public.

This policy sets out the requirements placed on all staff when sharing information within the NHS and between NHS and non-NHS organisations.

Person-identifiable information is anything that contains the means to identify a person, e.g., name, address, postcode, date of birth, NHS number and must not be stored on removable media unless it is encrypted as per current Welsh NHS Encryption Guidance, or a business case has been approved by Digital Services.

Confidential information within the NHS is commonly thought of as health information; however, it can also include information that is private and not public knowledge or information that an individual would not expect to be shared. It can take many forms including patient level health information, employee records, occupational health records, etc. It also includes the Health Board's confidential business information.

Information can relate to patients and staff (including temporary staff), however stored. Information may be held on paper, CD/DVD, USB sticks, computer file or printout, laptops, palmtops, mobile phones, digital cameras or even heard by word of mouth.

A summary of Confidentiality Do's and Don'ts can be found at Appendix A.

The Legal and NHS Mandated Framework for confidentiality which forms the key guiding principles of this policy can be found in Appendix B.

How to report a breach of this policy and what should be reported can be found in Appendix C.

The legal definition of confidential information can be found in Appendix D.

Roles and Responsibilities

The Chief Executive

The Chief Executive has overall responsibility for strategic and operational management, including ensuring that HDdUHB policies comply with all legal, statutory, and good practice guidance requirements.

The Caldicott Guardian

The Caldicott Guardian is responsible for ensuring implementation of the Caldicott Principles with respect to patient-identifiable information.

The Information Governance Sub-Committee

The Information Governance Sub-Committee oversees the development and implementation of Information Governance in the Health Board and ensure that the organisation complies with supporting the Legal and NHS Mandatory Framework with regard to Information Governance.

Director with responsibility for Workforce and Organisational Development (W&OD)

The Director with responsibility for W&OD is responsible for ensuring that the contracts of all staff (permanent and temporary) are compliant with the requirements of the policy and that confidentiality is included in corporate induction for all staff.

Senior Managers

Senior Managers are responsible for ensuring that the policy and its supporting standards and guidelines are built into local processes and that there is on-going compliance. They must ensure that any breaches of the policy are reported, investigated and acted upon via the Information Security Incident Reporting Procedure identified in the IT Security policy.

Head of Information Governance

The Head of Information Governance is responsible for maintaining the accuracy of this policy, providing advice on request to any member of staff on the issues covered within it, and ensuring that training is provided for all staff groups to further their understanding of the principles and their application.

All Staff

Confidentiality is an obligation for all staff. Staff should note that they are bound by the Duty of Confidentiality at Common Law. There is a Confidentiality clause in their contract and that they are expected to participate in induction, training and awareness raising sessions carried out to inform and update staff on confidentiality issues.

Any breach of confidentiality, inappropriate use of health or staff records, or abuse of computer systems is a disciplinary offence, which could result in dismissal or termination of employment contract and must be reported.

Corporate Level Procedures

Principles

All staff must ensure that the following principles are adhered to: -

- Person-identifiable or confidential information must be effectively protected against improper disclosure when it is received, stored, transmitted, or disposed of.
- Access to person-identifiable or confidential information must be on a need-to-know basis.
- Disclosure of person-identifiable or confidential information must be limited to that purpose for which it is required.
- Recipients of disclosed information must respect that it is given to them in confidence.
- If the decision is taken to disclose information, that decision must be justified and documented.
- Any concerns about disclosure must be discussed with either your Line Manager or the Corporate Services Information Governance Team.

HDdUHB is responsible for protecting all the information it holds and must always be able to justify any decision to share information.

Person-identifiable information, wherever possible, must be anonymised by removing as many identifiers as possible whilst not unduly compromising the utility of the data.

Access to rooms and offices where terminals are present, or person identifiable or confidential information is stored must be controlled. Doors must be locked with keys, keypads or accessed by swipe card. In mixed office environments measures should be in place to prevent oversight of person-identifiable information by unauthorised parties.

All staff should clear their desks of confidential or sensitive material at the end of each day. In particular, they must keep all records containing person-identifiable or confidential information in recognised filing and storage places that are locked.

Unwanted printouts containing person-identifiable or confidential information must be put into a confidential waste bin. Discs, tapes, printouts, and fax messages must not be left lying around but be filed and locked away when not in use.

Your Contract of Employment includes a commitment to confidentiality. Breaches of confidentiality could be regarded as gross misconduct and may result in serious disciplinary action up to and including dismissal.

Disclosing Confidential Information

To ensure that information is only shared with the appropriate people in appropriate circumstances, care must be taken to check they have a legal basis for access to the information before releasing it. It is important to consider how much confidential information is needed before disclosing it and ensure that only the minimal amount necessary is disclosed.

When information can be disclosed:

- When it is effectively anonymised.

- When the information is required by law or under a court order. In this situation staff must discuss with their Line Manager or Information Governance staff before disclosing, who will inform and obtain approval of the Caldicott Guardian when appropriate.

- In identifiable form, when it is required for a specific purpose, with the individual's written consent or with support under the Health Service (Control of patient information) regulations 2002, obtained via application to the Confidentiality Advisory Group (CAG) within the Health Research Authority.

- In Child Protection proceedings if it is considered that the information required is in the public or child's interest. In this situation staff must discuss with their Line Manager or Information Governance staff before disclosing, who will inform and obtain approval of the Caldicott Guardian.

- Where disclosure can be justified for another purpose, this is usually for the protection of the public and is likely to be in relation to the prevention and detection of serious crime. In this situation staff must discuss with their Line Manager or Information Governance staff before disclosing, who will inform and obtain approval of the Caldicott Guardian.

If staff have any concerns about disclosing information, they must discuss this with their Line Manager, or the Information Governance staff. Care must be taken in transferring information to ensure that the method used is as secure as it can be. In most instances a Data Sharing, Data Re-Use or Data Transfer Agreement will have been completed before any information is transferred. The Agreement will set out any conditions for use and identify the mode of transfer. For further information on Data Sharing Agreements whether under the Wales Accord on the Sharing of Personal Information) WASPI, Memorandum of Understanding (MOU's) or other regimes please contact the Information Governance team.

Staff must ensure that appropriate standards and safeguards are in place in respect of telephone enquiries, e-mails, faxes and surface mail. See the Safe Haven Procedure for guidance on the safe transfer of confidential or person-identifiable information.

Transferring patient information by email to anyone outside Welsh Health network may only be undertaken by using encryption as per the current HDdUHB All Wales Information Security Policy. Sending information via email to patients is permissible, provided the risks of using unencrypted email have been explained to them, they have given their consent and the information is not person-identifiable or confidential information.

Working Away from the Office Environment

There will be times when staff may need to work from another location or whilst travelling. This means that these staff may need to carry HDdUHB information with them which could be confidential in nature e.g., on a laptop, USB stick or paper documents. Taking home/removing paper documents that contain person-identifiable or confidential information from HDdUHB premises is discouraged. When working away from HDdUHB locations staff must ensure that their working practice complies with HDdUHB policies and procedures.

To ensure the safety of confidential information, staff must keep them on their person at all times whilst travelling and ensure that they are kept in a secure place if they take them home or to another location. Confidential information must be safeguarded at all times and kept in lockable locations. As a general rule, staff must minimise the amount of person-identifiable information that is taken away from HDdUHB premises. If staff need to carry person-identifiable or confidential information they must ensure the following:

- Any personal information is in a sealed non-transparent container i.e., windowless envelope, suitable bag, etc. prior to being taken out of HDdUHB buildings.
- Confidential information is kept out of sight whilst being transported.

If staff need to take person-identifiable or confidential information home, they have personal responsibility to ensure the information is kept secure and confidential. This means that other members of their family and/or their friends/colleagues must not be able to see the content or have any access to the information.

Staff must NOT forward any person-identifiable or confidential information via email to their home e-mail account. Staff must not use or store person identifiable or confidential information on a privately-owned computer or device (including mobile devices).

Carelessness

All staff have a legal duty of confidence to keep person-identifiable or confidential information private and not to divulge information accidentally. Staff may be held personally liable for a breach of confidence and must not:

- Talk about person-identifiable or confidential information in public places or where they can be overheard.
- Leave any person-identifiable or confidential information lying around unattended; this includes telephone messages, computer printouts, faxes, and other documents.
- Leave a computer terminal logged on to a system where person-identifiable or confidential information can be accessed.

Steps must be taken to ensure physical safety and security of person identifiable, or business confidential information held in paper format and on computers.

Passwords must be kept secure and must not be disclosed to unauthorised persons. Staff must not use someone else's password to gain access to information. Action of this kind will be viewed as a serious breach of confidentiality. This is a disciplinary offence and constitutes gross misconduct which may result in summary dismissal.

Abuse of Privilege

It is strictly forbidden for employees to knowingly browse, search for or look at any information relating to themselves, their own family, friends, or other persons, without a legitimate Health

Board purpose. Action of this kind will be viewed as a breach of confidentiality and of the Data Protection Act/UK General Data Protection Regulation 2016 or any subsequent legislation to the same effect.

When dealing with person-identifiable or confidential information of any nature, staff must be aware of their personal responsibility, contractual obligations and undertake to abide by the policies and procedures of the HDdUHB.

If staff have concerns about this issue, they should discuss it with their Line Manager or Information Governance Team.

Confidentiality Audits

Good practice requires that all organisations that handle person identifiable or confidential information put in place processes to highlight actual or potential confidentiality breaches in their systems, and also procedures to evaluate the effectiveness of controls within these systems. This function will be co-ordinated by Digital Services in conjunction with Information Governance team through a programme of audits.

Distribution and Implementation

This document will be made available to all Staff via the HDdUHB intranet site, and a global notice will be sent to staff notifying them of the release of this document.

A link to this document will be provided from the Publication scheme on the HDdUHB intranet site.

Training

Links to the Health Boards policy pages will be provided at staff induction and during local staff training sessions.

Monitoring

Compliance with the policies and procedures laid down in this document will be monitored via the Information Governance team, together with independent reviews by both Internal and External Audit on a periodic basis. The Head of Information Governance is responsible for the monitoring, revision and updating of this document on a 3 yearly basis or sooner if the need arises.

Equality Impact Assessment

This document forms part of the Health Board's commitment to create a positive culture of respect for all staff and service users. The intention is to identify, remove or minimise discriminatory practice in relation to the protected characteristics (race, disability, gender, sexual orientation, age, religious or other belief, marriage and civil partnership, gender reassignment and pregnancy and maternity), as well as to promote positive practice and value the diversity of all individuals and communities. As part of its development this document and its impact on equality has been analysed and no detriment identified.

Who to contact:

Should you have any queries in relation to this policy please email the Information Governance Team at Information.Governance3@wales.nhs.uk, alternatively, you can contact:

Data Protection Officer (DPO) at: DPO.HDD@wales.nhs.uk,

Senior Information Risk Officer (SIRO) at: SIRO.HDD@wales.nhs.uk

Caldicott Guardian at: caldicottguardian.hdd@wales.nhs.uk

Appendix A - Do's and Don'ts

Dos

1. Do safeguard the confidentiality of all person-identifiable or confidential information that you come into contact with. This is a statutory obligation on everyone working in or on behalf of the Health Board.
2. Do clear your desk at the end of each day if possible, keeping all portable records that contain person-identifiable or confidential information in recognised filing and storage places that are locked at times when access is not directly controlled or supervised.
3. Do switch off computers with access to person-identifiable or business confidential information, or put them into a password-protected mode, if you leave your desk for any period of time.
4. Do ensure that you cannot be overheard when discussing confidential matters.
5. Do challenge and verify where necessary the identity of any person who is making a request for person-identifiable or confidential information and ensure they have a need to know.
6. Do share only the minimum information necessary.
7. Do transfer person-identifiable or confidential information securely when necessary, i.e., use encryption to send confidential information to a non NHS email account or use a secure government domain e.g. gsi.gov.uk if possible.
8. Do seek advice if you need to share patient/person-identifiable information without the consent of the patient/identifiable person's consent and record the decision and any action taken.
9, Do report any actual or suspected breaches of confidentiality.
10. Do participate in induction, training and awareness sessions on confidentiality issues.

Don'ts

11. Don't share passwords or leave them lying around for others to see.
12. Don't share information without the consent of the person to which the information relates, unless there are statutory grounds to do so.
13. Don't use person-identifiable information unless absolutely necessary, anonymise the information where possible.
14. Don't collect, hold or process more information than you need, and do not keep it for longer than necessary.

Appendix B: Summary of Legal and NHS Frameworks

The Health Board is obliged to abide by all relevant UK legislation. The requirement to comply with this legislation shall be devolved to employees and agents of HDdUHB, who may be held personally accountable for any breaches of information security for which they may be held responsible.

The Health Board shall comply with the following legislation and guidance as appropriate:

The Data Protection Act/ UK General Data Protection Regulation 2016 or any subsequent legislation to the same effect regulates the use of "personal data" and sets out seven principles to ensure that personal data is:

1. Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.

2. Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

3. Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

5. Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

6. Personal data shall 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.

7. The controller shall be responsible for, and be able to demonstrate, compliance with the principles.

The UK General Data Protection Regulation contains clauses relating to the rights of data subjects namely: the right to be informed, the right of access, the right to rectification, the right to erasure, the right to restrict processing, the right to data portability, the right to object and rights in relation to automated decision making.

The Caldicott Report (1997) recommended that a series of principles be applied when considering whether confidential patient-identifiable information should be shared, a further review took place in January 2012 which resulted in a seventh principle being added. In December 2020 an 8th principle was also added:

1. Justify the purpose for using patient-identifiable information.

2. Don't use patient identifiable information unless it is absolutely necessary.

3. Use the minimum necessary patient-identifiable information.

4. Access to patient-identifiable information should be on a strict need to know basis

5. Everyone should be aware of their responsibilities

6. Understand and comply with the law.

7. The duty to share information can be as important as the duty to protect patient confidentiality.

8. Inform patients and service users about how their confidential information is used.

The Human Rights Act (1998)

Article 8 of which refers to an individual's "*right to respect for their private and family life, for their home and for their correspondence"*. This means that public authorities should take care that their actions do not interfere with these aspects of an individual's life.

The Computer Misuse Act (1990) this Act makes it illegal to access data or computer programs without authorisation and establishes three offences:

1. Unauthorised access data or programs held on computer e.g. to view test results on a patient whose care you are not directly involved in or to obtain or view information about friends and relatives.

2. Unauthorised access with the intent to commit or facilitate further offences e.g. to commit fraud or blackmail.

3. Unauthorised acts the intent to impair, or with recklessness so as to impair, the operation of a computer e.g. to modify data or programs held on computer without authorisation.

Each offence includes the making, supplying or obtaining articles for use in perpetrating these offence.

The Code of Confidentiality for Health and Social Care in Wales (2005) outlines for main requirements that must be met in order to provide patients with a confidential service:

- Protect patient information.
- Inform patients of how their information is used.
- Allow patients to decide whether their information can be shared.
- Look for improved ways to protect, inform and provide choice to patients.

Common Law Duty of Confidentiality

Information given in confidence must not be disclosed without consent unless there is a justifiable reason e.g. a requirement of law or there is an overriding public interest to do so.

Administrative Law

Administrative law governs the actions of public authorities. According to well established rules a public authority must possess the power to carry out what it intends to do. If not, its action is “ultra vires”, i.e. beyond its lawful powers.

The NHS Care Record Guarantee

The Care Record Guarantee sets out twelve high-level commitments for protecting and safeguarding patient information, particularly in regard to: patients’ rights to access their information, how information will be shared both within and outside of the NHS and how decisions on sharing information will be made. The most relevant are:

Commitment 3 - We will not share information (particularly with other government agencies) that identifies you for any reason, unless:

- You ask us to do so.
- We ask and you give us specific permission.
- We have to do this by law.
- We have special permission for health or research purposes; or We have special permission because the public good is thought to be of greater importance than your confidentiality, and if we share information without your permission, we will make sure that we keep to the Data Protection Act, the Code of Confidentiality for Health and Social Care in Wales and other national guidelines on best practice.

Commitment 9 - We will make sure, through contract terms and staff training, that everyone who works in or on behalf of the Health Board understands their duty of confidentiality, what it means in practice and how it applies to all parts of their work. Organisations under contract to the NHS must follow the same policies and controls as the NHS does. We will enforce this duty at all times.

Appendix C: Reporting of Policy Breaches

What should be reported?

Misuse of personal data and security incidents must be reported so that steps can be taken to rectify the problem and to ensure that the same problem does not occur again. All breaches should be reported either on Datix or via email. If staff are unsure as to whether a particular activity amounts to a breach of the policy, they should discuss their concerns with their Line Manager or Information Governance staff. The following list gives examples of

breaches of this policy which should be reported:

- Sharing of passwords.
- Unauthorised access to Health Board systems either by staff or a third party.
- Unauthorised access to person-identifiable information where the member of staff does not have a need to know.
- Disclosure of person-identifiable information to a third party where there is no justification and you have concerns that it is not in accordance with the Data Protection Act or duty of Confidentiality.
- Sending person-identifiable or confidential information in a way that breaches confidentiality.
- Leaving person-identifiable or confidential information lying around in public area.
- Theft or loss of person-identifiable or confidential information in any media.
- Disposal of person-identifiable or confidential information in a way that breaches confidentiality i.e. disposing off person identifiable information in ordinary waste paper bin.

Seeking Guidance

It is not possible to provide detailed guidance for every eventuality. Therefore, where further clarity is needed, the advice of a Senior Manager or the Information Governance Manager should be sought.

Reporting of Breaches

A regular report on breaches of confidentiality of person-identifiable or confidential information shall be presented to the Information Governance Sub Committee and the information will enable the monitoring of compliance and improvements to be made to the policy and procedures.

Appendix D: Legal definition of Confidentiality

Common law jurisdictions have established torts (breaches of duties not under contract with liability for damages) to protect individuals' rights to privacy. A number of common law torts afford protection to individuals' private interests and their confidential information. With regard to the use and disclosure of personal information, or information provided by third party organisations, the tort of breach of confidence is clearly the most relevant. Where the information is created internally and for internal use, the Common law Duty of Confidentiality clearly cannot apply, and then the Common Law Duty of Fidelity becomes the most relevant medium for action.

For something to be confidential, three elements are normally required if, apart from as a result of a contract, a case of breach of confidence is to succeed[1]".

First, the information itself, must "**have the necessary quality of confidence about it**". The information must be of a confidential nature, it cannot be trivial in content[2] "…something which is public property and public knowledge" cannot *per se* provide any foundation for proceedings for breach of confidence. However confidential the circumstances of communication there can be no breach of confidence in revealing to others something which is already common knowledge.

Secondly, that information must have been imparted in circumstances importing an obligation of confidence. The second requirement is that the information must have been communicated in circumstances importing an obligation of confidence, e.g. the doctor patient relationship, many professional relationships have this obligation. However secret and confidential the information there can be no binding obligation of confidence though, if that information is blurted out in public or is communicated in other circumstances which negative any duty of holding it confidential.

Thirdly, there must be an unauthorised use of that information to the detriment of the confider.

Confidence is not absolute and may be breached where:

- If a person has provided consent for the disclosure of their information.
- If there is a legal requirement to disclose information.
- If it is in the public interest to disclose information.

The basis of the public interest test may be summed up as follows "…although the basis of the law's protection of confidence is that there is a public interest that confidences should be

[1] Coco v A.N.Clarke (Engineers Ltd [1969] RPC 41

[2] Saltman Engineering Co. Ltd. v. Campbell Engineering Co. Ltd. (1948) 65 R.P.C. 203;

preserved and protected by the law, nevertheless that public interest may be outweighed by some other countervailing public interest which favours disclosure"[3]

A duty of confidence can also be enshrined in the contracts, to which all employees, are subject. The obligation of confidence may arise by virtue of a contract that imposes duties of confidence, or by the circumstances. In employment contracts, employees are under a fiduciary duty, known as fidelity, to their employers, which imports (or implies) an obligation on their part to refrain from disclosing employers' business to third parties without consent. Similarly, third parties and contractors are equally under a duty as a result of clauses in contracts.

Nothing in this policy will impinge on any rights enshrined in the Public Interest Disclosures Act (1998) or article 10 of the Human Rights Act (1998).

The following types of information are classed as confidential. This list is not exhaustive:

Person-identifiable information is anything that contains the means to identify a person, e.g. name, address, postcode, date of birth, NHS number, National Insurance number etc. Even a visual image (e.g. photograph) is sufficient to identify an individual. Any data or combination of data and other information, which can indirectly identify the person, will also fall into this definition.

Sensitive personal information as defined by the UK General Data Protection (2016) or the Data Protection Act (2018) refers to personal information about:

• Race or ethnic origin

• Political opinions

• Religious or similar beliefs

• Trade union membership

• Physical or mental health or condition

• Sexual life

• Commission or alleged commission of any offence, or

• Any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

Non-person-identifiable information can also be classed as confidential such as confidential business information e.g. financial reports; commercially sensitive information e.g. contracts, trade secrets, procurement information, which should also be treated with the same degree of care.

[3] Attorney General v Guardian Newspapers (No 2)[1990] 1 AC 109

APPENDIX E: GILLICK COMPETANCE / FRASER GUIDELINES

It is a principle of the law in England and Wales, that consent is needed before medical treatment is commenced on a patient. Without the consent of the patient a criminal offence is committed and the patient may bring a civil action against the health-care professional who initiated the treatment. The fact that a patient may be a child, who is under the age of 18 years in English law, does not remove the need for consent to be provided. The Family Law Reform Act [1969] section 8(1) states “The consent of a minor who has attained the age of sixteen years to any surgical, medical or dental treatment which, in the absence of consent, would constitute a trespass to his person, shall be as effective as it would be if he were of full age; and where a minor has by virtue of this section given an effective consent to any treatment it shall not be necessary to obtain any consent for it from his parent or guardian”. However, this provision did not apply to those under 16 years of age.

In 1982 Mrs Victoria Gillick took her local health authority (West Norfolk and Wisbech Area Health Authority) and the Department of Health and Social Security to court in an attempt to stop doctors from giving contraceptive advice or treatment to under 16- year-olds without parental consent. Mrs Gillick had challenged the lawfulness of Department of Health guidance that doctors could provide contraceptive advice and treatment to girls under the age of 16 without parental consent or knowledge in some circumstances. Mrs Gillick lost the case finally in 1985 when the Law Lords upheld the decision in **Gillick v West Norfolk & Wisbech Area Health Authority [1985] UKHL 7 (17 October 1985)**

When trying to decide whether a child is mature enough to make decisions, people often talk about whether a child is 'Gillick competent' or whether they meet the 'Fraser guidelines'. These labels are often used interchangeably but actually relate to separate though related terms,

Gillick competent, according to Mr Justice Woolf (1982); "...*whether or not a child is capable of giving the necessary consent will depend on the child’s maturity and understanding and the nature of the consent required. The child must be capable of making a reasonable assessment of the advantages and disadvantages of the treatment proposed, so the consent, if given, can be properly and fairly described as true consent."*

Therefore the test is that the young person;

- understands the problem and implications
- understands the risks & benefits of treatment
- understands the consequences if not treated
- understands the alternative options
- understands the implications on the family

- is able to retain (remember) the information
- is able to weigh the pros and cons

- is able to make and communicate a reasoned and weighed decision regarding their wishes.

Fraser guidelines are more specific and originally related only to the provision of contraceptive advice, as Lord Fraser (1985) put it; "...*a doctor could proceed to give advice and treatment provided he is satisfied in the following criteria:*

1) that the girl (although under the age of 16 years of age) will understand his advice;

2) that he cannot persuade her to inform her parents or to allow him to inform the parents that she is seeking contraceptive advice;

3) that she is very likely to continue having sexual intercourse with or without contraceptive treatment;

4) that unless she receives contraceptive advice or treatment her physical or mental health or both are likely to suffer;

5) that her best interests require him to give her contraceptive advice, treatment or both without the parental consent." While Fraser was specifically about contraceptive advice and treatment, the case *Axon, R (on the application of) v Secretary of State for Health [2006] EWHC 37 (Admin)* makes clear that the principles apply to decisions about treatment and care for sexually transmitted infections and abortion, too.

The question of whether the provision of such advice to a person below the age of consent would engage the criminal law was answered by “The Sexual Offences Act 2003”. This Act stated that “, a person is not guilty of aiding, abetting or counselling a sexual offence against a child where they are acting for the purpose of:

- protecting a child from pregnancy or sexually transmitted infection,
- protecting the physical safety of a child,
- promoting a child’s emotional well-being by the giving of advice.

This provision therefore permits health professionals and others working with young people to provide confidential advice or treatment on contraception, sexual and reproductive health to young people under 16.

As a general rule applying the tests provided by the Judge in “Gillick” will be sufficient for your decision to be ‘reasonable in all the circumstances of the case’.