	TRUST WIDE DOCUMENT
	Policy
DOCUMENT TITLE	**Confidentiality of Personal Information**
DOCUMENT NUMBER	**ELHT/C077 Version 2.10**
DOCUMENT REPLACES	**Version 2.9**
LEAD EXECUTIVE DIRECTOR DGM	**Director of Finance/SIRO**
AUTHOR	**Head of Information Governance & Data Protection Officer**

TARGET AUDIENCE	All Trust Personnel
DOCUMENT PURPOSE	To outline the approach to the management of confidential personal information
To be read in conjunction with	General Data Protection Regulations (GDPR) Information Security Policy –ELHT/C045
SUPPORTING REFERENCES	• Confidentiality - NHS Code of Practice, November 2003 Data Protection Act 1998 and 2018 • General Data Protection Regulations (GDPR) Information Security Policy – ELHT/C045 V

CONSULTATION		
	Committee/Group	**Date**
Consultation	Information Governance Steering Group	01/03/2023
Approval Committee	Information Governance Steering Group	01/03/2023
Document ratification date	3 March 2023	
NEXT REVIEW DATE	March 2026	
AMENDMENTS	No updates	

Table of Contents

Information Governance 4
Confidentiality 4
The Confidentiality Model 4
General Data Protection Regulations (GDPR) 5
Principles relating to processing of personal data .....
Definition of Personal Data under GDPR .....
The Data Protection Act 6
Data Protection Principles .....
The Caldicott Report 6
Caldicott Principles .....
Common Law Duty of Confidence 7
Responsibilities of all Staff 7
Responsibilities of a Manager 8
Inappropriate Access to Personal Data 9
Additional Laws and Guidance 9
Human Rights Act 1998 .....
The Health and Social Care Act 2001 (sections 60 and 61) .....
Freedom of Information Act 2000 .....
The Computer Misuse Act (1990) .....
Common Law duty of Confidentiality .....
The Environmental Information Regulations 2004 .....
The NHS Care Record Guarantee .....
Legislation Restricting Information Sharing .....
Professional Codes of Conduct/Guidance .....
Monitoring the effectiveness of the policy 12
Appendix 1- Organisational Standards 13
Telephone enquires .....
Use of Fax machines .....
Use of Answer phones .....
Overheard conversations .....
Electronic records .....
Manual Records .....
Transfer of Records .....
Working Away from Trust Premises or the Office Environment .....
Guidance on Disclosure of Personal Information 16
The use of Patient Information .....
Other Personal Information .....
Use of Sensitive Personal Information .....
Disclosures .....
Pseudonymisation General.....
Pseudonymisation Methodology.....
Anonymisation.....
Rights of Individuals 19
Access to Records .....
UK's withdrawal from EU 20
Appendix 2 – Who to Contact Regarding Confidentiality Matters..... 21
Appendix 3 – Equality Impact Assessment.....**22**

1. Information Governance

Information Governance (IG) is Department of Health policy. It provides a framework to bring together all the requirements, standards and best practice that apply to the handling of information in an organisation. One of the aims is to support the provision of high-quality care by promoting the effective and appropriate use of information.

Confidentiality is one part or the information governance agenda along with Information security, Records management, Freedom of Information, and Information Quality Assurance. This policy addresses the organisational approach to Confidentiality, Caldicott and the Data Protection.

2. Confidentiality

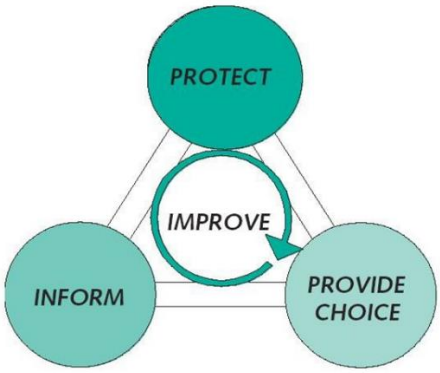
The increasing dependence on information for every aspect of patient care means there is a vast amount of personal information being exchanged between individuals, organisations and countries. The available technology means it is much quicker and easier to exchange information. The introduction of Independent treatment Centre's and Capture Assess and Treat initiatives all means that we need to be more alert to how easy it is for people to access confidential information where they shouldn't.

The NHS is about being open and fair with people – letting them know exactly what is happening regarding their health care and the use of their personal information.

In this environment, it is vital that staff are fully aware of their legal obligations.

2.1. The Confidentiality Model

The Trust will follow the model of confidentiality outlined in the Confidentiality: The NHS Code of Practice



This has four main requirements

1. **PROTECT** – look after the personal information;
2. **INFORM** – ensure that individuals are aware of how their information is used;
3. **PROVIDE CHOICE** – allow individuals to decide whether their information can be disclosed or used in particular ways.
4. **IMPROVE** – always look for better ways to protect, inform, and provide choice. In applying this policy the Trust will ensure that the requirements of the Data Protection Act, General Data Protection Regulations (GDPR), Caldicott principles and common law duty of confidence are complied with.

3. General Data Protection Regulations (GDPR)

3.1. Principles relating to processing of personal data

3.1.1. Personal data shall be:

(a) Processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

(b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) 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 ('accuracy');.

(e) 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 in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

(f) 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').

3.1.2. The controller (Trust) shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

3.2. Definition of Personal Data under GDPR

Personal data is defined as any information relating to a person who can be identified directly or indirectly. This includes online identifiers, such as IP addresses and cookies, if they are capable of being linked back to the data subject. Indirect information might include physical, physiological, genetic, mental, economic, cultural or social identities that can be linked back to a specific individual. There is no distinction between personal data about an individual in their private, public or work roles – all are covered by this regulation

4. The Data Protection Act

- The Data Protection Act 2018 defines how the organisation manages personal data.
  Personal data is information which could identify a living individual.
- It covers all computerised and paper records and in fact can cover all forms of personal information that are recorded i.e. – Biometric, X-rays, CCTV, photographic images.
- To legally store, disclose or use personal information, organisations and person(s) who hold personal information have to comply with the principles of the Act.
- A breach of the Act can carry stiff fines and penalties. In some cases individuals have the right to compensation because of a contravention of the Act.

4.1. Data protection Principles

1. Personal data shall be processed fairly and lawfully.
2. Personal data shall be obtained for only one or more specified and lawful purposes.
3. Personal data shall be adequate, relevant and not excessive.
4. Personal data shall be accurate and where necessary, kept up to date.
5. Personal data shall not be kept longer than is necessary.
6. Personal data shall be processed in accordance with the rights of data subjects.
7. Appropriate technical and organisational measures shall be taken to make personal data secure.
8. Personal data shall not be transferred to countries outside of the European Economic Area unless those countries ensure an adequate level of protection for that data.

When a major service changes or significant changes to use of Person identifiable information is anticipated or planned a Data Protection Impact Assessment (DPIA) should be undertaken to ensure that compliance with the Data Protection Act is being maintained and confidentiality of Person identifiable information upheld

5. The Caldicott Report

Dame Caldicott Committee's Report on the Review of Patient-Identifiable Information in 1997 was commissioned on behalf of the Chief Medical Officer of England. It was undertaken essentially out of concern with the transfer of patient information. It makes a number of recommendations, which are mandatory requirements for NHS organisations to implement.

5.1. Caldicott Principles

The report lists seven core principles to be considered where patient information is used:

1. Justify the purpose - i.e. there has to be a legitimate reason for the transfer of the data.
2. Don't use patient information unless it is absolutely necessary.
3. Use the minimum necessary patient information.
4. Access to patient information should be on a strict need to know basis.
5. Everyone with access to patient information 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.

6. Common Law Duty of Confidence

Personal information is owed a duty of confidence as is the case with most patient-health professional relationships, then this information must not be disclosed unless:

- It is with the consent and knowledge of the individual
- A statute of law dictates the disclosure of the information
- There is an overriding public interest in doing so – this could be for example for a child protection case or to assist the police solve a serious crime

7. Responsibilities of all staff

7.1. Protection of personal information

- You **must** be aware and fully understand your legal obligation to keep personal information obtained through your work confidential
- You **must not** share your computer passwords with anyone
- You **must** be aware who is the nominated Data

Protection/Caldicott lead in the Trust whom you should liaise with regarding confidentiality issues

- You **must** challenge and verify when necessary the identity of any person who is making a request for confidential information and determine the validity of their reason for requiring that information
- You **must** report any actual or suspected breaches of confidentiality to your line manager and use the incident reporting process (IR1 forms)
- When sharing information with others you **must** ensure that it is sent and received securely (especially when using a telephone or fax machine.).
- You **must** ensure that confidential information is appropriately secured when leaving your work area unattended.

7.2. Informing individuals how their information will be used

- Ensure that you are aware of how personal information will be used for patients.
- Ensure wherever possible that consent is obtained for the use of information.

7.3. Provision of Choice

Allow individuals to decide whether their information can be shared, disclosed or used in particular ways and ensure that this is recorded.

NB **Unless in consultation with your line manager and Information Governance Department, it is agreed that information should be given if:**

- A statute of law dictates the disclosure of the information

Or

- There is an overriding public interest in doing so

7.4. Improvement

Identify improvements to the systems and processes

8. Responsibilities of a manager

8.1. Protection of personal information

- Ensure that all staff have basic training in Confidentiality
- Ensure all staff are aware of their responsibilities
- Ensure that appropriate procedures for the safe and secure processing of personal information are maintained
- Ensure that you have operation procedures for the processing of confidential information.
- Maintain records in line with the Trust Record Management policy

8.2. Informing individuals how their information will be used

- Ensure that all staff are aware of how personal information is used
- Ensure all information leaflets contains information on use of Personal information

8.3. Provision of Choice

Ensure all staff are aware of their responsibilities if a patient chooses for their information not to be disclosed or used in particular ways.

8.4. Improvement

- Review systems and Processes regularly to identify better way of working
- Review system and Process in the light of incidents

Any breach of confidentiality must be reported using the Trust Incident reporting policy, all breeches of confidentiality will lead to disciplinary action being considered.

9. Inappropriate Access to Personal Data

Access to any personal data in the work environment must only ever occur when the staff member is working in the context of their professional duties. Staff must never access: -

- Their own record paper or electronic. This should be logged as a request through Information Governance.
- A family member or friend's records. If there is a direct work related requirement (e.g. not checking on a lab result for a relative or their appointment time) for this it must be logged with the staff members manager either before the event or immediately afterwards in an emergency scenario.
- The records of a visiting dignitary or celebrity unless as part of an individual's professional duties
- Any other personal data for which there is no professional work related requirement to do so.

Failure to follow this policy will result in the staff member being referred to Human Resources and a formal investigation being undertaken

10. Additional Laws and Guidance

10.1. Human Rights Act 1998

This sets out basic human rights for individuals, one of which is the right to privacy. Public bodies have to make sure their activities comply with individuals' legal rights**.**

10.2. The Health and Social Care Act 2001 (sections 60 and 61)

Section 60 gives the Secretary of State powers to permit the use of patient information for special cases without necessarily having to obtain patient consent. A recent example of these powers has been to allow confidential

patient information to support activities such as the cancer registries. The Patient Information Advisory Group (outlined in section 61) can advise the Secretary of State on requests that are made to process patient information under section 60.

10.3. Freedom of Information Act 2000

This Act provides a legal right to public information held by public sector organisations.

10.4. The Computer Misuse Act (1990)

Makes it illegal to access data or computer programs without authorisation and establishes three offences:

i. 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 yourself, friends and relatives.
ii. Unauthorised access with the intent to commit or facilitate further offences e.g. to commit fraud or blackmail.
iii. 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. a. Making, supplying or obtaining articles for use in offences i-iii

10.5. Common Law duty of Confidentiality

All staff working in both the public and private sector are aware that they are subject to a common law Duty of Confidentiality and must abide by this. The duty of confidence only applies to identifiable information and not to aggregate data derived from such information or to information that has otherwise been effectively anonymised i.e., it is not possible for anyone to link the information to a specified individual.

The Duty of Confidentiality requires that unless there is a statutory requirement to use information that has been provided in confidence it should only be used for purposes that the subject has been informed about and has consented to. This duty is not absolute but should only be overridden if the holder of the information can justify disclosure as being in the public interest (e.g., to protect others from harm).

10.6. The Environmental Information Regulations 2004

These regulations provide a right of access to environmental information held by public sector organisations.

10.7. The other relevant legislation includes:-

- The Children Act 2004
- Criminal Justice Act 2003
- Criminal Procedures and Investigations Act 1996
- Civil Contingencies Act 2004
- Regulation of Investigatory Powers Act 2000
- Health and Social Care Act 2001 (Section 60)
- Homelessness Act 2002
- Safeguarding Vulnerable Groups Act 2006
- Mental Capacity Act 2005
- Local Government Act 2000
- Digital Economy Act 2017

10.8. 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 NHS Confidentiality Code of Practice and other national guidelines on best practice.

10.9. Legislation Restricting Information Sharing

The following legislation allows information to be shared only between the healthcare professionals actually treating the individual:-

- Human Fertilisation and Embryology (Disclosure of Information) Act 1992
- Venereal Diseases Act 1917 & Venereal Diseases Regulations of 1974 and 1992
- Abortion Act 1967
- The Adoption Act 1976
- The Gender Recognition Act 2004

10.10. Professional Codes of Conduct/Guidance

These include substantial sections on confidentiality. A breach of the Code can mean a health professional being struck off their professional register.

The Nursing and Midwifery Council (NMC), General Medical Council (GMC), British Medical Association (BMA) and other professional bodies all provide guidance on confidentiality.

11. Monitoring Mechanism:

11.1. Monitoring the effectiveness of the policy

Measuring and monitoring compliance with the effective implementation of this procedural document is best practice and a key strand of its successful delivery. Hence, the author(s) of this procedural document has/have clearly set out how compliance with its appropriate implementation will be measured or monitored. This also includes the timescale, tool(s)/methodology and frequency as well as the responsible committee/group for monitoring its compliance and gaining assurance.

An annual report will be prepared reviewing the work of the Information Governance Steering Group (IGSG) and provide an analysis of issues relating to confidentiality reported.

An annual staff survey will be undertaken into understanding of confidentiality issues.

Aspect of compliance being measured or monitored.	Individual responsible for the monitoring	Tool and method of monitoring	Frequency of monitoring	Responsible Group or Committee for monitoring
GDPR compliance	Head of IG/	Audit	Yearly	IGSG
IG Training	Head of IG/DPO	Learning Hub Reports	Monthly	IGSG

Appendix 1- Organisational Standards

Telephone enquires

When telephone enquiries are received asking for disclosure of personal information, the caller should be asked to put their request in writing where applicable. Where requests have to be dealt with more quickly, you must follow these rules:

- You are certain that you can legally disclose the information and that the person who is requesting that information has a legal right to receive it.
- You are certain that the caller is who they say they are, you can do so by carrying out checks such as:
    - If the caller is a patient or an individual for whom the department holds personal information, you must verify personal details that only the caller would know
    - If the caller is part of another organisation, obtain the main switchboard number of that organisation (via phone book or other media) and then ring back
- In all cases you must only provide the minimum amount of information necessary. If in any doubt consult with your line manager.

Use of Fax machines

Fax machines must only be used to transfer personal information where it is absolutely necessary to do so. The following rules **must** apply:

- The fax is sent to a safe location where only staff that have a legitimate right to view the information can access it.
- The sender is certain:
    - That the correct person will receive it
    - That the fax number is correct
- Notify the recipient when you are sending the fax and ask them to acknowledge receipt.
- Care **must** be taken in dialing the correct number.
- Confidential faxes must not be left lying around for unauthorised staff to see.
- Only the minimum amount of information **must** be sent, where possible the data should be anonymised or a unique identifier used instead of personal details.
- Faxes sent **must** include a front sheet, which contains a suitable confidentiality clause

Use of Answer phones

You must only leave a message on a patient or individuals answer phone if it is urgent. If this is the case, leave your name and number only – do not say it is the hospital calling.

All hospital Phones with an answer machine or voicemail must have an appropriate message identifying

- Name, role and department
- Explain if you are to be away from your desk for a long time
- Explain what to do in the event of your message being urgent

Overheard conversations

Where confidential conversations are conducted by staff either over the phone, face to face or in the close proximity of public/receptions areas, care must be taken that personal information is not overheard by persons who do not have a right or need to hear such information. This can also apply where recorded messages are played. Where departments know or feel this is a problem, procedures and techniques should be implemented to minimise the occurrence. Care should be taken when discussing confidential information with patients in patient bays, discussions should be held elsewhere and/or consent sought from the patient to hold in the bay.

Electronic Records

- They should be stored securely in locked rooms or cabinets. It should be noted, however, that emergency out of office hour retrieval procedures have been agreed which allow staff to gain access to records for Accident and Emergency/ Acute admission purposes
- Personal records should only be kept as long as it is deemed necessary.
- Notes that are for destruction, and confidential waste must be destroyed using a secure method such as shredding or incineration
- Confidential information such as patients' records must not be left lying around in accessible areas such as reception desks where they may be viewed by person(s) unauthorised to do so

Manual Records

- They should be stored securely in locked rooms or cabinets. It should be noted, however, that emergency out of office hour retrieval procedures have been agreed which allow staff to gain access to records for Accident and Emergency/ Acute admission purposes
- Personal records should only be kept as long as it is deemed necessary.
- Notes that are for destruction, and confidential waste must be destroyed using a secure method such as shredding or incineration
- Confidential information such as patients' records must not be left lying around in accessible areas such as reception desks where they may be viewed by person(s) unauthorised to do so

Transfer of Records

- Every care should be taken transferring confidential records both internally and externally, ensuring that envelopes are sealed, addressed correctly (addresses should include a named person and title, department and location) and be clearly marked "private and confidential"
- When re-using transit or previously used envelopes previous addresses need to be deleted to ensure the records reach their correct destination

Transfer of confidential personal information, outside the Trust must not be made via the Internet/e- mail unless a secure means of transfer is used. This would be via NHS.net email or use of encryption when using ELHT email. If you would like further guidance please contact the IG team.

Working Away from Trust Premises or 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 ELHT 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 Trust premises is discouraged unless required to carry out Trust duties.

When working away from ELHT locations staff must ensure that their working practice complies with ELHT's policies and procedures.

Any removable media must be encrypted as per the current Encryption Guidance.

To ensure 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.

Staff must minimise the amount of person-identifiable that is taken away from Trust premises.

If staff members 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 Trust buildings.

- Confidential information is kept out of sight whilst being transported.

If staff members 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.

Guidance on Disclosure of Personal Information

Staff can legally use and disclose personal information in a number of situations, this section summarises some of the areas where this can happen.

The use of Patient information

Trusts and health care staff hold and use a great deal of personal information, the majority of which will be patient based. The obvious and justifiable reason for the use of patient records is that it is an essential component in the provision of healthcare for the patient. This will allow the relevant health professionals to view and share this information with other health professionals where necessary. Additionally, it will be feasible for other staff such as administrative and clerical staff to access the appropriate sections of the information in order to carry out the necessary functions that contribute towards that healthcare process, i.e. arrange outpatient appointments or to update details of patient records. Personal information which has been collected to provide patient care shouldn't be used for other purposes such as research, and education without the consent of the patient. Consent is appropriate if you can offer people real choice and control over how you use their data. The GDPR gives a specific right to withdraw consent. You need to tell people about their right to withdraw, and offer them easy ways to withdraw consent at any time. Keep records to evidence consent – who consented, when, how, and what they were told and keep consents under review and refresh them if anything changes. If you require any further guidance on this, please contact the IG team.

Other personal information

Personal information which doesn't contain patient details will also be used in healthcare organisations (such as personnel and finance information). This will be permissible where the use is a necessary contribution to the overall aim of that NHS organization i.e. the provision of healthcare. An example of this is:

Finance needs certain personal details in order to pay staff who in turn will contribute directly or indirectly to the organisation's healthcare process

Use of sensitive personal information

The Data Protection Act classes certain personal information as sensitive; this could be where it contains details about:

- Criminal convictions
- Physical or mental health condition
- Political opinions
- Racial or ethnic origin
- Religious beliefs
- Sexual life
- Trade Union membership

The GDPR defines special classes of information which are equivalent to sensitive data as defined by the Data Protection Act:

- Data revealing racial or ethnic origin
- Political opinions
- Religious or philosophical belief
- Trade union membership
- Processing of genetic data, biometric data for the purpose of uniquely identifying a natural person
- Data concerning health
- Data concerning a natural person's sex life or sexual orientation

Where you use this type of sensitive or special information you must be certain they have a justifiable reason to do so.

Disclosures

Where a patient's information is being considered for disclosure outside of the immediate healthcare environment, or to a person or place they would not have anticipated, then the consent of the individual must be sought or appropriate legal gateway, under the Data Protection Act or General Data Protection Regulation, identified to allow the disclosure. A Data Protection Impact Assessment (DPIA) must be completed and Data Sharing Agreement (DSA) if required.

It must be appreciated however there may be occasions where confidentiality is not absolute and it could be essential that it be breached. This may be appropriate where it becomes necessary to protect an individual from harm such as in a child protection case or personal information is required for a serious crime investigation.

Also, a stature of law might allow a disclosure without consent for example - **The Public Health Act 1984** stipulates that designated NHS staff need to notify the relevant authority where a person is suspected of contracting a notifiable disease.

When these types of disclosures are made without consent, then the reason for doing so and who made the decision to disclose must be documented.

Pseudonymisation

General

It is both NHS policy and a legal requirement that when patient data is used for purposes not involving the direct care of the patient, the data subject should not be identified unless other legal means hold, such as consent.

The NHS Confidentiality Code of Practice states the need to 'effectively anonymise' patient data prior to the non-direct care usage being made of the data.

Pseudonymisation is a technique that replaces or removes information in a data set that identifies an individual.

The GDPR defines pseudonymisation as:

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.

Pseudonymised data is still classed as personal data and must therefore be treated as such.

Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information, should be considered to be information on an identifiable natural person

Staff must only have access to the data that is necessary for the completion of the business activity which they are involved in. This applies to the use of Personal Identifiable Data (PID) for secondary or non-direct care purposes. By de-identification users are able to make use of patient data for a range of secondary purposes without having to access the identifiable data items. The PID must be stored within a new Safe Haven environment which only limited staff can access.

Data itself cannot be labelled as primary or secondary use data; it is the purpose of the disclosure and the usage of the data that is either primary or secondary. This means that it is legitimate to hold data in identifiable form, but it becomes essential to ensure that only authorised users are able to have identifiable data disclosed to them.

Pseudonymisation is a method which disguises the identity of patients by creating a pseudonym for each patient identifiable data item. This allows patient linking analysis needed within secondary uses.

Pseudonymisation is a core element of Secondary Uses Services (SUS) and should be applied across the Trust. Pseudonymisation should be applied to data held within a secure database.

Pseudonymisation methodology

When pseudonymisation techniques are consistently applied, the same pseudonym is provided for individual patients across different data sets and over time. This allows the linking of data sets and other information which is not available if the PID is removed completely.

To effectively pseudonymised data the following actions must be taken

- Each field of PID must have a unique pseudonym
- Pseudonyms to be used in place of NHS numbers and other fields that are to be used by staff must be of the same length and formatted on output to ensure readability. For example, in order to replace NHS numbers in existing report formats, then the output pseudonym should generally be of the same field length, but not of the same characters; i.e., 5L7 TWX 619Z. Letters should be

used within the pseudonym for an NHS number to avoid confusion with original NHS numbers
- Consideration needs to be given to the impact on existing systems both in terms of the maintenance of internal values and the formatting of reports
- Pseudonyms for external use must be generated to give different pseudonym values in order that internal pseudonyms are not compromised
- The secondary use output must only display the pseudonymised data items that are required. This is in accordance with the Caldicott guidelines
- Pseudonymised data should have the same security as PID

Anonymisation

This is information which does not identify an individual directly, and which cannot reasonably be used to determine identity. Anonymisation does not allow information about the same individual to be linked in the same way that Pseudonymisation does. Anonymisation is more likely to be used for 'one off' queries of data.

The GDPR does not apply to personal data that has been anonymised. Recital 26 explains that:
The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.

Rights of Individuals

Access to Records
Individuals have the right under the Data Protection Act to have access to the personal records that the Trust hold on them (this will of course include patient's health records). This can involve the Trust providing copies or sight of records to individuals. There may be charges made for this access. Contact the Health Records Department (Health Records access team).

Please be aware, everything you record about an individual, be it a patient/client/complainant etc. in paper or electronic records can be requested by that individual (or their representative).

Individuals also have rights:

- To object to their information being used in certain circumstances.
- To withhold consent to share their information.
- To request that an organisation or persons who has inaccurate data held on them has it rectified, erased or deleted
- To claim compensation where a breach of the Act has caused the data subject to suffer damage or distress

UK's withdrawal from the EU

From the 1st January 2021 the UK is no longer a member of the European Union, from this date no Personal Identifiable information should be transferred outside the United Kingdom If further information is required please contact IG.Issue@elht.nhs.uk for further advice.

Appendix 2 – Who to Contact Regarding Confidentiality Matters

Trust Caldicott Guardian	Medical Director Trust HQ Royal Blackburn Hospital
Lead Trust Director	Director of Finance / Senior Information Risk Owner Trust HQ, Royal Blackburn Hospital
Information Governance and Data Protection Officer	Head of Information Governance & Data Protection Officer, Information Governance Royal Blackburn Hospital
Records Management	Health Records Manager Clinical Outpatients & Administration Directorate Royal Blackburn Hospital
Subject Access	Freedom of Information/Subject Access and Request Officer Information Governance Royal Blackburn Hospital
Information Security Officer	Head of ICT Services Birch House Royal Blackburn Hospital
Head of Legal Services	Head of Legal Services Quality and Safety Unit Royal Blackburn Hospital

Appendix 3 Equality Impact Assessment Screening Form

Department/Function	Information Governance Department			
Lead Assessor	Head of Information Governance/Data Protection Officer			
What is being assessed?	Impact of document on equality			
Date of assessment	01/03/2023			
What groups have you consulted with? Include details of involvement in the Equality Impact Assessment process.	Equality of Access to Health Group	☐	Staff Side Colleagues	☐
	Service Users	☐	Staff Inclusion Network/s	☒
	Personal Fair Diverse Champions	☐	Other (Inc. external orgs)	☒
	Please give details: Information Governance Steering Group			

1) What is the impact on the following equality groups?		
Positive: ➢ Advance Equality of opportunity ➢ Foster good relations between different groups ➢ Address explicit needs of Equality target groups	**Negative:** ➢ Unlawful discrimination, harassment and victimisation ➢ Failure to address explicit needs of Equality target groups	**Neutral:** ➢ It is quite acceptable for the assessment to come out as Neutral Impact. ➢ Be sure you can justify this decision with clear reasons and evidence if you are challenged

Equality Groups	**Impact** (Positive / Negative / Neutral)	**Comments** ➢ Provide brief description of the positive / negative impact identified benefits to the equality group. ➢ Is any impact identified intended or legal?
Race (All ethnic groups)	Neutral	
Disability (Including physical and mental impairments)	Neutral	
Sex	Neutral	
Gender reassignment	Neutral	
Religion or Belief	Neutral	
Sexual orientation	Neutral	
Age	Neutral	
Marriage and Civil Partnership	Neutral	
Pregnancy and maternity	Neutral	
Other (e.g. caring, human rights)	Neutral	

2) In what ways does any impact identified contribute to or hinder promoting equality and diversity across the organisation?	N\A

3) If your assessment identifies a negative impact on Equality Groups you must develop an action plan **to avoid discrimination and ensure opportunities for promoting equality diversity and inclusion are maximised.**

- This should include where it has been identified that further work will be undertaken to further explore
- the impact on equality groups
- This should be reviewed annually.

Action Plan Summary

Action	**Lead**	**Timescale**
n/a		