healthshare

Data Protection, Caldicott and Confidentiality Policy

Policy Domain	IMG
Policy ID	IMG 005
Version Number	10
Author	Les De-Lara
Job Title	Information Governance Lead
First Release Date	04/01/2011
Ratification Date	17/09/2021
Ratified By	IT Steering Group
Implemented By	IT Steering Group
Audit and Review By	IT Steering Group
Review Frequency	Triennial
Last Review Date	10/08/2021
Next Review Date	01/08/2024

Table of Contents

REVISION SUMMARY

Version	Comments	Author	Date
V 1	Implementation of new policy	IT Manager	03/01/2011
V 2	Updated with IG Training Tool	IT Manager	01/03/2011
V 3	Policy Code Change	IT Manager	01/08/2012
V 4	Review and update.	IT Manager	01/10/2013
V 5	Review and updated	IT Manager	01/10/2014
V 6	Review and updated	IT Manager	01/10/2015
V 7	Review and updated	IT Manager	01/01/2017
V 8	Amalgamated policies	IT Manager	01/05/2018
V 9	Review and updated	IM&G Manager	01/04/2020
V 10	Review and updated	IG Lead	10/08/2021

1 STATEMENT OF PURPOSE

This document describes Healthshare's policy on Data Protection Act (DPA) and General Data Protection Regulations (GDPR), NHS Code of Confidentiality and Caldicott requirements, and employees' responsibilities for the safeguarding of confidential information held both manually (non-computer in a structured filing system) and electronically.

Healthshare holds and manages a great deal of personal and confidential information relating to patients, service users and staff.

Data protection laws exist to strike a balance between the rights of individuals to privacy and the ability of organisations to use data for legitimate business purposes.

The Data Protection Act 2018 come into force in 2018 and replaced the Data Protection Act 1998. The regulations are concerned with "personal and sensitive data" about living, identifiable individuals which is "automatically processed or manually stored as part of a relevant filing system or accessible record". It need not be particularly sensitive information; indeed, it can be as little as a name and address.

GDPR Regulations are divided to "Recitals" and "Articles" and works in two ways, giving individuals certain rights whilst requiring those who record and use personal information certain responsibilities. The Regulations incorporates 6 principles (see para 6.1), which are binding for all organisations processing data.

This policy applies to all staff, because:

ALL STAFF HAVE A LEGAL DUTY TO PROTECT THE PRIVACY OF INFORMATION ABOUT INDIVIDUALS

2 RATIONALE

Data Protection and Confidentiality are legal requirements on all staff working for Healthshare.

This policy provides the framework to ensure that Healthshare complies with the requirements of the General Data Protection Regulations (GDPR), Data Protection Act 2018 (DPA 2018), Caldicott Principles and NHS Code of Confidentiality.

GDPR brings in a new "principle" of "transparency and accountability". This means that Data Controllers and Data processors (i.e., Healthshare) has to ensure that Data Subjects (i.e., public; patients; staff) are aware of the processing of their personal data – and this information is readily available to them. To achieve this, Healthshare public and staff intranet websites have been updated with Privacy notices.

As a private company, Healthshare does not always rely on "consent" to process Data Subject's information.

However, staff should always consider gaining consent from patients when considering whether to share information (i.e., further processing). Consent to share information should be recorded in the patient's clinical record keeping system and/or tracker as appropriate.

Staff must respect a Data Subject's right to confidentiality and must not access patient or staff information on any system (electronic or paper) that relates to family (including spouses; children; parents etc.) or friends, even if it is considered to be within their role in the organisation. Staff must ensure that they have a good reason for accessing any patient data. Healthshare audits this and failure to comply could result in disciplinary action.

If staff require advice or support on any Data Protection or Confidentiality matter, they should contact the Information Governance Lead using the email IG@Healthshare.org.uk in the first instance, who may escalate the issue to either the Data Protection Officer or Caldicott Guardian if required.

3 SCOPE

This policy covers all identifiable information created, processed and stored on living individuals, patients or staff. Throughout this document the term "patient" is used to refer to an individual who is receiving a service from Healthshare, and this term includes those people who are also known as "Service Users", and "Clients". Similarly, the terms "clinician" and "health professional" are used, these may be Physiotherapists, Radiologists, Sonographers, Radiographers, General Practitioners etc.

Although the UK is now "a third country" under the EU's GDPR (i.e., a country outside of the EU without an adequacy decision), a provision in the agreement signed by the UK and EU in December 2020 secures an interim period of six months of unrestricted data flow between the two blocs.
On June 28, 2021, the EU adopted **an adequacy decision for the UK**, ensuring the free flow of personal data between the two blocs for a four-year period (until June 2025).

For UK websites, companies and organizations processing personal data from individuals inside the EU, this UK adequacy decision means unrestricted business-as-usual for the next four years.
After June 2025, the EU will have to engage in a new adequacy process to determine whether the UK still ensures an equivalent level of data protection for the adequacy decision to be renewed.

Healthshare is committed to protecting the information it holds and safeguarding all activities carried out both on and off any of its premises by Third Parties in accordance with its legal duty as a data controller and data processor under the Data Protection Act 2018 (DPA 2018) and the General Data Protection Regulations (GDPR).

The importance of robust Information Governance has risen rapidly in recent years following the ongoing concerns related to security and confidentiality of Public Sector data and the increased enforcement powers assigned to the Information Commissioner's Office.

It is paramount that all departments and individuals protect Healthshare's information assets in line with policy and standards of European and UK legislation.

This Policy has been produced in recognition of the need to provide clear and unambiguous confidentiality and information security requirements to Third Parties who may process information on behalf of Healthshare or potentially have access to Healthshare's information assets and must be adhered to by Healthshare when engaging Third Parties. These requirements are reflected within the NHS Data Security Protection Toolkit (DSPT).

This Policy should be read in conjunction with the Information Governance Policy including the Management of Risks Policy. Any questions of interpretation within this policy must be raised immediately with the Senior Information Risk Owner (SIRO) or Information Governance Lead.

4 DEFINITIONS

4.1 The General Data Protection Regulations (GDPR) 2016

This provides controls on the handling of personal identifiable information for all European living individuals. Central to the Act is compliance with the principles (above), designed to protect the rights of individuals about whom personal data is processed whether an electronic or a paper record.

4.2 Data Protection Act (DPA) 2018

The Data Protection Act 2018 is a United Kingdom Act of Parliament which updated data protection laws in the UK. It is a national law which complements the European Union's General Data Protection Regulation and replaces the Data Protection Act 1998.

4.3 The Access to Health Records Act 1990

The Access to Health Records Act 1990 provides controls on the management and disclosure of health records for deceased patients. Thus, the personal representative of the deceased or a person who might have a claim arising from the patient's death can apply to request access to the files.

4.4 The Caldicott Report 1997

This provides guidance on the use and protection of personal confidential data, and emphasises the need for controls over the availability of such information and access to it. It makes a series of recommendations, which led to the requirement for all NHS organisations or those such as Healthshare who have contracts with the NHS to appoint a Caldicott Guardian who is responsible for compliance with the six (original) Caldicott confidentiality principles.

A review of the Caldicott Principles took place during 2012, Chaired by Dame Fiona Caldicott. The report "The Information Governance Review – To share or not to share" was published in April 2013, which included an added Principle. The recommendations from the report were ratified by the Government in September 2013.

4.5 The Common Law Duty of Confidentiality

This law prohibits use and disclosure of information, provided in confidence unless there is a statutory requirement or court order to do so. Such information may be disclosed only for purposes that the subject has been informed about and has consented to, provided also that there are no statutory restrictions on disclosure. 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, for example, to protect the vital interests of the data subjects or another person, or for the prevention or detection of a serious crime.

4.6 NHS Code of Confidentiality (2003)

The NHS Code of Confidentiality (2003) provides the standards and framework that all staff working within the NHS or as Healthshare, who have contracts with the NHS and must adhere to this.

5 RESPONSIBILITIES

5.1 Board Responsibility

The Board defines Healthshare's policy in respect of Information Governance taking into account legal and NHS requirements. The Board is also responsible for ensuring that sufficient resources are provided to support the requirements of the policy.

5.2 IT Steering Group (ITSG)

The ITSG is chaired by the IT Applications and Data Lead and is the forum responsible for ensuring that Healthshare complies with the GDPR/DPA 18. It meets fortnightly – and SIRO who is a member reports to the Healthshare Board.

5.3 The Senior Information Risk Officer (SIRO)

SIRO has ultimate responsibility for the management and mitigation of risks associated with the Healthshare Group information management processes. The SIRO shall:

- Be accountable for the management and protection of all Information Assets.
- Take overall ownership of the Information Risk Management Policy.
- Provide a focal point for managing information risks and incidents.
- Lead on Business Continuity in the context of Information Risk.
- Act as champion for Information Risk on the Board.
- Advise the Board on the effectiveness of Information Risk Management.
- Ensure that Information Risk Assessments and management processes are embedded.
- Lead and foster a culture for protecting and using information and data.
- Lead communications on Information Governance and Security throughout the organisation.
- Meet on a quarterly basis with the IG Lead.
- Attend the Healthshare IT Steering Group.

5.4 The Caldicott Guardian

The Caldicott Guardian is responsible for ensuring that Caldicott principles are followed. Caldicott Guardian is an advisory role and acts as the conscience of the Healthshare group, actively supporting work to facilitate and enable information sharing, and advising on options for lawful and ethical processing of information as required. Further information can be found, but it is important to understand what the Guardian shall do to promote a focal point for patient confidentiality and information sharing issues.

5.5 The Data Protection Officer (DPO)

The primary role of the DPO is to ensure that Healthshare processes the personal data of its staff, patients, providers or any other individuals (also referred to as data subjects) in compliance with the applicable data protection rules. The DPO is the first point of contact for the Information Commissioner's Office (ICO), who are the Regulatory body for data protection.
The DPO attends the IT Steering Group, and also has a trained Deputy to cover in case of absence.

5.6 The Information Governance (IG) Lead

The IG Lead has responsibility for providing guidance on all areas of Information Governance, ensuring relevant legislation and guidance are incorporated into the Healthshare Group practice via the IT Steering Group.

- To support the overall development, management and delivery of Information Governance Strategy and work programme, to assist the DPO, SIRO and Caldicott Guardian.
- To provide support on issues related to Data Protection and maintenance of Healthshare's Data Protection Registration. Assisting SIRO, ensuring that all staff are aware and understand their responsibilities in respect of Data Protection and the confidentiality of personal identifiable information.
- To co-ordinate, publicise and monitor standards of information handling throughout Healthshare. To be responsible for answering first line enquiries and provide advice, guidance and interpretation on matters relating to Information Governance.
- To play a full part in the Information Governance agenda and to be an integral part of the Governance framework.
- Attend the IT Steering Group meeting.

5.7 Information Asset Owners

The SIRO will ensure that there is a framework of identified Senior Information Asset Owners, Operation Directors who are individually responsible for ensuring that the Healthshare Group policy and information security principles shall be implemented, managed and maintained in their business areas. This includes:

- Appointment of Information Asset Owners (IAO) who are responsible for Information Assets in their area(s) of responsibility.
- Awareness of information security risks, threats and possible vulnerabilities within the business area and complying with relevant policies and procedures to monitor and manage such risks.
- Supporting personal accountability of users within the business area(s) for Information Security.
- Ensuring that all staff under their management have access to the information required to perform their job function within the boundaries of this policy and associated policies and procedures.

Senior Information Asset Owners will ensure that there are senior/responsible individuals (e.g., Operational Managers, Heads of Departments) who are directly involved in running the business are identified as Information Asset Assistants and shall be responsible for:

- Understanding what information is held.
- Knowing what is added and what is removed.
- Understanding how information is moved.
- Knowing who has access and why.

5.8 Managerial Accountability and Responsibility

All line managers from all operational and corporate services within The Healthshare Group are responsible for ensuring that the policy and its supporting strategy, standards, procedures and guidelines are built into local processes and there is ongoing compliance.

5.9 Individual Responsibility

Every individual staff member (both permanent and temporary) and contractors are responsible for ensuring they are aware of the requirements incumbent upon them and for ensuring they comply with these on a day-to-day basis. Any staff member who does not comply with this policy, or breaches the confidentiality of patients/staff, will be subject to Disciplinary Procedures as per Healthshare Group policy, which may result in their dismissal, and if professionally registered, reported to their professional body.

6 MAIN CONTENT

The General Data Protection Regulations (GDPR)/Data Protection Act (DPA 2018). Principles and Practices to ensure compliance.

6.1 GDPR Article 5: Data Protection 6 Principles

- Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject [lawfulness, fairness and transparency].
- Personal data shall be collected only for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with those purposes [purpose limitation].
- Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed [data minimisation].
- Personal data processed shall be accurate and, where necessary, kept up to date [accuracy].

- 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 [storage limitation].
- 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 of organisation measures [integrity and confidentiality].

6.2 Under the GDPR/DPA 18, data subjects have certain rights, which must be upheld

- **Be informed** - through privacy notices and Data Protection Impact Assessments.
- GDPR Article 13 – **Right of Access** – via Subject Access Requests.
- GDPR Article 16 - **Rectification** - to have inaccuracies corrected. However, it should be noted that diagnosis and clinical opinion is a matter of clinical judgement and cannot be changed solely at the patient's request.
- GDPR Article 17 – **Right to Erasure** - to have information erased (right to be forgotten). This right is not absolute and only applies in certain circumstances.
- GDPR Article 21 - **Object to processing** Article 21 of the GDPR gives individuals the right to object to the processing of their personal data at any time. This effectively allows individuals to stop or prevent Healthshare from processing their personal data. An objection may be in relation to all of the personal data we hold about an individual or only to certain information. It may also only relate to a particular purpose Healthshare is processing the data for.

The right to object only applies in certain circumstances. Whether it applies depends on the purposes for processing and Healthshare's lawful basis for processing.

Healthshare can refuse to comply if:

- Healthshare can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual (which in this case may include a clinical risk assessment of the individual's circumstances).
- The processing is for the establishment, exercise or defence of legal claims.

In these circumstances, if the individual is objecting to having clinical information kept in an electronic format, (i.e., in SystmOne or Soliton) then this should be raised with the IG Lead via email: ig@healthshare.org.uk who will support the team to manage the process. Ultimately, it is the decision of the Caldicott Guardian whether the objection is to be upheld or refused, depending on the clinical circumstances.

- Prevent automated decision-making and profiling.
- Data portability – have information provided in electronic format and not hinder the data subject's transmission of personal data to a new data controller.
- Consent to process - silence, pre-ticked boxes or inactivity does not constitute consent to process.

6.3 Privacy Notice

GDPR requires data controllers to provide certain information to people whose data they hold and use; this is known as a Privacy Notice. Healthshare publishes its Privacy Notice on the Healthshare Public Website: https://healthshare.org.uk/privacy/

6.4 Lawful/legal basis for processing

GDPR/DPA 2018 requires that Healthshare identify the legal basis for any processing (i.e., collecting, using, storing etc.) of personal or special category information relating to data subjects (patients, staff and suppliers).

For more information relating to lawful basis – refer to Appendix A.

6.5 Caldicott Principles for handling personal confidential data

6.5.1 Justify the purpose(s)

Every proposed use or transfer of personal confidential data within or from Healthshare should be clearly defined and scrutinised, with continuing uses regularly reviewed, by an appropriate Guardian.

6.5.2 Don't use personal confidential data unless it is absolutely necessary

Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

6.5.3 Use the minimum necessary personal confidential data

Where the use of personal confidential data is considered to be essential, the inclusion of each individual item of information should be considered and justified so that the minimum amount of identifiable information is transferred or accessible as is necessary for a given function to be carried out.

6.5.4 Access to personal confidential data should be on a strict need-to-know basis

Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one information flow is used for several purposes.

6.5.5 Everyone with access to personal confidential data should be aware of their responsibilities

The organisation must ensure that those handling personal confidential data, both clinical and non-clinical staff, are made fully aware of their responsibilities and obligations to respect patient confidentiality.

6.5.6 Understand and comply with the law

Every use of personal confidential data must be lawful. The Caldicott Guardian is responsible for ensuring that Healthshare complies with legal requirements.

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

Clinical professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

The Health and Social Care (Safety and Quality) Act 2015 includes a legal duty requiring health and adult social care bodies to share information where this will facilitate care for an individual. [Refer to IMG 028 Data Sharing Policy for details.]

6.6 The 'Confidentiality: NHS Code of Practice'

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/200146/Confidentiality_-_NHS_Code_of_Practice.pdf was published by the Department of Health following major consultation

in 2002/2003. The Code of Practice is a guide to required practice for those who work within or under contract to NHS organisations concerning confidentiality and patients' consent to the use of their health records. This document uses the term 'staff' a convenience to refer to all those to whom this code of practice should apply. Whilst directed at NHS staff, the Code is also relevant to any one working in and around health services. This includes local authority staff working in integrated teams and private and voluntary sector staff.

This document:

- Introduces the concept of confidentiality.
- Describes what a confidential service should look like.
- Provides a high-level description of the main legal requirements.
- Recommends a generic decision support tool for sharing/disclosing information.
- Lists examples of particular information disclosure scenarios.

Following the publication of the Caldicott Review in March 2013, the Health & Social Care Information Centre published "A guide to confidentiality in health and social care" which identified five rules for treating confidential information with respect:

- Rule 1: Confidential information about service users or patients should be treated confidentially and respectfully.
- Rule 2: Member of a care team should share confidential information when it is needed for the safe and effective care of an individual.
- Rule 3: Information that is shared for the benefit of the community should be anonymised.
- Rule 4: An individual's right to object to the sharing of confidential information about them should be respected.
- Rule 5: Organisations should put policies, procedures and systems in place to ensure the confidentiality rules are followed.

The full version is available here:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf

6.7 Patient Confidentiality

Health information is collected from patients in confidence and attracts a common law duty of confidence until it has been effectively anonymised. This legal duty prohibits information use and disclosure without consent – effectively providing individuals with a degree of control over who sees information they provide in confidence. This duty can only be overridden if there is a statutory requirement, a court order, or if there is a robust public interest justification.

As a research discovering organisation staff might screen patients' records to identify any potential research participants with the Consultants permission. Patients may also be approached by staff regarding participation in a particular research study in order to obtain consent.

In the event of the patient being unable to give permission the Mental Capacity Act 2005 must be followed. Staff should refer to the Mental Capacity Act Policy and procedures for detail.

In all cases, the wishes expressed must be appropriately documented in the patient's clinical records.

6.8 Staff Confidentiality

All staff are required to keep confidential any information regarding patients and staff, only informing those that have a need to know. In particular, telephone conversations and electronic communications should be conducted in a confidential manner.

Confidential information must not be disclosed to unauthorised parties without prior discussion and confirmation with a senior manager in Healthshare. Staff must not process any personal information in contravention of the GDPR/DPA 2018.

Staff must not access patient or staff information on any system (electronic or paper) that relates to family (including spouses; children; parents etc.) or friends, even if it is considered to be within their role in Healthshare. Any breaches of these requirements will potentially be regarded as serious misconduct and as such may result in disciplinary action.

All staff have a confidentiality clause in their contract of employment. Healthshare has an approved Data Protection and Confidentiality clause in all contracts with 3rd party contractors and suppliers who process personal information.

6.9 Exemptions to confidentiality

In certain circumstances personal information may be disclosed and guidance is below. However, it is vital in each case that staff make an assessment of the need to disclose the information and document that the information has been released to whom and for what reason. If they are in any doubt, they should seek advice from their Team Manager/Senior Clinician or the IG Lead.

6.10 Disclosing Information against the Subject's wishes

The responsibility to withhold or disclose information without the data subject's consent lies with the senior manager or senior clinician involved at the time and cannot be delegated.

Circumstances where the subject's right to confidentiality may be overridden are rare. Examples of these situations are:

- Where the subject's life may be in danger, or cases in which s/he may not be capable of forming an appropriate decision.
- Where there is serious danger to other people, where the rights of others may supersede those of the subject, for example a risk to children or the serious misuse of drugs.
- Where there is a serious threat to the healthcare professional or other staff.
- Where there is a serious threat to the community.
- In other exceptional circumstances, based on professional consideration and consultation.

The following are examples where disclosure without consent is required:

- Births and deaths - National Health Service Act 1977
- Notifiable communicable diseases - Public Health (Control of Diseases) Act 1984
- Poisonings and serious accidents at the work place - Health & Safety at Work Act 1974
- Terminations - Abortion Regulations 1991
- Child abuse - Children’s Act 1989 and The Protection of Children Act 1999
- Drug Addicts - Drugs (Notification of Supply to Addicts) Regulations 1973
- Road traffic accidents - Road Traffic Act 1988
- Prevention/detection of a serious crime e.g., terrorism, murder - The Crime and Disorder Act 1998

If in doubt, staff should seek guidance, in confidence, from the senior Clinician or the appropriate Senior Manager or the IG Lead.

Healthshare will support any member of staff who, after using careful consideration, professional judgement, and has sought guidance from their manager, can satisfactorily justify and has documented any decision to disclose or withhold information against a patient's wishes.

6.11 Non–Disclosure of personal information contained in a health record

An individual requesting access to their health records may be refused access to parts of the information if an appropriate clinician deems exposure to that information could cause physical or mental harm to the data subject or a third party. Clinicians should be prepared to justify their reasons in a court of law if necessary. In all cases reasons for non-disclosure must be documented.

Where access would disclose information relating to or provided by a third party, consent for release must be sought from the third party concerned, unless that third party is a health professional who had provided the information as part of their duty of care. Where the third party does not consent, the information may be disclosed provided the identity of the third party is not revealed. The Information Commissioner's Code of Practice suggests that this might be done by omitting names and identifying particulars from the records. Care should be taken to ensure that the information if released is genuinely anonymous.

The Information Commissioner's Guide provides guidance on issues of law concerning the right of access to personal data – in particular their website *Right of access/subject access requests and other rights*.

6.12 Personal Identifiable Data in Medical Research

All project-based research within Healthshare must comply with the Data Protection & Caldicott Guardian Principles as set out within this Policy and to be prepared to provide assurance to Healthshare, our patients and the public that all research meets the necessary legal and compliance standards.

6.13 Data Protection Impact Assessment Procedure

All projects and processes that involve processing personal information or intrusive technologies give rise to privacy issues and concerns. To enable Healthshare to address the privacy concerns and risks the GDPR/DPA 2018 requires a Data Protection Impact Assessment (DPIA) be completed, and signed off by the Data Protection Officer or the Information Governance Lead.

7 STAFF TRAINING

Training will be supported and monitored through the Healthshare Group induction programme, by clauses in employment contracts, personal development plans, professional codes of conduct and the Healthshare Group training (for example, via the NHS *e-Learning for Health* platform).

Permanent new staff will receive information governance training as part of their Induction via an on-line eLearning package. Face to face, bespoke training is also available on request from the Information Governance Lead or external providers to meet learning needs. All staff must pass the Information Governance Training before being able to access any personal data.

Annual mandatory on-line e-learning Information Governance training is required for all employed staff (both permanent and temporary). This is available from the NHS on-line training tool. Facilitated face to face sessions are available on request from the Information Governance Lead for staff who do not have access to a computer or require additional training support.

In addition, some roles are required to complete additional annual training, (e.g., the Data Protection Officer and their Deputy, SIRO, Caldicott Guardian and IG Lead).

8 MONITORING AND COMPLIANCE

Monitoring/audit arrangements	Methodology	Reporting		
		Source	Committee	Frequency
100% of all staff complete General Data Protection e-learning modules on an annual basis	Review training data	E-learning system	IT Steering Group	Annual
All staff are aware of General Data Protection processes in induction	Review of Induction checklists	Induction Data	IT Steering Group	Annual

9 EQUALITY IMPACT STATEMENT

During the development of this policy the Company has considered the needs of each protected characteristic as outlined in the Equality Act (2010) with the aim of minimising and if possible, remove any disproportionate impact on employees for each of the protected characteristics, age, disability, gender, gender reassignment, pregnancy and maternity, race, religion or belief, sexual orientation.

If staff become aware of any clinical exclusions that impact on the delivery of care an incident form would need to be completed and an appropriate action plan put in place.

9.1 Equality Impact Assessment

The Company aims to design and implement services, policies and measures that meet the diverse needs of our service, population and workforce, ensuring that none are placed at a disadvantage over others. The Equality Impact Assessment tool assesses the impact of this policy.

		Yes/No	Comments
1.	Does the document/project affect any group less or more favourably than another on the basis of:		
	• Disability	No	
	• Sex	No	
	• Race	No	
	• Age	No	
	• Gender Reassignment (including transgender)	No	
	• Sexual orientation	No	
	• Pregnancy & Maternity	No	
	• Other identified groups	No	

2.	Is there any evidence that some groups are affected differently?	No	
3.	If you have identified potential discrimination, are there exceptions valid, legal and/or justifiable?	NA	
4.	Is the impact of the document/project likely to be negative?	NA	
5.	If so, can the impact be avoided?	NA	
6.	What alternative is there to achieving the document/project without impact?	NA	
7.	Can we reduce the impact by taking different action?	NA	

Completed by:

Name	**Position**	**Date Completed:**
Les De-Lara	**Information Governance Lead**	**11/08/2021**

10 REFERENCES

REFERENCES	UK Data Protection Act 2018 General Data Protection Regulation 2018 General Data Protection Toolkit: https://nww.igt.hscic.gov.uk/ The Access to Medical Reports Act 1988 The Data Protection (Processing of Sensitive Personal Data) Order 2000 The Electronic Communications Act 2000 The Human Rights Act 1998 The National Health Service Act 2006 The Privacy and Electronic Communications (EC Directive) Regulations 2003 The Public Records Act 1958 The Caldicott Manual UK Information Commissioners Office website https://ico.org.uk/ Information: To share or not to share? The Information Governance Review NHS Code of Confidentiality https://digital.nhs.uk/search?q=confidentiality&s=s
RELATED POLICIES	IMG 001 Information Security Management System Policy IMG 003 Information Technology Team and Networking Policy IMG 028 Data Sharing Policy IMG 009 Security Incident Reporting Procedure IMG 020 Data Quality Procedure Policy IMG 037 Records Management and Lifecycle Policy

APPENDIX A - GDPR/DPA 18 PROCESSING – LEGAL BASIS

Personal data – any information relating to an identifiable person who can be directly or indirectly identified – name; identification number, location data or online identifier o Personal data that has been pseudonymised can fall within the scope depending on how difficult it is to attribute the pseudonym to an individual.

Lawfulness of processing personal data – GDPR Article 6

6.1a	**The data subject has given consent to the processing of his or her personal data for one of more specific purposes.**
6.1b	**Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.**
6.1c	**Processing is necessary for compliance with a legal obligation to which the data controller is subject.**
6.1d	Processing is necessary in order to protect the vital interests of the data subject or of another natural person.
6.1e	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 *see below for detail of legal obligations.
6.1f	Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Sensitive data – "special categories of personal data"

Processing of 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 shall be prohibited.

Above shall NOT APPLY if one of the following applies:

2 (a)	The data subject has given EXPLICIT consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject.
2 (b)	Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law, in so far as it is authorised by Union or member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject.
2 (c)	Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent [Capacity Act would apply – or if the person is at risk i.e. Mental Health Act Assessment].
2 (d)	Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects.
2 (e)	Processing relates to personal data which are manifestly made public by the data subject.

2 (f)	Processing is necessary for the establishment, exercise or defence or legal claims or whenever courts are acting in the judicial capacity.
2(g)	Processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.
2 (h)	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 Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3 Paragraph 3: Personal data referred to in para 1 may be processed for the purposes referred to in point (h) of para 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.
2 (i)	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 Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, particular professional secrecy; or
2 (j)	Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject.