Bridgewater Community Healthcare NHS Foundation Trust

Data Protection and Confidentiality Policy

Policy Number	**IG/Pol/014**
Target Audience	**All Trust Staff including permanent, temporary, contractors, learners in practice, apprentices and volunteers**
Approving Committee	**Corporate Clinical Policy Group**
Date First Approved	**May 2021**
Last Full Review Date	**New Policy**
Next Full Review Date	**May 2024**
Policy Author	**Information Governance & Records Manager**
Version Number	**1.0**

Applicable Statutory, Legal or National Best Practice Requirements	Data Protection Act 2018, c.29 Equality Act 2010, c. 15 Freedom of Information Act 2000, c.36 GOV.UK. 2018 Data protection impact assessments for surveillance cameras Health Service (Control of Patient Information) Regulations 2002 No. 1438 Health and Social Care Act 2012 c. 7 Human Rights Act 1998, c.42 Information Commissioner's Office 2018, Guide to the General Data Protection Regulation (GDPR) National Health Service Act 2006 Section 251 NHS Digital (2021) Data Security and Protection Toolkit Protection of Children Act 1999 c. 14

The Trust is committed to an environment that promotes equality, embraces diversity and respects human rights both within our workforce and in service delivery. This document should be implemented with due regard to this commitment.

This document can only be considered valid when viewed via the Trust's intranet. If this document is printed into hard copy or saved to another location, you must check that the version number on your copy matches that of the one online.

Version Control Sheet

Version	Date	Reviewed By	Comment
0.1	3/1/2021	S. Ramsdale	First Draft
0.2	March 21	DIGIT Members	See Consultation Section.
0.3	April 21	M. Corkery	Comments made
0.4	April 21	S. Ramsdale	Comments addressed
0.5	May 2021	Corporate Clinical Policy Group	Approved subject to minor amendments and final chair approval
0.6	May 2021	S. Ramsdale	Amendments completed
1.0	May 2021	S. Arkwright	Approved by chair action

Does this policy impact/potentially impact on: • **Staff** • **Patients** • **Family Members** • **Carers** • **Communities**	**Yes**	**Please contact the Trust's Equality & Inclusion Manager at:** **Email: ruth.besford@nhs.net**
	No	**Please sign and date below:** **Name:** **Email Address:** **Date:**

Education & Professional Development Question

In order to ensure that any training requirements are discussed and resources planned and allocated to meet the needs of the service, you must consider whether this document has additional training requirements.

Please answer the following question by entering a cross in the box below:

	Yes	No
Does this document have any additional training requirements or implications?		x

Contents

1	Introduction	4
1.1	Objective	5
1.2	Scope	6
2	Definitions	6
3	Abbreviations	10
4	Other Relevant Procedural Documents	10
5	Roles and Responsibilities	11
6	Equipment List	14
7	Data Protection	14
7.1	Lawfulness, fairness and transparency	15
7.2	Data minimisation - Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed	16
7.3	Accurate and kept up to date	18
7.4	Storage limitation	19
7.5	Processed in a manner that ensures appropriate security of the personal data 'integrity and confidentiality'	19
7.6	Confidentiality	20
7.7	Consent	20
7.8	Exemptions to Confidentiality	21
7.9	Accountability	22
8	Consultation	23
9	Dissemination and Implementation	24
9.2	Dissemination	24
9.3	Implementation	24
10	Process for Monitoring Compliance and Effectiveness	24
11	Standards/Key Performance Indicators	24
12	References	24

The following appendices can be accessed electronically by clicking on the following link:

Appendix 1 - Anonymisation checklist
Appendix 2 - Pseudononymisation checklist
Appendix 3 - National data opt out checklist
Appendix 4 - Disclosure of Personal Information Model

1 Introduction

This policy aims to detail with how Bridgewater Community Healthcare NHS Foundation Trust (hereafter the Trust) will meet its legal obligations and NHS requirements concerning data protection and confidentiality primarily regarding the General Data Protection Regulation (GDPR) and Data Protection Act (DPA) 2018. The Data Protection Act (DPA) 2018 is the UK's implementation of the General Data Protection Regulation (GDPR). The GDPR and the DPA set out specific responsibilities for those who process "personal data".

All employees 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 data protection legislation.

Confidentiality is also a requirement within the NHS Care Record Guarantee, produced to assure patients regarding the use of their information.

The DPA and GDPR sets out the legal requirements and duties placed on data controllers and data processors and explains the 'information rights' held by data subjects. The Trust is both a data controller and a data processor; it also has joint responsibilities with other data controllers. The Trust is required to register annually with the Information Commissioner, the regulators of DPA and GDPR. The Trust's unique registration number is **Z2436346.**

As a healthcare Trust, we declare our compliance with the Data Security and Protection Toolkit (DSPT) run by NHS Digital on an annual basis.

The Trust principles regarding data protection are:

- We will be open and transparent with service users and those who lawfully act on their behalf in relation to their care and treatment. We will adhere to our duty of candour responsibilities as outlined in the Health and Social Care Act 2012

- We will establish and maintain policies to ensure compliance with the Data Protection Act 2018, Human Rights Act 1998, the common law duty of confidentiality, the General Data Protection Regulation and all other relevant legislation

- We will establish and maintain policies for the controlled and appropriate sharing of service user and staff information with other agencies, taking account all relevant legislation and citizen consent

- Where consent is required for the processing of personal data we will ensure that informed and explicit consent will be obtained and documented in clear, accessible language and in an appropriate format. The individual can withdraw consent at any time through processes which have been explained to them. We ensure that it is as easy to withdraw as to give consent

- We will undertake a programme of audits to assess our compliance with legal requirements.

We acknowledge our accountability in ensuring that personal data shall be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')
- Accurate and kept up to date
- 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')
- Processed in a manner that ensures appropriate security of the personal data.

We uphold the personal data rights outlined in the GDPR:

- 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
- Rights in relation to automated decision making and profiling.

There are numerous appendices that support this policy these are:

- Anonymisation checklist – appendix 1
- Pseudononymisation checklist – appendix 2
- National data opt out checklist – appendix 3
- Disclosure of Personal Information Model – appendix 4

1.1 Objective

The purpose of this policy is to support the 10 Data Security Standards, UK GDPR the Data Protection Act (2018), the common law duty of confidentiality and all other relevant national legislation. We recognise data protection as a fundamental right and embrace the principles of data protection by design and by default.

This policy is to establish a framework in which the Trusts personal data can be managed, and to provide staff members with a high-level overview of the legal obligations that apply to data protection and confidentiality.

This policy applies to all employees and must be strictly observed. Failure to do so could result in disciplinary action.

It is expected that local procedures are produced to support the specific aspects of this policy – see the Development and Management of Procedural Documents Policy.

1.2 Scope

This policy, together with the associated standards, is aimed at all staff, including permanent, temporary, contractors, learners in practice, apprentices and volunteers, that manage and handle personal information/data or come across personal information/data in their work.

This policy relates to all information held or due to be held by the Trust or those who process information on behalf of the Trust.

2 Definitions

The definitions applicable to this document are as follows:

Name	Definition
Biometric Data	Facial imaging and fingerprint data are just two examples, but these are not exhaustive. Many other types of physical, physiological or behavioural 'fingerprinting' fall within the definition. Examples of physical or physiological biometric identification techniques: • Facial recognition • Fingerprint verification • Iris scanning • Retinal analysis • Voice recognition • Ear shape recognition.
Personal Data	Personal data is defined in the GDPR as: *"'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".*
Natural Persons	Natural person is a person who is alive. Note: a health record for a deceased person may contain personal information of a natural person and this should be considered in the event of a data breach.
Data Subject	The personal information to the identifiable living individual to whom personal data relates.

Information Governance	Information Governance is a framework for handling personal information in a confidential and secure manner to appropriate ethical and quality standards in a modern health service. It provides a consistent way for employees to deal with the many different information handling requirements including: • Information Governance Management • Clinical Information assurance for Safe Patient Care • Confidentiality and Data Protection assurance • Corporate Information assurance • Information Security assurance • Secondary use assurance • Respecting data subjects' rights regarding the processing of their personal data • Freedom of Information rights See the Information Governance Framework Policy for more details.
Special Category Data	The GDPR singles out some types of personal data as likely to be more sensitive, and gives them extra protection: • Personal data revealing racial or ethnic origin • Personal data revealing political opinions • Personal data revealing religious or philosophical beliefs • Personal data revealing trade union membership • Genetic data • Biometric data (where used for identification purposes) • Data concerning health • Data concerning a person's sex life • Data concerning a person's sexual orientation.
Third Party	Article 4(10) of the GDPR defines 'third party' as "a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data".
Data Security Protection Toolkit	"The Data Security and Protection Toolkit is an online self-assessment tool that allows organisations to measure their performance against the National Data Guardian's 10 data security standards. All organisations that have access to NHS patient data and systems must use this toolkit to provide assurance that they are practising good data security and that personal information is handled correctly. This system is subject to ongoing development" (NHS Digital 2021)

Data Breach	A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data. Personal data breaches can include but not limited to (ICO 2021): • Access by an unauthorised third party • Deliberate or accidental action (or inaction) by a controller or processor • Sending personal data to an incorrect recipient • Computing devices containing personal data being lost or stolen • Alteration of personal data without permission • Loss of availability of personal data • Not sharing information when it should have been shared.
Privacy Notice	NHS England's definition of a privacy notice: *The UK General Data Protection Regulation (GDPR) requires that data controllers provide certain information to people whose information (personal data) they hold and use. A privacy notice is one way of providing this information. This is sometimes referred to as a fair processing notice.* *A privacy notice should identify who the data controller is, with contact details for its Data Protection Officer. It should also explain the purposes for which personal data are collected and used, how the data are used and disclosed, how long it is kept, and the controller's legal basis for processing (NHSE 2021).*
Information Commissioner's Office (ICO)	The ICO are independent regulators of GDRP and DPA who have the powers to impose fines if they deem that the organisation has made an "infringement." on the regulations They also regulate Privacy and Electronic Communication Regulation (PECR) (see below).
Privacy and Electronic Communication Regulation	The PECR sit alongside the Data Protection Act (2018) and the UK GDPR. They give people specific privacy rights in relation to electronic communications. There are specific rules on: • Marketing calls, emails, texts and faxes • Cookies (and similar technologies) • Keeping communications services secure • Customer privacy as regards traffic and location data, itemised billing, line identification, and directory listings. (ICO 2021)

Data Flow	A continuing or repeated flow of information which takes place between individuals or organisations and includes personal data.
Direct Care	The provision of clinical services to a patient that require some degree of interaction between the patient and the health care provider.
Legitimate relationship	A relationship that exists between a patient and an individual or group of record users involved in their treatment which provides the justification for those users to access a patient record.
Secondary Purpose	A purpose other than direct care such as healthcare planning, commissioning, public health, clinical audit and governance, benchmarking, performance improvement, medical research and policy development.
Duty of Confidence	A duty of confidence arises when one person discloses information to another in circumstances where it is reasonable to expect that the information will be held in confidence.
Gender Recognition Certificate	A legal document that includes issuing of a new birth certificate in the person's identified gender. People who hold a Gender Recognition Certificate (GRC) have particular protections in relation to consent and information sharing – it is an illegal act under the Gender Recognition Act 2004 to disclose that an individual holds a GRC without express consent. It is good practice to assume any transgender person holds a GRC and the information about their previous gender is a confidential item that must not be disclosed without consent. This relates to all records, including health and Human Resources (HR) records.
Business Continuity Plans	Outlines the procedures in the event of a security failure or disaster affecting digital systems or mass loss of hardcopy information necessary to the day to day running of our organisation.
Consent	Consent has to be explicit it must be unambiguous and involve a clear affirmative action (an opt-in). It specifically bans pre-ticked opt-in boxes. It also requires distinct ('granular') consent options for distinct processing operations. Consent should be separate from other terms and conditions and should not generally be a precondition of signing up to a service. The UK 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.
Surveillance Camera Commissioner	Like the ICO the surveillance commissioner regulates the use of surveillance cameras like CCTV.

3 Abbreviations

The abbreviations applicable that are not explained in full within the document are as follows:

IT	Information Technology
GDPR	General Data Protection Regulation
GRC	Gender Recognition Certificate
ICO	Information Commissioner's Office
DPA	Data Protection Act
PECR	Privacy and Electronic Communication Regulation
DPO	Data Protection Officer
IG	Information Governance
SIRO	Senior Information Risk Owner
DPIA	Data Protection Impact Assessment
IAO	Information Asset Owners
DIGIT	Digital, Information Governance and Information Technology Group
ROPA	Record of Processing Activities
EPR	Electronic Patient Record
DPST	Data Security and Protection Toolkit
HR	Human Resources
CNIO	Clinical Informatics Chief Nurse
TOR	Terms of Reference
DOB	Date of Birth

4 Other Relevant Procedural Documents

This document should be read in conjunction with the following documents not elsewhere linked within this document are:

Incident Reporting Policy

Incident Investigation Procedure

Risk Management Framework

Development and Management of Procedural Documents Policy

Disciplinary Policy and Procedure

Corporate Records (including Document Management) Policy

Information Asset and System Audit Policy

Health Records Policy

Records Management: Storing and Movement of Records Policy

Records Management: Archiving, retention and disposal policy

IT Asset Management Policy

Acceptable use (IT) Policy

Information Security Policy

Data Encryption Policy

Information Governance Framework Policy

Subject Access/Access to Health Records Policy

Procurement Policy

5 Roles and Responsibilities

5.1 Chief Executive

The Chief Executive, as Accountable Officer, has overall responsibility for this policy ensuring its effectiveness.

5.2 Senior Information Risk Owner

The Senior Information Risk Owner (SIRO) is the Board Member who has overall responsibility for Information Risk Management in the Trust.

The SIRO will report to the Quality and Safety Committee on information risks and through the Statement of Internal Controls following assurance from the Information Asset Owners. The SIRO is the Director of Finance. The Deputy SIRO is Assistant Director of IT.

5.3 Caldicott Guardian

The Caldicott Guardian is the Board Member who has responsibility for overseeing the implementation of the laws that govern personal information and ensuring that good practice in relation to access and reuse is implemented within the Trust.

The Caldicott Guardian is the Trust champion in respect of the Caldicott Principles and as such is obligated to always make Caldicott decisions in the best interests of the patient.

The Caldicott Guardian is the Chief Nurse. The Deputy Caldicott Guardian is the Deputy Chief Nurse.

5.4 Data Protection Officer

The Data Protection Officer (DPO) has responsibility for informing and advising, and monitoring compliance with data protection principles. The DPO for the Trust is held by the Trust Secretary. With the support of their office, the DPO will:

- Provide advice to the organisation and its employees on compliance obligations with data protection law
- Advise on when data protection impact assessments are required
- Monitor compliance with data protection law and organisational policies in relation to data protection law
- Co-operate with, and be the first point of contact for the Information Commissioner
- Be the first point of contact within the organisation for all data protection matters
- Be available to be contacted directly by data subjects
- Take into account information risk when performing the above
- Will be the key contact in the event of a data breach.

5.5 Assistant Director of IT

The Assistant Director of IT supported by the Head of IT and their teams are responsible for developing, implementing and enforcing suitable and relevant information security procedures and protocols to ensure the Trust systems and infrastructure remain compliant with data protection legislation.

They are responsible for ensuring that all of the Trust electronic equipment and assets have adequate security measures to comply with data protection and data security legislation and regulations, which includes undertaking a Data Protection Impact Assessment (DPIA) where necessary.

5.6 Information Governance Manager and Records Manager

With the support of the Information Governance (IG) team, the Information Governance and Records Manager will:

- Maintain an awareness of information governance issues within the Trust
- Keeps up to date with changes in legislation to ensure the Trust remains compliant
- Review and update the information governance policies and procedures in line with local and national requirements
- Work with Information Asset Owners (IAO's) and project managers to complete a DPIA and recommend any areas of risk
- Review and audit all procedures relating to this policy where appropriate on an ad-hoc basis
- Ensure that line managers are aware of the requirements of the policy
- Work with the Caldicott Guardian, SIRO and DPO functions to ensure organisational authority and awareness regarding issues relating to data protection or confidentiality concerns.

5.7 Information Asset Owners

IAO's are responsible for ensuring the asset they 'own' or due to own is managed in accordance with this policy, and also for maintaining adequate records within the context, both legal and regulatory, of the business area the asset operates. The Information Asset Owners are supported by the Information Asset Administrators.

5.8 Digital, Information Governance and Information Technology Group

The Digital, Information Governance and Information Technology (DIGIT) group will monitor compliance with this policy on behalf of the Trust, and will report on the management and accountability arrangement for Information Governance (IG), and provide assurance to the Board through the Trusts sub committees.

5.9 Digital Development Group

The Digital Development Group is a sub group of the DIGIT group. The Digital development group has been assigned specific projects to oversee and manage on behalf of DIGIT. The projects are mainly to support the digital development or enhancement of clinical systems.

5.10 Borough Directors/Clinical Managers

Borough Directors and Clinical Managers will:

- Monitor compliance with IG/data protection standards within their work areas

- Actively seek guidance from the IG team and provide feedback to the services.
- Report identified incidents or risks within their department through the Trusts on-line Risk Management Reporting System (Ulysses)
- Ensure a DPIA is undertaken as per this policy.

5.11 Procurement Team

The Procurement Team will ensure, where personal information is being processed, the contract will have the legal responsibilities for the Trust. See section 7.9.1 (contracts) for full details.

5.12 Staff

All staff (employees) have a responsibility to abide by this policy. Staff have a duty to familiarise themselves with this policy and abide by its principles. They must understand and comply with the processes and confidentiality that support this policy.

Inappropriate access to any confidential, restricted or personal records including health or corporate records and documents can result in disciplinary and possible dismissal. To access your own health or staff record, or that of your family member's staff, should submit a subject access request in writing to the relevant service or department.

6 Equipment List

Not applicable

7 Data Protection

The Trust is a public authority which collects and processes vast quantities of personal and special category data. The Trust is a Data Controller but does act as a Data processor in some occasions along with has Joint controller responsibilities.

The Trust is required to abide by all relevant legislation pertaining to Data Protection and Confidentiality.

The key principles of data protection are set out in Article 5 – The principles relating to processing of personal data. These principles have been divided into sub headings below with explanations on what is expected within the Trust.

The Trust should understand what personal and special category data it is processing and is required to keep a record of processing activities (ROPA). The processing activities are reviewed each year via the service data flow tool. A completed service data flow tool informs the trust of the categories of data being processed and sets out the legal basis for sharing the information. The recording obligation is stated by article 30 of the GDPR.

7.1 Lawfulness, fairness and transparency

Ensuring that the legal basis for the processing of information is identified before processing commences is called “data protection by design and by default” Article 25 of GPDR summarises what is needed:

“…..to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects”

To ensure that the processing is within the legal requirements, a DPIA is to be undertaken on all new or changes to processing of personal information. Undertaking a DPIA will risk assess the aspects of the data protection principles.

As a large majority of our projects involve special category data, it’s the Trust decision to undertake a DPIA on all projects. Where there is a high risk highlighted in the DPIA this will need to be reviewed and accepted by the SIRO and or DPO.

As a health organisation we process personal and special category information on a large scale we do this on the legal basis for processing information for the provision of direct care these are normally Article 6 (1) (e) public task and/or Article 9 (2) (h) …health or social care or treatment.

The Trust is transparent on how it processes and collects information by detailing this in our Privacy Notices. Under GPDR its states that individuals have a “right to be informed” we do this within our Privacy Notices which are supplied to individuals regarding to the processing of their personal data it is written in clear, plain language which is concise, transparent, easily accessible and free of charge.

We have three main privacy notices available on the Trust website one for all of our clients and stakeholders, which outlines our responsibilities as a data controller, along with details of our DPO. A bespoke one for the children we care for and one for our staff which is on the intranet. Under the Data Protection Act (2018) everyone aged 13 or over is presumed to be competent to give consent for themselves unless the opposite is demonstrated.

Included on the website is additional information regarding information sharing for the COVID 19 response.

- Trusts privacy notice
- Childrens privacy notice
- Staff privacy notice – Staff Zone on the Intranet

To comply with the common law duty of confidentiality; any personal information given or received in confidence for one purpose may not be used for a different purpose or passed on to anyone else without the consent of the individual.

It is impracticable to obtain explicit written consent every time that health care information needs to be shared, nor is it required to share information for direct patient care.

In these instances consent is implied, provided that it is known and understood by the data subject that such information needs to be made available to others involved. GDPR states that consent when sharing patient information for direct patient care is a legal basis and consent is therefore not required.

The Trust can process information based on consent, but this is rare, and through the DPIA process will consider the additional implications when consent is used as the legal basis. When consent is used as a legal basis there are additional aspects that need to be considered for example the right to withdraw consent or the right of erasure, all need to be documented and retained.

An example where the trust would process information with consent is a subject access request.

7.1.1 Surveillance Cameras

The Trust uses security CCTV cameras in various locations across its geographical area. The use of CCTV cameras is regulated by the Surveillance Camera Commissioner.

Cameras have specific requirements regarding protecting people's privacy. To support organisations a good practice DPIA has been used to support the use of CCTV. It is recommended that data protection impact assessments are carried out when (GOV.UK 21):

- Cameras are added or removed from systems
- Cameras are moved or change position
- Whole or parts of systems are upgraded
- New systems are installed
- Where systems that include biometrics capabilities such as automatic facial recognition are in use.

7.2 Data minimisation - Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

As a Trust we collect different kinds of data and hold different kinds of records. We only collect information for a specific legitimate purpose. The Corporate Records Policy and the retention schedule have details on the types of information we hold and how long we hold the information for. The Information Asset and system Audit Policy has details information on what is expected of those individuals who are accountable for managing systems that process information.

Where information is held by individual members or teams for example in a cabinet or electronic folder, this need to be reviewed on a periodical basis to ensure that the information held is still that is necessary, any information held even past the retention date can be requested under a subject access request, this means if we have it we have to supply it.

When personal information is processed where it can be made anonymised or pseudonymised; this should be undertaken. Using anonymised data is not subject to data privacy laws if the Anonymisation is done correctly. Pseudonymised information is subject to data privacy laws as this information is only shielded and is reversible.

7.2.1 Anonymisation

Anonymisation is a valuable tool that allows data to be shared, whilst preserving privacy. The process of anonymising data requires that identifiers are changed in some way such as being removed, substituted, distorted, generalised or aggregated.

A person's identity can be disclosed from:

- **Direct identifiers** such as names, postcode information or pictures

- **Indirect identifiers** which, when linked with other available information, could identify someone, for example information on workplace, occupation, salary or age.

Each service that shares information in an anonymised format is to regularly assess if they meet the Anonymisation standards in Appendix 1.

7.2.2 Pseudonymisation

Pseudonymisation takes the most identifying fields within a database and replaces them with artificial identifiers, or pseudonyms. For example a name is replaced with a unique number. The purpose is to render the data record less identifying and therefore reduce concerns with data sharing and data retention.

Pseudonymised data is typically used for analytics and data processing, often with the aim of improving processing efficiency data files at a patient level sometimes need to be shared for secondary purposes between agencies.

Each service that processes information in a pseudonymised format is expected to have a local procedure that embeds the following Pseudonymisation standards set in Appendix 2. As pseudonymised data is subject to data protection laws this should be included in the services annual review of ROPA/data flow audit.

7.2.3 National Data Opt Out

The information in patient's record can sometimes be used to help with research and planning. The National Opt Out Program which was introduced in May 2018 allows patients to opt out of sharing their personal information for planning and research. There is a useful guide on if National Opt Out applies and in what circumstances in Appendix 3 – National Opt Out.

The patient is opting out of sharing information that identifies them as an individual. The national opt out for planning and research does not include clinical research which has a different governance process.

Clinical and frontline admin staff are not expected to facilitate the opt outs, this will be done by the trusts informatics teams. However, clinical and front line admin staff are expected to signpost patients to how they can opt out.

How patient can opt out of sharing their information for planning and research purposes can be found here using the following link:

https://www.nhs.uk/your-nhs-data-matters/

7.3 Accurate and kept up to date

The Trust hold different types of personal information but largely this is special category information gained from the patient. The accuracy of data recorded should be verified at every contact with the patient, to ensure all contact details are up to date.

Information can only be relied upon when it is accurate and up to date. Information should be:

- Accurately recorded based on the information provided
- Accurately record the source of the information
- Take reasonable steps in the circumstances to ensure the accuracy of the information
- Carefully consider any challenges to the accuracy of the information.

The Corporate Records Policy has information on how information should be named and filed, to ensure it can be accessed quickly and accurately.

Inaccurate demographic data should be corrected immediately without delay, as this can have a risk on the patients not receiving the correct information. The data subject or patient has a “right of access” to their information and for that information to be correct. The data subject can ask for their data to be corrected but not erased.

The Trust Electronic Patient Records (EPR) has a full audit trail of any actions taken within a record. The Trusts Caldicott Guardian can authorise complete removal or erasure of information within a health record.

Data quality audits are to be regularly undertaken to ensure that information recorded for the patient represents a true picture of their encounter with the Trust.

To ensure patient care meets evidence based standards and to improve outcomes for patients, a clinical audit programme of audits is undertaken. In addition and to support data quality audits the Trust has a programme of regular record keeping audits.

The Health Records Policy has more details on the standards expected by the Trust to ensure our health records are accurate.

7.4 Storage limitation

All staff have the responsibility to store information securely this includes when the information needs to be moved. The Records Management: Storing and Movement of Records Policy has the standards for storing and moving of paper records. The Records Management: Archiving, retention and disposal policy has the standards retaining and disposal of records.

The retention schedule has information on how long information needs to be retained before being destroyed to specific standards. The retention schedule is based on the NHS Records Management Code of Practice; sometimes the schedule does not reflect all the records held by the Trust, therefore the schedule can be updated if needed. Contact the IG team bchft.ig@nhs.net to discuss adding to the schedule.

Where information is held by individual members or teams for example in cabinets or electronic folders, this need to be reviewed on a periodical basis to ensure we only hold information that is necessary.

Each team is expected to have a schedule or a bespoke procedure to ensure all information is reviewed on a regular basis, this includes who has access to the information – see the Development and Management of Procedural Documents Policy. Any information held even past the retention date can be requested under a subject access request; this means if we have it we have to supply it.

All staff wishing to destroy personal data can contact the Information Governance on bchft.ig@nhs.net to discuss the best method of destruction.

7.5 Processed in a manner that ensures appropriate security of the personal data 'integrity and confidentiality'

The IT Asset Policy and the Acceptable use (IT) policy has information on what IT equipment is used within the Trust and what is expected of the users (staff) when using this equipment to ensure the information held is secured at all times.

The Information Security Policy has information on transfers of electronic information and how the protection of Information Assets. The Data Encryption Policy has the Trusts approach on how to secure information within the IT assets. Where there has been unauthorised access, loss, destruction or damage to information, including any attempts accidental or otherwise will be managed through the Trusts management of incidents process.

The Information Governance Framework Policy, section 7.7 entitled "Data breaches and Data incidents" has details on how the Trust manages a serious data breach and when it is reportable to the ICO.

Staff must **never** send personal, sensitive or confidential information to a non-secure email address unless it is encrypted.

The Trust uses NHSmail along with other associated components like Microsoft Teams. NHSmail has enhanced features where you can send emails securely even to patients it encrypts and secures PID. NHSmail also has its own Acceptable use (IT) policy and other policies like the NHSmail Access Policy (2020) that staff need to uphold.

7.6 Confidentiality

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, Gender Recognition Certificate etc.

All employees 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. We only share healthcare information that is needed to deliver the current care they are receiving.

7.7 Consent

As a health care provider we rarely use consent as a legal basis for obtaining and sharing information. This is supported by the ICO who state:

"In the healthcare context consent is often not the appropriate lawful basis under the GPDR. This type of assumed implied consent would not meet the standard of a clear affirmative act – or qualify as explicit consent for special category data, which includes health data. Instead, healthcare providers should identify another lawful basis (such as vital interests, public task or legitimate interests). For the stricter rules on special category data, Article 9(2)(h) specifically legitimises processing for health or social care purposes."

We should always ensure that the data subjects are informed unambiguously, particularly in the case of sensitive personal information what is happening with their information; the individual should understand how and for what purpose their information will be used. We do have the ability to shield certain information or "restrict the processing" or "the right to object" for the data subject which they do not want to share, this will be on an individual basis but each IAO or IAA will have supporting information on how this can be undertaken.

The data subject has a "right of access" and the "right of data portability" to their records; this is covered within the data Subject Access/Access to Health Records Policy, which has details for patients and staff.

Where personal data is processed for direct marketing purposes, the Trust will stop processing personal data for direct marketing purposes as soon as an objection is received. The trust cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.

When we do require consent this is always recorded through our records; we will explicitly explain to the individual information on how they can withdraw consent and when the “right of erasure” is relevant. There will be circumstances of course, when seeking the consent of the individual will not be desirable or possible because it will prejudice delivery of the intended outcome, or may increase the risk of significant harm to the individual or the public, see examples below.

7.8 Exemptions to Confidentiality

There are exceptions where the sharing of information is undertaken without the direct knowledge of the data subject. In rare circumstances, when it is overwritten by a senior person within the Trust, personal information is shared. In these circumstances, documented assessment for the need to disclose the information needs to be undertaken, with details on why and by who has released the information.

Section 251 of the NHS act of 2006 and DPA 2018 Schedule 2.1.2 has specific details on when information can be shared without consent from the individual.

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

- Where the data subject's life may be in danger or cases in where the data subject 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 a global pandemic
- Where there is a serious threat to the healthcare professional or other staff
- In other exceptional circumstances based on professional consideration and consultation
- The prevention or detection of a serious crime.

The Trust has contractual responsibilities as a health organisation, where information is disclosed examples of these are:

- 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
- Child abuse - Children’s Act 1989 and The Protection of Children Act 1999
- Drug Addicts – Misuse of Drugs (Supply to Addicts) Regulations 1979
- Road traffic accidents - Road Traffic Offenders Act 1988

- Prevention/detection of a serious crime e.g. terrorism, murder – DPA 2018 Schedule 2.1.2. The Crime and Disorder Act 1998

To help manager/senior clinicians to assess before information should be disclosed see - Appendix 4 Disclose Model.

7.9 Accountability

The Trust is a "Data Controller" and will process information to support joint working with our partners as this may mean we become "joint controllers" to aid patient care when we are processing the same personal data. We also procure third parties as "Processors" to process information on our behalf. Accountability is a legal requirement for data sharing; it too is one of the principles applicable to general data processing under the GDPR.

7.9.1 Contracts/Data Processors

The law makes written contracts between controllers and processors a legal requirement. Contracts which involve patient or staff data must now include specific minimum terms. These terms are designed to ensure that processing carried out by a processor meets all the GDPR requirements, not just those related to keeping personal data secure. As a data controller we are liable for what the processor undertakes on our behalf.

The minimum terms or clauses that need to be in a contract or processing agreement are:

- Subject matter and duration of the processing
- Nature and purpose of the processing, including when changes are needed
- Type of personal data and categories of data subject
- Controller's obligations and rights
- Processing only on the controller's documented instructions
- The duty of confidence
- Appropriate security measures
- The use of sub-processors
- Data subjects' rights
- Assisting the controller
- End-of-contract provisions
- Audits and inspections.

7.9.2 Joint Controllers and/or sharing agreements

An agreement with another healthcare provider where the data subject is shared for direct care is not legally necessary; however the agreement can determine the purpose and means of the processing, and includes the rights of the data subject, therefore is a requirement by the Trust. An example of what the agreement of this kind can ascertain is:

- How the information is being processed and secured
- Who will handle subject access request
- How to notify the other controller in the event of a data breach
- Who will undertake an investigation when things have gone wrong.

The annual data flow should record where a sharing agreement is in place.

All sharing agreements are to be held corporately by the Information Governance Team. There are templates for a Data/Information Sharing agreement template, a data transfer agreement and a Joint controller agreement please request from the IG team on bchft.IG@nhs.net.

8 Consultation

Key individuals/groups involved in the development of the document to ensure it is fit for purpose once approved.

Name	Designation
DIGIT Members as per Terms of Reference (TOR)	Associate Director: Quality Governance Director of Finance/ Senior Information Risk Owner Responsible Non-Executive Director Assistant Director For IT/Deputy SIRO Deputy Director Information & Clinical Performance Data Protection Officer Information Governance and Records Manager Senior Information Governance Officer Head of IT Head of Data Security Clinical Informatics Chief Nurse (CNIO) Registration Authority & Training Lead Head of Procurement Human Resources Director of Operations/Nominated Deputy – Warrington Director of Operations/Nominated Deputy – Halton & St Helens Director of Operations/Nominated Deputy – Dental Director of Operations/Nominated Deputy – Health & Justice

Name	Designation
	Education & Professional Development Lead
Mary Corkery	Policy Officer
Razia Nazir	Knowledge and Library Service Manager
Paul Foster	Senior Procurement Officer
Corporate Clinical Policy Group	

9 Dissemination and Implementation

9.2 Dissemination

The Information Governance and Records Manager will disseminate this policy to Borough Directors for disseminating to staff.

This policy will be made available on the Trust intranet and public facing website. The policy will be published on the in the bulletin and team brief and sent out via global e-mail.

New employees will be made aware of this policy through the Induction process.

9.3 Implementation

All staff will be made aware of their personal and organisational responsibilities set out in the responsibilities section of this document. Information governance programme of mandatory training, local induction and monitoring audits.

10 Process for Monitoring Compliance and Effectiveness

The core aspects outlined within the policy are monitored through the Trusts Information Governance audit program, which is both internally and external to the Trust for example the Data Security and Protection Toolkit

11 Standards/Key Performance Indicators

Submission of the Data Security and Protection Toolkit (DPST) on annual basis
Quarterly incident summary reported to DIGIT.

12 References

Data Protection Act 2018, c.29. [online]. Available at: http://www.legislation.gov.uk/ukpga/2018/12/contents

Equality Act 2010, c. 15 [online]. Available at: http://www.legislation.gov.uk/ukpga/2010/15/contents

Freedom of Information Act 2000, c.36 [online]. Available at: http://www.legislation.gov.uk/ukpga/2000/36/contents

GOV.UK. 2018 Data protection impact assessments for surveillance cameras [online] Available at: https://www.gov.uk/government/publications/data-protection-impact-assessments-for-surveillance-cameras
[Accessed 20 April 2021]

Health Service (Control of Patient Information) Regulations 2002 No. 1438 [online]. Available at: https://www.legislation.gov.uk/uksi/2002/1438/contents/made

Health and Social Care Act 2012 c. 7 online]. Available at: https://www.legislation.gov.uk/ukpga/2012/7/contents/enacted

Human Rights Act 1998, c.42 [online]. Available at: https://www.legislation.gov.uk/ukpga/1998/42/contents

Information Commissioner's Office 2018, Guide to the General Data Protection Regulation (GDPR) [online]. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/711097/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf found here https://www.gov.uk/government/publications/guide-to-the-general-data-protection-regulation

Information Commissioner's Office (2021) Personal Data Breaches [webpage]. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

Information Commissioner's Office (2021) When is consent appropriate? [webpage]. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/when-is-consent-appropriate/

Information Commissioner's Office (2021), What is PECR? [webpage]. Available at https://ico.org.uk/for-organisations/guide-to-pecr/what-are-pecr/

National Health Service Act 2006 Section 251 [online]. Available at: https://digital.nhs.uk/services/data-access-request-service-dars/how-the-national-data-opt-out-affects-data-released-by-nhs-digital/national-data-opt-out-guidance-for-researchers/appendix-1-section-251-of-the-national-health-service-act-2006

NHS Digital (2021) Data Security and Protection Toolkit [online]. Available at: https://www.dsptoolkit.nhs.uk/

NHS England [no date] What is a privacy notice? [online]. Available at: https://www.england.nhs.uk/nhse-nhsi-privacy-notice/what-is-a-privacy-notice/#:~:text=A%20privacy%20notice%20is%20one,for%20its%20Data%20Protection%20Officer.&text=We%20may%20collect%20and%20use,functions%20that%20we%20exercise%20jointly

Protection of Children Act 1999 c. 14 [online]. Available at: https://www.legislation.gov.uk/ukpga/1999/14/contents