



Confidentiality Policy

Policy number and category	IG 01	Information Governance
Version number and date	7	April 2025
Ratifying committee or executive director	Information Governance Steering Group	
Date ratified	June 2025	
Next anticipated review	June 2028	
Executive director	Medical Director/ Caldicott Guardian	
Policy lead	Head of Information Governance	
Policy author (if different from above)	As above	
Exec Sign off Signature (electronic)		
Disclosable under Freedom of Information Act 2000	Yes	

Policy context

Birmingham and Solihull Mental Health NHS Foundation Trust (BSMHFT) aims to maintain as confidential all personal information it collects and stores. The Trust will only obtain, record, store, use, disclose or delete personal information according to existing legislation and within the framework of the NHS Confidentiality Code of Practice.

Caldicott 2, Principle 7 (2013): "The duty to share information can be as important as the duty to protect patient confidentiality".

"For the purposes of direct care, relevant personal confidential data should be shared among the registered and regulated health and social care professionals who have a legitimate relationship with the individual."

Policy Requirement (see Section 2)

- All Staff to follow the NHS Confidentiality Code of Practice.
- The policy covers all personal identifiable information about service users, carers, staff and other Persons that may have contact with the Trust.
- Data subjects must be given information on how information may be shared.
- Sharing confidential information with other organisations must be supported by an agreed Information Sharing Protocol.
- Access to and sharing of confidential information should be on a need to know/ minimum basis.
- All breaches of confidentiality should be reported through the incident reporting process.

Change Record

Date	Version	Author (Name & Role)	Reasons for review / Changes incorporated	Ratifying Committee
Feb 2025	6	Kirstie Macmillian, Head of information Governance	3 Yearly Review	IGSG

CONTENTS PAGE

1.1. Rationale	4
1.2. Scope	5
1.3. Principle	5
2. Policy	6
2.1. Overview	6
2.2. Definition Of Terms	7
2.3. The Data Protection Principles	7
3. Procedure -Achieving The Policy	8
3.1 Records/ Information Covered	8
3.2. Data Protection By Design and Default	8
3.3. General Responsibility for Confidentiality	9
3.4. Training	10
3.5. Information Collection	10
3.6. Keeping Patients Informed	10
3.7. Secure Transfer of Personal Identifiable Information	11
3.8. Request for Access to Information	11
3.9. Regular Sharing	12
3.10. Disclosure Without Consent	13
3.11 Sharing information with the police	16
3.12. Research and Audit	17
3.13 National Data Opt Out	18
3.14. Information Storage	19
3.15. Transferring Information Securely	19

3.16. Disposing of Confidentiality	20
3.17 Handling of confidentiality Breaches/ Incidents	20
3.18 Access/ Sharing of Confidential information	21
3.19 Remote Working and Maintaining Confidentiality	22
3.20 Video Conferencing	22
3.21. Children and Young People	23
3.22. Complaints	24
3.23. Sharing Information with Relatives, Friends and Carers	24
3.24 Staff taking Audio and Visual Recordings of Patients for Direct Care or Secondary Use	25
3.25 Audio or Visual Recordings taken by Trust Staff for Purposes other than Patient Care	26
3.26 Staff Use of Personal Mobile Phones and Cameras	26
3.27 International Transfers	27
4. Roles and Responsibilities	27
5. Development and Consultation	28
6. Reference Documents	28
7. Bibliography	29
8. Glossary/Definitions	30
9. Audit and Assurance	31
10.1. Appendix 1. Equality Impact Assessment	33
10.2. Appendix 2: Supporting Information	37
10.3. Appendix 3: Public Interest Exemplar Cases	40
10.4. Appendix 4 Data Protection Impact Assessment Questionnaire	43
10.5. Appendix 5 Full Data Protection Impact Assessment	45
10.6. Appendix 6 Root Cause Analysis	70
10.7. Appendix 7 Flow chart for sharing information with the police	73

1. INTRODUCTION

1.1. Rationale

The Data Protection Act (2018) and the General Data Protection Regulation sets the legal framework by which the Trust can process personal information. It applies to information that might identify any living person. The common law duty of confidentiality governs information given in confidence to a health professional (about a person alive or deceased) with the expectation it will be kept confidential. The Human Rights Act (1998) article 8 provides a person with the right to respect for private and family life. The key rights provided by this legal Framework are also set out in the NHS Constitution (section 3A)

The Trust maintains many records containing personal information and the duty of confidence and other legislation, especially the Data Protection Act apply equally to these records (e.g., service user records, staff records, complaints records, forms etc.).

The Trust is committed to following the patient confidentiality model as described in the NHS Confidentiality Code of Practice:

- Protect - look after the patient's information.
- Inform – ensure that patients are aware of how their information is used.
- Provide choice – allow patients to decide what information can be disclosed or used in a way and,
- Improve – always look for better ways to protect, inform and provide choice.

The Trust has a core principle of **Honesty and openness**- *We will keep each other well informed through regular communication. We will have honest conversations and explain our decisions.* This value needs to be met alongside ensuring confidentiality is managed appropriately.

The purpose of this policy is to lay down principles that must be observed by BSMHFT staff and who have access to person-identifiable information or confidential information.

The Trust has a legal duty to individuals e.g., service users, carers, and staff to; protect personal information, inform them how information is being used, of their rights to access information and where appropriate seek consent before disclosing to other parties.

This means ensuring all personal information is processed lawfully, fairly and transparently, so that they:

- Understand the reason for collecting, storing and sharing personal information (processing).
- Give consent for the use and disclosure of personal information (where applicable).
- Have confidence in the way the Trust handles personal information.
- Understand their rights, including the right to access information held about them or the right to give consent to others to access this information on their behalf.
- Are aware of the role of the Information Commissioners Office (ICO) and their right to seek advice from or complain to the ICO if they feel their rights are being breached by the Trust.

1.2.Scope

All employees of the Trust (substantive, agency, and contractor, temporary, those in partnership / under contract, volunteers, students or apprentices) are bound by a legal duty of confidence to protect personal information they may come into contact with during the course of their work. This is not just a requirement of their contractual responsibilities but also a requirement within the common law duty of confidence and the Data Protection Act.

This policy sets out requirements placed on staff when sharing information in the NHS and between NHS and non-NHS organisations. It also reinforces responsibilities of Information Asset Owners and requirement to ensure confidentiality for their system.

1.3. Principles

The Trust always works on the basis that sharing information to support service user's care and to prevent risk to data subjects or others is essential. It is not acceptable that the care a service user receives might be undermined because organisations providing health and care to an individual do not share information effectively. Sharing personal information effectively is a key requirement of good information governance and health and social care professionals should have the confidence to share information in the best interests of their service.

There is a need for trust between providers, particularly at the boundary between health and social care – the best interests of patients and service users must not be undermined by cultural differences between different parts of the health and care system.

Caldicott principle 7- *The duty to share information can be as important as the duty to protect patient confidentiality. Health and social care 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.*

People should feel confident that health and social care bodies handle confidential information appropriately. The Trust will always respect the confidentiality of service users, families, carers, staff and other third parties and not disclose personal information without consent, unless there is a legal basis to allow the sharing, if there is an overriding public interest (e.g., to prevent a serious crime), or if there are reasons to believe that failing to share information could put someone at risk. Individuals will never be placed at potential risk through a lack of information sharing.

An individual may express an objection to uses of their personal information on occasions. Such objections may limit the use of their information for certain purposes. However, there are other purposes for which an individual does not have a right to prevent data about them being used, for example, the use of personal data to prevent the spread of infection of notifiable diseases and to prevent further outbreaks in future or for the prevention of a serious crime.

All staff must ensure service user information is processed fairly, lawfully and as transparently as possible. All staff has a responsibility to meet the standards outlined in this policy in accordance with the standard terms and conditions of their employment. All staff must ensure the following principles are adhered to:

- Person-identifiable/ confidential information must be protected against improper disclosure when it is received, stored, transmitted or disposed of.
- Access to person-identifiable/ confidential information must be on a need-to-know basis.
- Disclosure of person identifiable/ confidential information must be limited to that purpose for which it is required.
- Recipients of disclosed information must respect that it is given to them in confidence.
- If the decision is taken to disclose information, that decision must be justified and documented.
- Comply with the Duty of Candour- general duty to act in an open and transparent way in relation to care and treatment provided to service users.

Government Guidance, *Every Child Matters*, “*Information Sharing: Guidance for practitioners and managers*”, (2008) highlights seven golden rules for information sharing:

1. **Remember Data Protection is not a barrier to sharing information.** It provides a framework to ensure personal information about living persons is shared appropriately.
2. **Be open and honest** with the person (and/or their family and carers) from the outset about why, what, how and with whom information will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so.
3. **Seek advice from the IG Team or Caldicott Guardian.** If you are in any doubt, without disclosing the identity of the person where possible.
4. **Share with consent where appropriate** and, where possible, respect the wishes of those who do not consent to share confidential information. You may still share information without consent if, in your judgement, that lack of consent can be overridden in the public interest. You will need to base your judgement on the facts of the case.
5. **Consider safety and well-being:** Base your information sharing decisions on considerations of the safety and well-being of the person and others who may be affected by their actions.
6. **Necessary, proportionate, relevant, accurate, timely and secure:** Ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those people who need to have it, is accurate and up to date, is shared in a timely fashion, and is shared securely.
7. **Keep a record of your decision and the reasons for it** – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose. If you decide not to share, then record why.

The maximum value is gained from information when it is used to make sound decisions. Sharing or disclosure of information or making it public where this does not breach confidentiality enables the value of the information to be harnessed.

2. POLICY

2.1. Overview

The main purpose of the Confidentiality Policy is to ensure that data protection legislation is adhered to, and staff understand their responsibilities. A breach of this Policy could jeopardize the confidentiality of service users and the security of clinical information and could breach the Data Protection Act.

Breaches are to be reported as incidents and will be managed in line with the Incident Reporting and Management Policy. They will be investigated by the Service, supported by the Information Governance Team and in serious cases may lead to disciplinary action against staff or penalties against the Trust by the Information Commissioner's Office.

Any instances where it is suspected that fraud or bribery have taken place, will be reported to the Local Counter Fraud Specialist (LCFS) as soon as practicable and managed in line with the Anti-Fraud and Bribery Policy. For more information on how to contact the LCFS or NHS Counter Fraud Authority, please visit the Trust's Counter Fraud Intranet page

Confidential information can be used without explicit consent for direct healthcare purposes or the management of healthcare:

GDPR 2016 9(2)(h) – Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health profession.

(1)(d) – Processing is necessary to protect the vital interests of a data subject or another person.

6(1)(e) – 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.

Most processing of confidential data within the Trust does not require the explicit consent of the individual as it will fall under the following sections of the Data Protection Act

The Data Protection Act sets a very high standard for relying on consent to share information outside of direct healthcare purposes in that the Trust cannot rely on implied consent. Consent must be informed and freely given; it must also be unambiguous and involve a clear affirmative action (such as written or verbal). Consent must also be as easy to withdraw as it is to provide, and an individual has the right to remove their consent at any time.

Possible circumstances for disclosure of information without consent when the service user has capacity are when statute law requires us to do so, when there is a court order and when disclosure may be necessary in the public interest.

All requests to access records should be processed following the "Procedures for Trust Staff on How to Deal with Requests for Access

2.2. Definition of Terms

For clarity there are a number of terms the Trust will adopt in relation to confidentiality. These are explained in section 8 of the policy.

2.3. The Data Protection Principles

Article 5 of the Data Protection Act requires that personal data shall be:

- (a) Processed lawfully, fairly and in a transparent manner in relation to individuals.

- (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- (c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and Organisational measures required by the Data Protection Act in order to safeguard the rights and freedoms of individuals;
- (f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or Organisational measures.

Article 5(2) requires that:

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

3. PROCEDURE- ACHIEVING THE POLICY

3.1. Records/ Information covered

This policy covers all records/ documents that contain personal or confidential information. Confidential information within the NHS is commonly thought of as health information; however, it can include information that is private and not public knowledge or information an individual would not expect to be shared. It can take many forms including patient level health information, employee records, occupational health records, etc. It also includes BMSHFT confidential business information.

The Trust will also apply the duty of confidence to clinical records of deceased clients, as suggested by NHS guidance.

The storing, issuing and transferring of health (care) records (or part thereof) comes under the responsibility of the Head of Care Records (see Care Records Management Policy and Procedures).

3.2. Data Protection by Design and by Default

Data protection by design and default is mandated by GDPR and DPA 2018 ensuring privacy and data protection issues are considered at the design phase of any system, service, product or process and this consideration continues throughout the lifecycle.

It is of paramount importance that only the necessary level of information should be processed in order to be able to achieve a specific purpose, and the default position should always be to use anonymised data where possible. If more information is required to achieve the objective, consideration should be given to using pseudonymised information and finally use of the full record if no other option is suitable.

Safeguards need to be integrated into any processing of personal information in order to ensure the rights of individuals (data subjects) are protected.

To support data protection by design and by default, completion of a data protection impact assessment (DPIA) pre-assessment questionnaire (appendix one) must be completed and if required a full DPIA (appendix two) completed in the following circumstances:

- Introduction of a new paper or electronic information system to collect and hold personal data.
- Update or revision of a key system that might alter the way in which the organisation uses, monitors and reports personal information.
- Changes to an existing system where additional personal data will be collected.
- Proposal to collect personal data from a new source or for a new activity.
- Plans to outsource business processes involving storing and processing personal data.
- Plans to transfer services from one provider to another that include the transfer of information assets.
- Any change to or introduction of new data sharing agreements
- Introduction of new technology

The pre-assessment questionnaire and full DPIA if required should be submitted to the Data Protection Officer for review with final approval from the DPIA Review Group escalated for approval to the Information Governance Steering Group.

The DPIA includes a section regarding National Data opt Out and the steps that must be taken if applicable.

Please refer to the Data Protection by Design and by Default Procedure.

3.3 General Responsibility for Confidentiality

All employees, (substantive, agency, and contractor, temporary, those in partnership/ under contract, volunteers, students or apprentices) are responsible for maintaining the confidentiality of information whilst working within the Trust and after they have left the Trust.

Staff must only access personal information if they have a genuine 'need to know/ legitimate reason'. Unauthorized access or use of information will be investigated and may lead to disciplinary action and could be actioned under the Data Protection Act.

Everyone working for the Trust should be aware of their responsibilities in order to comply with law. (Including the Caldicott Principles)

All staff must ensure they know of, understand and apply recommended practical measures to maintain confidentiality when obtaining, sharing, storing or disposing of personal

information in different communication forms. The Trust has a number of procedures and guidance document for staff which are available on the Intranet.

In addition to the Data Protection Act 2018 and also Caldicott Principles, staff should be aware of the Computer Misuse Act 1990, which includes:

- Unauthorised access to computer material, which includes ID and password misuse, to alter, copy delete or move a program or data or simply to output a program or data, laying a trap to obtain a password.
- Unauthorised access to a computer with intent, this includes gaining access to financial or administrative records.
- Unauthorised modification of computer material including destroying another's files creation of a virus, introduction of a virus and any deliberate action to cause a system malfunction.
- Any examples of the above must be reported to the Head of Information Security and the Trusts Counter Fraud Specialist (CFS).

3.4 Training

IG training must be completed in line with the Fundamental Training Policy for all staff on an annual basis and more specific training can be requested via the Head of Information Governance.

3.5 Information Collection

As soon as an individual is accepted as either a potential service user or employee, records must be created. Staff are responsible for keeping these records accurate, up-to date, and confidential and ensuring they are not shared outside the Trust unless required to do so.

On initial contact with the Trust the service user must be given information, *orally* and in writing, explaining the Trust's requirement to keep records, how these may be shared and service users' rights to access their information (Trust privacy notice) along with their right to raise complaints or concerns directly with the Information Commissioners Office.

Care Coordinators/ Lead Clinicians must routinely discuss information recording and sharing with service users, carers and families to confirm understanding, identify any issues and provide an opportunity to discuss and concerns to sharing information. All such discussions must be documented in clinical notes.

3.6 Keeping Patients Informed

It is neither practicable nor necessary to seek the consent of a patient or other informants each time there is a need to share personal information. **Therefore, at their first appointments services users, carers and family need to be fully informed, unless exceptional circumstances dictate otherwise (these should be documented clearly within the patient record) to the best of our ability of how the information which they give may be used. This will be achieved in a number of ways;**

- The Trust will inform patients of the purposes for which information is collected, the legal basis for obtaining and processing their data and the categories of people/ organisations information may need to be passed on to. This is achieved by a privacy notice being available via the Trust's website although it should be noted that notices,

newsletters and other publicity materials are not considered sufficient on their own and all Trust staff are responsible for ensuring that patients are made aware of the potential to share information.

- Where information is required to be shared, patients are to be advised before they are asked to provide it and should have the opportunity to discuss any aspects that are special to their treatment or circumstances.
- Advice must be presented in a convenient form and be available both for general purposes and before a particular programme of care or treatment begins.
- In cases of multi-agency working for example, integrated health and social care teams, staff are required to ensure that a patient is fully informed who is part of the team, what information they will have access to and the legal basis for processing. There is a general duty on all health service bodies to act in an open and transparent way in relation to care and treatment provided to service users. This Duty of Candour is an NHS Standard Contract contractual duty and encompasses the principles of openness and transparency.

3.7 Secure Transfer of Personal Identifiable Information

All transfers of personal identifiable information are subject to strict governance and technical security controls. All staff intending to undertake in-bound and/ or out-bound personal identifiable information transfers must ensure it complies with all Trust policies including the ICT Policy

Staff must consider:

- a) what information is to be transferred (only transfer minimum information required for the purpose),
- b) purpose of transfer,
- c) nature of recipient,
- d) Method of transfer (e.g., is the email secure?),
- e) Physical and technical security measures proposed by the sender and the recipient.

3.8 Requests for Access to Information

Data subjects have the right of access to their own personal information. These rights are embodied within:

- The Data Protection Act – entitles individuals to a copy of personal information held about them (both manual and automated).
- Access to Medical Reports Act 1988 – in respect of reports prepared for employment or insurance purposes.
- The Human Rights Act 1998 – the means by which certain ‘rights and freedoms’ contained in the European Convention of Human Rights have become a direct
- Part of UK law.
- Access to Health Records Act 1990 – for applications relating to deceased persons only, right of access are to manual health records made after 1 November 1991 and earlier records if they are necessary to understand the later ones.

The Trust will always work on the principle of being open and accountable and look to share as much information with service users, the public etc.... as possible.

Individuals, or an appointed representative, have a right to request copies of personal data (e.g., staff records, clinical notes, complaints) under Article 12 of the Data Protection Act. We have a duty to check the validity of requests and once confirmed are legally required to

respond within 1 month of receipt of the request. Information on how to deal with requests is detailed in the [Information Governance](#) section on the Trust Intranet. In the first instance all such requests must be directed to the Information Legislation Requests Department.

Where a request to disclose personal information has been received and is considered appropriate, the decision to disclose, what to disclose and the reasons for this decision must be recorded. The current/ most recent clinician in charge for a service user or line manager for a staff member has responsibility for determining what information is disclosed- they are required to ensure the information is reviewed prior to disclosure and that no inappropriate information is released.

Guidance is available on reviewing records and the Trust process will ensure actions are monitored and logged for evidential purposes. When a service user gives consent to disclose information about themselves, clinicians should make sure that the service user understands what will be disclosed, the reasons for the disclosure, the likely consequences and record this information in the clinical notes. For more information regarding access to information requests please refer to [Access to Information Policy](#) (IG06).

If it appears a service user does not have capacity to consent to sharing of information, clinicians should carry out a formal assessment of capacity, recording this in the care records. If the test demonstrates a lack of mental capacity the clinician must ensure nobody else has a right to make the decision (such as a lasting power of attorney for welfare decisions or a Court of Protection appointed deputy). If there is nobody authorized to make the decision for the service user, the clinician should make a decision in the service user's best interests and record this decision on the appropriate form and in the service, user notes (see Mental Capacity Act 2005 Policy (C20)).

3.9 Regular Sharing

The Trust must agree an **Information Sharing Protocol**/ contractual arrangement with any partner organisation where it is anticipated regular information sharing will be required for personal data. The Service Lead in BSMHFT is responsible for ensuring a data privacy impact assessment is undertaken and a protocol is developed and approved prior to any sharing. All protocols must be logged centrally with the Head of Information Governance, who will review protocols prior to agreement and signing by the Caldicott Guardian.

The protocol will lay down the principles under which information can and should be shared, how the information will be shared (e.g., hard copy, electronic), security, and details of the information to be shared in line with legislation.

Staff being asked to release service user information must be familiar with the relevant protocol and only release the minimum information required to fulfil the obligation and meet the request, in line with the arrangements in the protocol. Protocols will recognize that the duty to share information can be as important as the duty to protect confidentiality and provisions exist to allow sharing in all appropriate circumstances.

Where an information sharing request is received from an agency with whom the Trust has no information sharing protocol the requests must be passed to the Head of Information Governance who will determine if there is a valid/ legal reason to disclose and acceptable conditions at the receiving organisation, consulting with Clinicians where appropriate. Any disclosure must only be made in line with this policy.

3.10 Disclosure without Consent

The Trust will work on the basis that sharing information to support service user care and prevent risk to data subjects or others is essential. It is not acceptable that the care a service user receives might be undermined because organisations do not share information effectively, in the majority of circumstances sharing will be necessary for the delivery of direct patient care, providing a patient has been fully informed and advised under section 3.5 of this policy, explicit consent will not need to be obtained. Sharing personal information effectively is a key requirement of good information governance and professionals should have the confidence to share information in the best interests of their service users; this means that sharing will happen without consent sometimes.

Under common law and in the best interests of the public, staff are permitted to disclose personal information in order to prevent and support detection, investigation and punishment of serious crime and/or to prevent abuse or serious harm to others where they judge, on a case by case basis, that the public good that would be achieved by the disclosure outweighs the individuals rights or freedoms under the Data Protection Act , the obligation of confidentiality to the individual patient concerned and the broader public interest in the provision of a confidential service. Staff can seek advice from the IG team or Caldicott Guardian on a case-by-case basis or request additional training if they are routinely making these decisions.

Decisions about disclosures of confidentially sensitive information must be made on a case-by-case basis. In considering whether to disclose staff should consider the merits of each case however, certain considerations will need to be taken in all cases:

- Extent of the information which is to be disclosed – *it will be easier to justify disclosure of demographic data or the fact that someone attended a clinic rather than detailed health information.*
- The nature and impact of the crime or harm justifying the disclosure - it will be easier to justify disclosure of information relating to a physical attack against a person than it would be for shoplifting.
- Whether the disclosure is for detection or prosecution of crime or harm to others or whether it is preventative - it may be more justifiable to disclose information to support prosecution in relation to a crime that has occurred than to prevent a crime which has not yet occurred.

A public interest justification for disclosure can be considered, and this guide becomes useful, in situations where:

- Disclosure would be in the public interest¹; AND
- The purpose of the disclosure cannot be achieved with anonymised information; AND
- There is no statutory basis for disclosure; AND
- Patient consent¹ has not been given because:
- It is not practicable to ask the patient(s) for consent e.g., because, for example, there are no up-to-date contact details for the patient, or the matter is urgent and the patient cannot be contacted; OR

¹ Known as Prevent- part of the Government counter-terrorism strategy. Prevent operates in the pre-criminal space. It is about supporting individuals who are at risk of radicalisation away from becoming terrorists or supporting terrorism.

- It would be inappropriate to ask the patient(s) because, for example, they lack the capacity to give consent, or they are suspect(s) who should not be informed that they are under criminal investigation, OR
- The patient(s) have been asked for consent and refused.

The courts, including coroner's, some Tribunals and persons appointed to hold inquiries have legal powers to require disclosure of information that may be relevant to matters within their jurisdiction. This does not require consent of the service user; whose records are to be disclosed. Such disclosures must be strictly in accordance with the terms of a court order and should only provide required information to the bodies in the order.

Disclosures in the public interest may be necessary to prevent serious crime or risk of significant harm. Public interest is described as exceptional circumstances that justify overruling the right of an individual to confidentiality in order to serve a broader societal interest. Decisions about the public interest are complex and must take account of both the potential harm that disclosure may cause and the interest of society in the continued provision of confidential health services. An example of this is sharing information to Prevent terrorism² (Prevent.) Data collected about people for the purposes of Prevent must be necessary and proportionate. The Channel guidance, Prevent works to, provide.

A clear statement about the information sharing principles and legislative framework for Channel and covered the following areas:

- Necessity and proportionality: personal information should only be shared where it is strictly necessary to the intended outcome and proportionate to it.
- Consent: wherever possible the consent of the person concerned should be obtained before sharing any information about them. In the absence of consent personal information cannot be shared without satisfying one of the gateway or exemption conditions.
- Power to share: the sharing of data by public sector bodies requires the existence of a power to do so, in addition to satisfying the requirements of the Data Protection Act and the Human Rights Act 1998.
- Data Protection Act and the Common Law Duty of Confidentiality: in engaging with non-public bodies, the Channel coordinator should ensure that they are aware of Their own responsibilities under the law.

“Serious crime” is not clearly defined in law but will include crimes that cause serious physical or psychological harm to individuals. This will include murder, manslaughter, rape, treason, kidnapping, and child abuse or neglect causing significant harm and will likely include other crimes which carry a five-year minimum prison sentence but may also include other acts that have a high impact on the victim.

Alternatively, theft, fraud or damage to property where loss or damage is not substantial are less likely to constitute a serious crime and may not warrant breach of confidential information, though proportionality is important here. It may, for example, be possible to disclose some information about an individual's involvement in crime without disclosing any clinical information.

Disclosures to prevent serious harm or abuse also warrant breach of confidence. If gaining consent would delay or put individuals at increased risk, information can be shared on the

basis of 'vital interests' of the individual(s).² The risk of child abuse or neglect, assault, or the spread of an infectious disease are perhaps the most common staff may face. However, consideration of harm should also inform decisions about Disclosure in relation to crime. Serious fraud or theft involving NHS resources would be likely to harm individuals waiting for treatment. It is also important to consider the impact of harm or neglect from the point of view of the victim(s) and to take account of psychological as well as physical damage.

There are also cases where disclosure of information may be in the public interest for a reason unrelated to serious harm or crime. The decision to disclose must take account of the likelihood of detriment (harm, distress or loss of privacy) to individuals concerned, but a proportionate disclosure may be acceptable where there is clear benefit to the public. The key factors in deciding whether or not to share confidential information are **necessity and proportionality**. The disclosure of personal information must be necessary in order to satisfy an important public interest. Public interest must be judged on the merits of the case. Such a defence is only applicable in limited circumstances; public interest does not mean "of interest to the public".

Health professionals must objectively assess public interest (e.g., through conferring with colleagues). Colleagues may identify additional factors to consider and assist in weighing up the options. Where appropriate the Caldicott Guardian should be involved.

Seeking such advice may not be practicable in cases where the decision is urgent and there are no suitable colleagues available.

Disclosure should be to the appropriate person(s), and the confidential information provided should be limited to that necessary to fulfil the purpose of the disclosure. It may be possible to restrict the contents, recipient(s), or conditions of disclosure to limit the detriment caused but still achieve the public interest aim so that the disclosure is proportionate.

A fair balance should be struck between the rights of the individual and potential damage to the relationship between the health professional(s) and the service user, and the potential impact of the service user terminating that relationship. This will be a professional judgement made on the basis of the information they have to hand.

In circumstances, where it is difficult to make a judgment, staff should contact the Head of Information Governance or seek legal or other advice through Trust Legal Services. Should a request be submitted out of hours and an urgent decision be needed staff should discuss with the on-call Director prior to the sharing of any information.

1 Disclosure of the information must result in public benefit; this is not the same as something being of interest to the public (e.g., a scandal).

2 Or those empowered to make decisions on behalf of the patient, which for an incompetent child is a person with parental responsibility, and for an adult lacking capacity it is someone empowered to make decisions under the

Mental Capacity Act 2005 (see in particular paragraph 3 of the Act available at:

http://www.opsi.gov.uk/ACTS/acts2005/ukpga_20050009_en_2#pt1-pb2-l1g3).

² E.g., where a child or vulnerable adult may be in need of protection, at risk of death or serious harm. Professionals who have such concerns should draw them to the attention of the relevant authorities.

⁵

3.11 Sharing information with the Police (Appendix 7)

The Police may ask you to provide them with information about members of staff, patients and service users to support their work. There are times when this information:

- Must be provided to the police because the law requires it to be disclosed(e.g. there is warrant for disclosure)
- Information may be provided to the police because it is important in relation to the prevention or detection of a serious crime(rape, murder, etc) and there is substantial public interest in the disclosure . In this instance it may not be appropriate to inform or ask the patient or service user for consent.

Staff should be aware that police disclosures should be made on a case-by-case basis and if they cannot identify a lawful reason which outweighs the duty of confidentiality to the patient for sharing the information then they should seek advice from Data protection officer or the Caldicott Guardian for the Trust.

Police should present a completed WA170 form when requesting information.

When Information by the Police is requested the following should be considered

Is the request a mandatory or voluntary request?

If the Police request is in the form of a warrant, BSMHFT will have no choice but to respond accordingly and disclose. More often than not however, the Police request is not a mandatory demand for information and therefore it should not be assumed that we must automatically disclose the personal data requested. It is for BSMHFT to determine whether it wishes to assist the Police by providing this personal data. This could be a request for information about employees, patient records or a copy of CCTV recording etc.

Any request must be considered on the merits of its own facts and circumstances. While we may wish to be helpful to the Police, one ought to also consider the impact this could have on the individual concerned and also how it would affect the disclosing clinicians/staffs/organisations relationship with the individual and wider public from a trust perspective. Would disclosure be in the reasonable expectation of the individual concerned? Any disclosure must also be permitted under GDPR or DPA.

Does the GDPR/DPA permit sharing with Police?

While each case will turn on its own facts, the GDPR/DPA generally allows organisations to disclose personal data to the Police where this is deemed necessary (a) for the prevention or detection of crime; or (b) the apprehension or prosecution of offenders. These provisions could permit disclosure even if there is no legal obligation to disclose (e.g., under a warrant) and/or such disclosure is not covered in any applicable privacy notice.

If permitted, are other parts of GDPR/DPA still applicable?

Even where an organisations is of the view it can disclose the personal data to the Police, remaining parts of the GDPR and DPA are still relevant and must be considered. Indeed the organisation would need to establish and document a legal basis for this sharing under Article 6 of GDPR (e.g., legitimate interest of the Police or public interest). To the extent that the requested information consisted of special category data (e.g., health care records data), it would need to also establish a legal basis under Article 9 (e.g. Substantial Public Interest).

Should all personal data requested be disclosed to the Police?

The recipient organisation(BSMHFT) should only hand over personal data/documents that is actually necessary, relevant and proportionate for the requirements of the Police investigation as opposed to automatically giving the Police access to everything they request.

It is important that should this situation arise that we/the organisation ask the Police to document what they need and why this information is relevant as this will enable the request to be restricted where appropriate. It will also create a paper trail which could be helpful if the disclosure is ever challenged. It will be important for the organisation to be able to establish the legal basis it relied on and that it only shared information that was actually necessary for a clear purpose as outlined by the Police. Lastly, the organisation should also be mindful how it shares the personal data with the Police in a practical sense and ensure it does so in a secure manner, particularly given the information is sensitive.

What should staff do if they receive a request for information from the Police?

The Police could ask any staff member to disclose information to them. To ensure that our organisation can give the request proper consideration, it is important that staff contact the IG team / data protection officer or Caldicott guardian and seek advice. With regard to patient information normally any such request would be handled by a senior member of staff i.e. consultant Psychiatrist involved in the care of the patient or Band 8 or above member of clinical staff with support by the Data Protection Officer or Caldicott guardian or member of IG team with data protection experience.

Please also refer to the Police Interventions Policy

3.12 Research and National Clinical Audit

If information is required for medical research, audit or planning purposes, staff should always evaluate each project and determine whether personal identifiable information or confidential patient information is needed for such purposes.

Unless there is genuine justification, all personal identifiable information described in this policy should be taken out to anonymise the data for research purposes.

Article 89 of the Data Protection Act states the principle of minimizing use of personal identifiable data in research and related activities and recognises pseudonymisation - a procedure by which the most identifying fields within a data record are replaced by one or more artificial identifiers, or pseudonyms – as a tool for minimizing use of identifiable data while still distinguishing between separate individuals within study data sets. Staff wishing to pseudonymise records can seek advice from the Trust's Information Team

There may be exceptional circumstances, where the use of patient identifiable information and confidential patient information in research and clinical audit outweighs issues of privacy for public good. The Confidentiality Advisory group of the Health Research Authority has been given the powers provided under Section 251 of the NHS Act (2006) (formerly Section 60 of the Health and Social Care Act 2001) in such circumstances. It is important to note that Section 251 permits the temporary setting aside of the common law duty of confidentiality but does not set aside the requirements of the Data Protection Act.

If staff identify a potential application of Section 251 of the NHS Act (2006) prior to ethical approval of a project, the case should be made to the Caldicott Guardian following the initial approval, who will assess each S251 case individually and refuse or accept the initial

decision by the Confidentiality Advisory Group under Health Research Authority, to disclose the required information for research without consent for the public good.

All staff must keep personal identifiable information and confidential patient information secure at all times. Associated researchers should clarify in research proposals the arrangements to obtain permission to access clinical information. Once explicit consent is obtained, researchers can use clinical information to conduct research.

3.13 National Data opt Out for Research, National Clinical Audit and Planning

The national data opt-out enables patients to opt out from the use of their confidential patient information for research or planning purposes by using an online service. Patients can view or change their national data opt-out choice at any time.

Confidential patient information is defined in section 251 of the National Health Service Act 2006 as information that meets all of the following three requirements:

1. Information that is identifiable or likely identifiable (for example from other data likely to be in the possession of the data recipient); **and**
2. Information that is given in circumstances where the individual is owed an obligation of confidence; **and**
3. Conveys some information about the physical or mental health or condition of an individual, a diagnosis of their condition; and/or their care or treatment.

The national data opt-out **does not apply** to:

1. Information that is anonymised in line with the Information Commissioner's Office (ICO) Code of Practice on Anonymisation or is aggregate or count type data.
2. Workforce or staff data.

As confirmed by the ICO, pseudonymised personal data remains personal data within the scope of GDPR and thus falls within the scope of the national data opt-out.

With respects to research and national clinical audit, national data opt-out applies to a disclosure of confidential patient information when a research or audit team confirms they have approval from the Confidentiality Advisory Group (CAG).

CAG approval, also known as a section 251 approval, enables the common law duty of confidentiality to be temporarily lifted so that confidential patient information can be disclosed without the data controller being in breach of the common law duty of confidentiality (i.e., without obtaining individual service user consent). **It is only in these cases where opt-outs apply.**

The national data opt-outs **do not apply** in the following situations:

1. If a patient has agreed to a specific use of data for a research or national clinical audit study, after being fully informed, then the national data opt-out does not apply. Even patients who have registered a national data opt-out can agree to take part in a specific research project or clinical trial, by giving their explicit consent.
2. The national data opt-out does not apply to the disclosure of confidential patient information required for the monitoring and control of communicable disease and other risks to public health.
3. The national data opt-out does not apply to the disclosure of confidential patient information where there is an overriding public interest in the disclosure, i.e., the public interest in disclosing the data overrides the public interest in maintaining confidentiality.

The national data opt-out does not apply to the disclosure of confidential patient information where the information is required by law or a court order.

Where it has been identified that national data opt out applies, the Information Department will apply the national data opt-out prior to providing any information via NHS Digital's technical solution.

3.14 Information Storage

Appropriate security arrangements must be in place to ensure that files are protected from unauthorised access and disclosure and from loss and destruction (see ICT Security Policy and/ or Care Records Management Policy).

Storing information electronically means that access to this information could be more widely available and therefore additional safety measures will be put in place:

- Every user requiring access to a patient system will be given a unique user id and password that must not be shared.
- staff will be required to sign a network access agreement form in which they accept responsibility for confidentiality and information security while using Trust systems (additional requirements will be covered in the Trust Information Systems Security policy)
- Staff will be required to read and accept a confidentiality agreement/ notice when logging into the Trust network and, where possible, to individual applications.

Only ICT approved and Trust issued electronic systems must be used to store personal information (a list of approved systems is held by the ICT Department). No non-Trust issued media is permitted to be attached to Trust equipment or used to transfer Trust information. Trust encrypted memory sticks can be requested from ICT. Only under exceptional circumstances will personal devices be allowed to be used, for instance during a global pandemic such as COVID-19, but this use must be approved by ICT.

Electronic systems must be password protected (in line with Trust standards) and must have a robust back-up and recovery strategy in place to ensure the ability to recover from unexpected data loss with minimal impact on the Trust business.

Manual confidential/ personal files or information must be locked away when not in use, E.g., locked filing cabinet, secure office.

This also applies to both internal and external systems and is the responsibility of the information asset owner.

3.15 Transferring Information Securely

Where personal identifiable information needs to be shared electronically safeguards must be in place to ensure confidentiality (e.g., use of NHS.net (secure email) or encrypted devices). Advice is given in the Safe Haven Procedures, ICT Policy or by contacting the ICT Service Desk.

Refer to the Care Records Management Policy for further information on transferring Care (Health) Records securely.

3.16 Disposing of Confidential Information

Disposal of Trust records must be in accordance with the NHS Records Management Code of Practice and the Trusts Corporate Records Management Policy.

Where confidential information needs to be disposed, care must be taken to ensure it is destroyed safely so that confidentiality is not breached (see Disposal Guidelines).

Disposal of confidential information on magnetic media (e.g., CDs, DVDs, memory sticks) must follow Trust ICT Department procedures.

All Information sharing agreements and contracts relating to the sharing of information must contain provisions on data retention and set out not only how long information will be retained for but also how it will be disposed of and whether certificates of destruction are required.

3.17 Handling of Confidentiality Breaches/ Incidents

All breaches of information governance must be recorded onto the Trusts incident reporting system Eclipse in line with the Incident Reporting and Management Policy.

If a reasoned disclosure without consent has been made under section 3.10 of the policy, you must inform the Information Governance Team or Caldicott Guardian so this can be recorded on the Caldicott Log.

Under article 33 of the Data Protection Act the Trust is required to report all serious breaches of confidentiality to the Information Commissioners Office within 72 hours and failure to do so may result in the Information Commissioner's Office issuing a monetary penalty to the Trust.

Reporting to the Information Commissioner's Office can only be done via the Information Governance Team with agreement from either the SIRO, Caldicott Guardian or Associate Director of Performance and Information.

If you suspect that a serious breach has occurred, you must raise this on the Trust's internal Eclipse incident reporting system within 24 hours.

The Information Governance Team will support local team investigations for all information governance incidents, including serious information governance incidents. Learning from information governance incidents will be shared with relative teams and significant Trust wide learning will be included within the information governance awareness sessions.

Root cause analysis methodologies, such as five why's and the cause-and-effect model (appendix five) will be used to aide investigations following a serious information governance incident as in line with the process described in the Trust's Reporting, Management and Learning from Incidents Policy.

Nominated senior managers will formally investigate serious breaches and where appropriate use the Trust's Disciplinary Procedure.

Staff who breach this Policy may be subject to disciplinary action which could lead to dismissal.

3.18 Access / Sharing of Confidential Information

Staff will be required to read and accept an ICT acceptance screen when logging on to the Trust network; which includes confidentiality; and, where possible, to individual applications as well.

In order to protect confidentiality:

- Service user information must not be disclosed under any circumstances for the purposes of fund raising or commercial marketing, although the Trust or its agents may do so with explicit consent from the service user.
- Care should be taken that images of Trust sites and services (e.g., photos) do not identify service users or staff members without their permission.
- Although there is no legal obligation to keep personal information confidential after the death of a person there is an ethical obligation and ongoing duty of confidentiality for NHS organisations to do so (see NHS Confidentiality Code of Practice). This duty of confidentiality will in most cases reduce over time. Information about a deceased person should only be passed on with the consent of their executor (such as next of kin, solicitor or someone with written confirmation that they are administering the deceased Estate). Access requests to health records for a deceased person can also be made under the Access to Health Records Act 1990.
- Anybody providing services to the Trust who is not a substantive employee, temporary staffing member or covered by a contract/ sharing protocol will be required to sign a Local Confidentiality Agreement.

3.19 Remote Working and Maintaining Confidentiality

Whilst the Trust is supportive of remote working, including staff working from home, the need to adhere to information governance policies, and staff understanding their own information governance responsibilities remains of paramount importance. Patient and confidential information should be treated in same manner, ensuring appropriate safeguards and policy requirements are satisfied, regardless of whether a member of staff is working on a Trust site or remotely, including working from home. When working remotely and accessing patient and confidential information, all staff must adhere to the following additional requirements:

- Only use Trust issued equipment to access the Trust Network. The Trust does not allow for remote access with non-Trust devices and if any equipment is required, the ICT team must be contacted. ICT is developing new and more flexible ways to securely connect to the Trust network. If you are planning to use any personal device, first check with ICT. Only use approved ways of connection to the Trust network and systems.
- Staff must ensure their own Wi-Fi connection is secure.
- Trust equipment must only be used for Trust business and not for personal use.
- If any Trust equipment or patient clinical records are taken home, they must be stored securely and not left in cars. Staff will take full responsibility for the safe keeping of Trust equipment and clinical records ensuring they cannot be accessed inappropriately (please refer to the Safe Haven Guidance).
- All Trust Information Governance policies must be adhered to when working remotely (including working from home), and the best way to ensure staff understand their information governance responsibilities is by completion of the mandatory annual Information Governance training.

- Staff need to be vigilant of phishing risks and to not open any suspicious emails or click links or open attachments in emails and video chat that they suspect may be a security risk.
- Staff must ensure that their work area at home or other remote location, is secure and that privacy and security is maintained for all their daily work tasks, including reviewing and responding to emails, accessing patient and staff records, accessing confidential information and making and receiving telephone calls. Staff will need to ensure computer screens are not easily visible to others, no confidential, patient or staff information is viewable during video calls and consultations, and telephone calls can be made in a area where the member of staff will not be overheard.
- Patient and members of staff privacy rights must always be respected.

3.20 Video Conferencing

A key area of working remotely, including working from home is the use of video conferencing applications which provide staff with the ability to conduct remote meetings with colleagues and hold clinical consultations with patients, and also hold group therapy sessions.

The key benefits of using video conferencing applications include:

- Saving time by reducing time spent travelling to and from meetings.
- Enabling staff to stay in more frequent face to face contact with patients, providing consultations and therapy in a more accessible way which is of particular benefit to patients who may have mobility issues and have previously struggled to physically attend appointments.
- The ability to quickly organise real time face to face meetings for critical decision making.
- Allowing staff to work from different locations, including home.
- Saving money by reducing travel and expenses costs
- Environmental benefits - a reduction of CO2 emissions

To support staff in the secure use of video conferencing, there are information governance considerations that staff need to be aware of when arranging or attending video meetings:

- If you are asked to join a meeting using an application you are unfamiliar with, ask ICT if it is safe to use.
- Check that only the correct people have been invited to the meeting. Any unexpected attendees must be asked to leave the meeting to avoid a data breach.
- Be aware of privacy settings in any software being used - for example using the default 'private' setting within Microsoft Teams rather than changing to 'public'.
- If you need to share personal/confidential patient information during your video call you should apply the same principles you would at any other time, i.e., adhere to the Caldicott Principles, only share the minimal necessary information, consider whether all participants of the meeting need to have the information.
- Established procedures of confirming the identity of a patient or their representative

- Patients must be made aware of their responsibilities when using video conferencing,
- i.e., they should ensure they are in a private area where no one can overhear them. Advise patients to not have any of their personal information displayed in the background, for example photographs of their children or information containing their home address. Patients also need to be advised not to share their meeting login details with anyone else.
- Staff need to consider whether anyone else can overhear their conversation. Only relevant colleagues or the patient themselves should be able to hear the conversation, particularly if patient data is being discussed.
- Staff must ensure that there is no confidential information on display that may be seen when video conferencing.
- Staff must ensure that only the correct individuals attend a video conference meeting if patient data is being discussed.
- Staff should be aware that patients have a right to record their consultation as it is classified as their data.
- Video consultations are still consultations and appropriate updates must be made to a service users record.
- Staff should be aware that if they are considering the use of a new video conferencing platform, they should complete a Data Privacy Impact Assessment. This will provide assurance that use of such a solution will be secure and that the privacy of service users will be maintained.

3.21 Children and Young People

Young people aged 16 and over are regarded as adults for purposes of consent to treatment and are therefore entitled to the same duty of confidence as adults.

Children aged 13 and over who have the capacity, maturity and understanding to take decisions about their own treatment are entitled to decide whether personal information may be passed on and generally to have their confidence respected (for example, they may be receiving treatment or counselling about which, they do not wish their parents to know). This right is supported under the Data Protection Act 2018 and is also commonly referred to as the Gillick Competence. Gillick competence should be made on a case-by-case basis, considering age, experience, and ability to weigh up the information. However, the child should be encouraged to involve parents or other legal guardians. If sharing info is deemed to be in the child's best interests, even if it goes against their wishes, it may be necessary to do so.

Generally, children between the ages of 0-12 will not have the capacity to withdraw consent for their information to be shared with their parents or guardians, any such decision to do so can only be made with the approval from the Trusts Caldicott Guardian.

Services which are provided to children must create specific privacy notices which are understandable to children, therefore written in clear, simple language, brief and concise.

In other instances, with regard to children, decisions to pass on personal information may be taken by a person with parental responsibility in consultation with the health professionals concerned.

Under the Children Act 2004 key people and bodies have the duty to make arrangements which ensure their functions are discharged with regard to the need to safeguard and promote the welfare of children. This extends to the member agencies of the Local Safeguarding Children's Board and services they commission. Information sharing is fundamental for complying with this statutory regulation. Child protection is an area where information may be shared without the consent of the child or their parent. In child protection cases, if the health professional (or other member of staff) has knowledge of abuse or neglect relevant information will be shared with others on a strictly controlled basis so that decisions regarding the child's welfare can be taken in the light of all relevant information.

When information regarding an individual indicates that a child may be at risk from that individual there is a duty to share that information with the appropriate agency.

3.22 Complaints

Complaints from patients regarding confidentiality of their information will be dealt with through either the Trust's complaint procedure or the health professionals' administrative bodies, with support from the Information Governance Team. The Trust will support and inform individuals of their statutory right to complain to the Information Commissioner, as well as rights to take action for compensation if the individual has suffered damage (physical and/or mental) as a result of the breach of confidentiality. Also, to have any inaccurate personal information corrected or erased.

3.23 Sharing Information with Relatives, Friends and Carers

Clinical teams and individual professionals must ensure that families and carers are actively engaged as part of our duty of care to our service users.

Clinicians should have discussions with service users about the benefits to them when information is shared with family and friends.

How this discussion is held will be the main factor in whether consent is given by the service user. Clinicians should explore any reservations the service user may have, and negotiate with the service user about what they do, and do not want shared with others. If a service user refuses to share any information with family and friends, this should be noted, but should not end the process of negotiating with the service user.

Lack of consent to share information should not terminate the relationship the family member or carer has with the clinical team, nor impact upon routine, positive engagement of families and carers. Professionals should continue to provide an active welcome to families and carers, along with support and engagement without breaching confidentiality. This can be done through provision of high-quality information, advice and assistance on the management and support for their treatment. Clinicians should actively engage with the needs of carers and families in their own right, as caring for an individual with major mental health issues requires stamina and resilience and can impact upon mental health.

Clinicians should, where appropriate, encourage a service user to consent to sharing information with families and carers to support their care and ensure that a service user is informed they can consent to certain aspects of their information being disclosed whilst not consenting to others. For example, consenting to information about care and treatment being disclosed but not about social activities or relationships. Gaining consent is not a "one off" activity and needs to be part of regular conversation with service users.

Special care and attention is required regarding the area of information sharing and risk. Risk refers to risk to the service user, directly to families and carers and more widely to the community. Serious incident reviews and Domestic Homicide Reviews indicate that poor information sharing with family and carers, and lack of engagement with families and carers who are wishing to share risk information has at times led to catastrophic events, at times leading to the death of service users and to family members. It is critical that we protect families and carers where risks may present, also that they can share concerns about risks that may be escalating with clinical teams, and be confident these concerns will be heard and acted upon. Special care and attention is required regarding the area of information sharing and risk where there are domestic abuse concerns.

Clinicians should bear in mind that, when information is shared with family and friends, this can help to create a collaborative relationship, which is mutually beneficial for all working together can create consistency in the support for the service user. A lack of information being shared with family and friends can create challenges in relationships between the service user, their family and the clinician. A proactive discussion with service users about information being shared can mitigate against this.

In this context, the term '**carers**' relates not only to a patient's family or friends who may assist and provide care to the patient on a regular basis but can also refer to a residential home or healthcare team who are at that time, involved in caring for the patient and may therefore be given information about a patient unless the patient has indicated otherwise. Explicit consent should be sought wherever possible, and the individual's wishes recorded in the hospital case notes.

3.24 Staff taking Audio and Visual Recordings of Patients for Direct Care or Secondary Use

When undertaking any audio or visual recording of patients, particular care must be taken to respect patients' dignity and privacy. There must be a fully justifiable purpose for an audio or visual recording to be carried out.

Legal Basis

Making an audio or visual recording for patient care is classed as processing personal data and therefore subject to the provisions of data protection legislation.

Under the GDPR, the legal basis for processing information relating to **patient care** is **Article 6(1) (e)**. Because information relating to patient care constitutes special category personal data, the Trust must also identify a legal basis in Article 9 which is **Article 9(2) (h)**; that processing is necessary for the provision of health or social care.

It is not necessary to obtain consent from patients to make an audio or visual recording for patient care.

Explicit consent should still be obtained when using recordings for secondary use, such as teaching, training and for publication. This consent should be retained within the patient's clinical record.

Patient's must be informed that they can withdraw their consent at any time, and the clinician or lead manager, who took the original consent must have a process in place to

ensure the audio or visual recording can be deleted by all those who have received or saved a copy. This same clinician or lead manager must also request confirmation that the recordings have been deleted.

3.25 Audio or Visual Recordings taken by Trust Staff for Purposes other than Patient Care

It is good practice and courteous to inform staff at formal meetings that a recording is taking place (usually for the purpose of minute taking), although explicit consent is not necessary as the recording will be capturing staff acting in a professional capacity.

Recordings are often taken at organised events and can be published on the internet. Organisers of events should ensure that delegates know that recordings are taking place and be given the opportunity to opt out if they wish to do so.

If staff wish to take team photographs in a clinical environment, then this is permitted as long as care is taken to ensure there is no risk to patient confidentiality.

Patients attending complaint/concern/feedback meetings where the recording would not form part of the patient record should provide consent for the recording to take place and be given assurance on the purpose for the recording, the storage and retention arrangements.

Staff should seek prior consent if they wish to record other events, including 1:1 meeting, regular management supervision, sickness discussions, appraisals etc. Consent should be sought from the chair of the meeting and if consent is not granted, then the recording should not go ahead.

3.26 Staff Use of Personal Mobile Phones and Cameras

The Trust has an obligation to provide a safe environment to deliver care.

Staff should be aware that personal mobile phone/cameras should not be used for private use in areas where care is delivered and where patient confidentiality could be compromised and should therefore make use of more suitable areas.

Staff must be vigilant when taking a mobile phone into an area where care is delivered, even if it is not being used at the time, i.e., in a pocket in order to prevent incidents of inadvertent live streaming on social media.

It is not usually permitted to take any type of patient recording on personal mobile phones. However, in exceptional circumstances where there is no Trust owned equipment available and the situation is time critical, then the recording can take place as long as a risk assessment is carried out.

Staff that have no option but to make a recording on their own personal device must upload the recording to the Trust network as soon as possible and ensure it is permanently deleted from the device and cannot be recovered. It is the responsibility of the staff member to ensure that features such as “recently deleted items” and cloud storage backups have not inadvertently stored the recording.

Recordings should not be sent over a mobile phone network to another device, nor should they be emailed outside NHSmail, transferred via instant messaging such as WhatsApp or published on social media.

3.27 International Transfers of Personal Data

The Trust may sometimes use service providers who process information in other countries, both within and outside the European Economic Area (EEA). Because of this it may sometimes be necessary for personal data to be transferred overseas. However, before any transfer is made appropriate safeguards must be implemented to ensure that the transfer of the data, its processing, storage and retention are securely controlled and in full compliance with the requirements of the GDPR. The Information Governance Team must be contacted prior to any international transfers of data commencing.

4 ROLES AND RESPONSIBILITIES

Post(s)	Responsibilities	Ref
Caldicott Guardian	The Medical Director is the Caldicott Guardian. The Caldicott Guardian has accountable for the safe management of patient data. However, each member of staff is responsible for patient confidentiality.	
Senior Information Risk Owner (SIRO)	The SIRO is the Executive Director of Finance, and a mandated role which has overall responsibility for managing information risk across the Trust. The SIRO is a member of the Executive team and is assisted by; <ul style="list-style-type: none"> • The Trust's Data Protection Officer- the Head of Information Governance • The Trust's Deputy SIRO- Associate Director of Performance and Information • The Trust's Information Systems Security Officer- Head of ICT • The Head of Information Governance • An Information Asset Owner will be identified for each of the Trust's critical information assets. 	
Head of Information Governance / Data Protection Officer	This role will lead the Information Governance agenda for the Trust and is managerially accountable to the SIRO. They will have day to day operational responsibility for all aspects of Information Governance (except specific elements of information security and data quality). This role holds the post of the Data Protection Officer under the new Data Protection Act to fulfil the statutory functions and responsibilities of that role, including providing leadership, challenge and support to achieve organisational compliance.	

Information Asset Owners	Information Asset Owners (IAO) are individuals involved in running/ administrating relevant systems - asset. Their role is to understand what information is held, identify the legal condition/basis for processing the data, what is added and what is removed, how information is moved, and who has access and why. As a result, they are able to understand and address risks to the information and ensure that information is fully used within the law and confidentiality and provide written input to the SIRO on the security and use of their asset.	
Managers	It is the responsibility of managers and supervisors of temporary staff, students and contractors who have access to sensitive personal information to ensure staff are aware of the need for confidentiality under the Data Protection Act and complete annual IG training. Managers and supervisors must make individuals aware of the guidelines that need to be followed in the handling of all sensitive personal information. Any staff not signed up to NHS Terms and Conditions must sign a Local Confidentiality Agreement	
All Staff	<p>All members of staff must be aware of the confidential nature of their work and sensitive information they may come across. All staff are provided with an introduction to Information Governance standards during their corporate induction and are expected to familiarise themselves with organisational policy in relation to these issues.</p> <p>All staff are required to undertake mandatory information governance training on an annual basis.</p> <p>Breach of confidentiality may result in disciplinary action in accordance with the disciplinary policy and is seen as a serious offence which will be treated as gross misconduct and could result in dismissal. (See Disciplinary Policy)</p>	

5 DEVELOPMENT AND CONSULTATION

Consultation summary	
Date policy issued for consultation	February 2025
Number of versions produced for consultation	1
Committees / meetings where policy formally discussed	Date(s)
Information Governance Steering Group	February 2025
PDMG	May 2025

Where received	Summary of feedback	Actions / Response

6. REFERENCE DOCUMENTS

In writing this policy the author has made reference to the following documents:

- General Data Protection Regulations and Working Party 29 guidance
- Common Law of Confidentiality
- General Data Protection Regulation 2016 4. Data Protection Act 2018 (DPA18)
- Human Rights Act 1998 (HRA98):
- Freedom of Information Act 2000
- Access to Health Records Act 1991
- Computer Misuse Act 1990
- Administrative Law
- Caldicott Review 2013
- Confidentiality NHS Code of Practice 2003 (And supplementary guidance dated November 2010)
- Confidentiality: Protecting and Providing Information (GMC 2017)
- Mental Capacity Act 2005
- NHS Act 2006

7. BIBLIOGRAPY

There are a range of statutory provisions which limit or prohibit the use and disclosure of information in specific circumstances and, similarly, a range of statutory provisions that require information to be used or disclosed. The following legislation and national guidance is relevant when considering whether confidential information should be accessed and/or disclosed and has been taken into account in the creation of this policy.

- [Common Law of Confidentiality](#) **
- [General Data Protection Regulation 2018 \(GDPR\)](#) **
- [Human Rights Act 1998 \(HRA98\)](#) **
- [Freedom of Information Act 2000](#) **
- [Access to Health Records Act 1991](#)
- [Computer Misuse Act 1990](#) **
- [Caldicott Principles \(revised 2013\)](#)
- [Confidentiality NHS Code of Practice 2003](#) ** (And supplementary guidance dated November 2010)
- [Confidentiality: Protecting and Providing Information \(GMC 2017\)](#) [Data Protection Act 2018](#)
- [Fraud Act 2006](#)
- [Bribery Act 2010](#)

(Note: ** indicates that this legislation and guidance equally applies to service user records, staff records or records relating to third parties)

This policy is in line with best practice advice given by regulatory bodies to their registered health professionals (e.g., Royal College of Psychiatrists). It is re-enforced by the guidance on the need to protect confidentiality of patient information held on electronic systems which was issued jointly by the NHS, GMC and the Information Commissioner (Joint

Guidance on use of IT Equipment and Access to Patient Data – DoH 25 April 2007). These state:

‘No IT system can be immune to inappropriate use by individuals who have been authorised to use the system and to access data. It is important therefore that all those who are provided with such authorisation by virtue of their role in delivering or supporting the delivery of care, understand and meet the standards of behaviour that are required by law and professional codes’.

It concludes:

‘The General Medical Council, Information Commissioner and the Department of Health have agreed this joint statement to ensure that all those who have access to patient information in the course of their work are clear about what is expected of them. The Department of Health has strongly supported the Information Commissioner’s call for stronger penalties to apply where individuals obtain information unlawfully, and the law is to be changed to provide the possibility of a custodial sentence for those found guilty’.

8. GLOSSARY/ DEFINITIONS

Commercially sensitive information

This is non-personal information (therefore not covered by the Data Protection Act), which may be sensitive to the Trust (e.g., some financial information) and therefore must be kept confidential.

Confidential Information

Information which can be classified as ‘**confidential**’ is defined as information of a specific and personal nature about service users, their families or friends and carers, our employees and their families (e.g., health information, complaints, references etc.) and other persons who are in contact with the Trust. In the context of Trust services, the simple fact of referral to a service would meet this definition and therefore all personal data held should be so classified.

‘Confidential information’ covered by this policy includes any information that has not been fully anonymised. If the name and address are not present but an NHS number is, then this is considered to be pseudo-anonymous, because it is still possible for the person to be identified (the NHS number is a unique identifier given to each person in England and Wales). Similarly, presence of date of birth and postcode may be sufficient, in combination with other information, to identify an individual. When producing statistical analyses, it is important to not present data at too disaggregated a level as this may also lead to individuals being recognisable and others being able to infer confidential information.

Data

Data means information which –

1. is being processed by means of equipment operating automatically in response to instructions given for that purpose,
2. is recorded with the intention that it should be processed by means of such equipment,
3. is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system,
4. does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68, or

5. Is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d).

Emergency Situation

Situations which involve emergency services working with our staff (e.g. the evacuation of one of our inpatient facilities)

Explicit consent

The person was specifically asked and has given permission to record, store or disclose information. This must be supported by a written signed authorization. You cannot rely on implied consent to process sensitive information.

Care Record

A Service User's Care Record containing notes by all Health and Social Care workers involved in the treatment- can be paper and electronic. This may contain information not always written by BSMHFT staff (e.g., Birmingham Social Care staff and/or Solihull Care Trust staff who support BSMHFT teams).

Personal Information/ Data

Data which relates to a living individual who can be identified from that data or from data and from other information, which is in the possession of, or is likely to come into the possession of the data controller (e.g., our Trust)

Special Categories of data

GDPR also refers to 'special categories of data'. Special consideration and justification need to be given for the collection and disclosure of such data. Sensitive personal data according to the Data Protection Act is:

- Physical or Mental Health or condition
- Racial or ethnic origin
- Political opinions
- Religious beliefs or other beliefs of a similar nature
- Trade Union membership
- Sexual life
- The commission or alleged commission of any offence
- Genetic Data
- Biometric Data were processed to uniquely identify a person
- Any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence any court in such Proceedings.

From the above list it can be seen that most of the information the Trust collects and uses on service users (in clinical notes or electronically) and staff is considered to be '*sensitive personal information*' and subject to the highest level of protection under the Data Protection Act.

Treating Team

Any clinical staff within the Trust involved in the direct care and treatment of the service user.

9. AUDIT AND ASSURANCE

Implementation of this policy will be monitored through regular audits across the Trust; interviewing staff and service users and regularly reviewing confidentiality incidents.

Incidents will be logged and reported to the Information Governance Steering Group (IGSG).

Element to be monitored	Lead	Tool	Frequency	Reporting Committee
IG Training Compliance Monitoring (90% required)	Head of IG	Insight Reports	Bi-monthly	IGSG
Various policy aspects, e.g., physical security	Head of IG/ Head of Care Records	IG Site Audit of all Teams	Annually	IGSG
Requests for access to information	Head of IG/ Head of Care Records	ILR Master Log and reports	Every six months	IGSG
Handling of Confidentiality Breaches/ Incidents	Head of IG	Standing item on agendas/ themed reviews	Every six months and as needed	IGSG

APPENDIX 1

Equality Analysis Screening Form

A word version of this document can be found on the HR support pages on Connect

<http://connect/corporate/humanresources/managementsupport/Pages/default.aspx>

Title of Policy	Confidentiality Policy		
Person Completing this policy	Kirstie Macmillan	Role or title	Head of Information Governance
Division	Resources	Service Area	Information Governance
Date Started	February 2025	Date completed	February 2025
Main purpose and aims of the policy and how it fit in with the wider strategic aims and objectives of the organisation.			
The main purpose is to ensure that data protection legislation is adhered to, and staff understand their responsibilities			
Who will benefit from the proposal?			
Staff Patients			
Does the policy affect service users, employees or the wider community? <i>Add any data you have on the groups affected split by Protected characteristic in the boxes below. Highlight how you have used the data to reduce any noted inequalities going forward</i>			
No			
Does the policy significantly affect service delivery, business processes or policy? <i>How will these reduce inequality?</i>			
No			
Does it involve a significant commitment of resources? <i>How will these reduce inequality?</i>			
No			
Does the policy relate to an area where there are known inequalities? (e.g., seclusion, accessibility, recruitment & progression)			

No				
Impacts on different Personal Protected Characteristics – Helpful Questions:				
<i>Does this policy promote equality of opportunity?</i> <i>Eliminate discrimination?</i> <i>Eliminate harassment?</i> <i>Eliminate victimisation?</i>			<i>Promote good community relations?</i> <i>Promote positive attitudes towards disabled people?</i> <i>Consider more favourable treatment of disabled people?</i> <i>Promote involvement and consultation?</i> <i>Protect and promote human rights?</i>	
Please click in the relevant impact box and include relevant data				
Personal Protected Characteristic	No/Minimum Impact	Negative Impact	Positive Impact	Please list details or evidence of why there might be a positive, negative or no impact on protected characteristics.
Age	x			No negative impact identified
Including children and people over 65 Is it easy for someone of any age to find out about your service or access your policy? Are you able to justify the legal or lawful reasons when your service excludes certain age groups				
Disability	x			No negative impact identified
Including those with physical or sensory impairments, those with learning disabilities and those with mental health issues Do you currently monitor who has a disability so that you know how well your service is being used by people with a disability? Are you making reasonable adjustment to meet the needs of the staff, service users, carers and families?				
Gender	x			No negative impact identified
This can include male and female or someone who has completed the gender reassignment process from one sex to another. Do you have flexible working arrangements for either sex? Is it easier for either men or women to access your policy?				
Marriage or Civil Partnerships	x			No negative impact identified
People who are in a Civil Partnerships must be treated equally to married couples on a wide range of legal matters. Are the documents and information provided for your service reflecting the appropriate terminology for marriage and civil partnerships?				
Pregnancy or Maternity	x			No negative impact identified

<p>This includes women having a baby and women just after they have had a baby.</p> <p>Does your service accommodate the needs of expectant and post-natal mothers both as staff and service users?</p> <p>Can your service treat staff and patients with dignity and respect relation into pregnancy and maternity?</p>			
Race or Ethnicity	x		No negative impact identified
<p>Including Gypsy or Roma people, Irish people, those of mixed heritage, asylum seekers and refugees</p> <p>What training does staff have to respond to the cultural needs of different ethnic groups?</p> <p>What arrangements are in place to communicate with people who do not have English as a first language?</p>			
Religion or Belief	x		No negative impact identified
<p>Including humanists and non-believers</p> <p>Is there easy access to a prayer or quiet room to your service delivery area?</p> <p>When organising events – Do you take necessary steps to make sure that spiritual requirements are met?</p>			
Sexual Orientation	x		No negative impact identified
<p>Including gay men, lesbians and bisexual people</p> <p>Does your service use visual images that could be people from any background or are the images mainly heterosexual couples?</p> <p>Does staff in your workplace feel comfortable about being 'out' or would office culture make them feel this might not be a good idea?</p>			
Transgender or Gender Reassignment	x		No negative impact identified
<p>This will include people who are in the process of or in a care pathway changing from one gender to another.</p> <p>Have you considered the possible needs of transgender staff and service users in the development of your policy or service?</p>			
Human Rights	x		No negative impact identified
<p>Affecting someone's right to Life, Dignity and Respect?</p> <p>Caring for other people or protecting them from danger?</p> <p>The detention of an individual inadvertently or placing someone in a humiliating situation or position?</p>			
<p>If a negative or disproportionate impact has been identified in any of the key areas would this difference be illegal / unlawful? I.e. Would it be discriminatory under anti-discrimination legislation. (The Equality Act 2010, Human Rights Act 1998)</p>			
	Yes	No	

What do you consider the level of negative impact to be?	High Impact	Medium Impact	Low Impact	No Impact
				x
<p>If the impact could be discriminatory in law, please contact the Equality and Diversity Lead immediately to determine the next course of action. If the negative impact is high a Full Equality Analysis will be required.</p> <p>If you are unsure how to answer the above questions, or if you have assessed the impact as medium, please seek further guidance from the Equality and Diversity Lead before proceeding.</p> <p>If the policy does not have a negative impact or the impact is considered low, reasonable or justifiable, then please complete the rest of the form below with any required redial actions, and forward to the Equality and Diversity Lead.</p>				
Action Planning:				
How could you minimise or remove any negative impact identified even if this is of low significance?				
No negative impact identified				
How will any impact or planned actions be monitored and reviewed?				
No negative impact identified				
How will you promote equal opportunity and advance equality by sharing good practice to have a positive impact other people as a result of their personal protected characteristic.				
No negative impact identified				
<p>Please save and keep one copy and then send a copy with a copy of the policy to the Senior Equality and Diversity Lead at bsmhft.edi.queries@nhs.net. The results will then be published on the Trust's website. Please ensure that any resulting actions are incorporated into Divisional or Service planning and monitored on a regular basis</p>				

APPENDIX 2: SUPPORTING INFORMATION

Caldicott Principles for handling personal confidential data:

1. Justify the purpose(s)

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

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).

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.

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. Health care organisations should be aware of the research conducted within the organisation and should ensure research teams are accountable to them (from MRC Executive Summary – Personal Information in Medical Research).

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. Understand and comply with the law

Every use of personal confidential data must be lawful. The Caldicott Guardian, Medical Director, is responsible for ensuring that the organisation complies with legal requirements.

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

Health and social care 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.

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

A range of steps should be taken to ensure no surprises for patients and service users, so they can have clear expectations about how and why their confidential information is used, and what choices they have about this. These steps will vary depending on the use: as a minimum, this should include providing accessible, relevant and appropriate information - in some cases, greater engagement will be required.

Confidentiality Code of Practice: **(And supplementary guidance dated November 2010)**

The 'Confidentiality: NHS Code of Practice' was published by the Department of Health following major consultation in 2002/2003. The consultation included patients, carers and citizens; the NHS; other health care providers; professional bodies and regulators. The Guidance was drafted and delivered by a working group made up of key representatives from these areas.

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 anyone working in and around health services. This includes local authority staff working in integrated teams and private and voluntary sector staff.

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

For the full document, which contains helpful guidance – go to:
<http://www.hscic.gov.uk/confguideorg>

Data Protection Considerations

The General Data Protection Regulation 2016 provides a framework that governs the processing of information that identifies living individuals – personal data in Data Protection terms. Processing includes holding, obtaining, recording, using and disclosing information and the Act applies to all forms of media, including paper and images.

GDPR prohibits processing unless conditions set out in Article 6

Lawfulness of processing conditions

6(1)(a) – Consent of the data subject

6(1)(b) – Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract

6(1)(c) – Processing is necessary for compliance with a legal obligation

6(1)(d) – Processing is necessary to protect the vital interests of a data subject or another person

6(1)(e) – 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

6(1)(f) – Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject

Note that this condition is not available to processing carried out by public authorities in the performance of their tasks.

Conditions for special categories of data

9(2)(a) – Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law

9(2)(b) – Processing is necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement.

9(2)(c) – Processing is necessary to protect the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.

9(2)(d) – Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent.

9(2)(e) – Processing relates to personal data manifestly made public by the data subject

9(2)(f) – Processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.

9(2)(g) – Processing is necessary for reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards.

9(2)(h) – Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional.

9(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 healthcare and of medicinal products or medical devices.

9(2)(j) – Processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1)

It is important to understand the role of consent in relation to these articles.

More information on the regulation's requirements can be found at

[Data Protection Act 2018 | ICO](#)

APPENDIX 3: PUBLIC INTEREST EXEMPLAR CASES

Taken from Department of Health, Confidentiality Code of Practice:
Supplementary Guidance: Public Interest Disclosures

Scenario 1: A receptionist at a GP surgery sees a patient leave the building and get into a car. On driving from the car park, the patient's car collides with and damages another patient's car. The driver does not stop, believing that nobody has seen the incident and instead drives away without leaving their details. Through her role at the surgery, the receptionist knows the identity of the patient. Can the receptionist report the crime? What details can the receptionist provide about the accident and the driver?

Decision 1: A minor crime has been committed, but no serious crime or serious harm done. Therefore, there is insufficient public interest (or any other) justification for revealing confidential patient information (e.g. from within the patient's case notes or even reveal that the patient had attended the surgery). However, a crime has been committed and the receptionist would be entitled to report the incident, including the identity of the patient, to the police, but (s) he should not reveal confidential patient information.

Scenario 2: In one evening, at separate times, two patients enter an Accident & Emergency Department. Each of the patients has been a victim of a knife crime. Both patients report that they have been attacked by an individual and both describe what seems to be the same person. The patients claim that the attacks were unprovoked and that they did not know the attacker. The attacks happen within a mile of each other in a busy city Centre. One of the patients is happy to speak to police and informs A & E staff of this. However, the other victim does not wish to have his information disclosed to the police because he does not want to be a police witness. He leaves before the police are called out. Should the A & E staff report both incidents to the police? Should the identity of the patients and the details of the injuries be reported?

Decision 2: It is generally accepted that the reporting of knife and gun crimes will be within the public interest. A & E units should have standard procedures for informing the police that a knife crime has occurred. It should also be standard practice for staff to seek patient consent to involve the police. A knife attack may be sufficient to justify a public interest disclosure of confidential information even when consent is not given, where it is likely to assist in the prevention, detection or prosecution of a serious crime. Staff should ensure that they consider the proportionality of any disclosures. In this example, police could be called to interview the first patient, who could then be expected to identify himself, and provide a description of the attack and the attacker, and of his injuries. If the patient refused to provide some of these details, the hospital could provide them. For the second patient, it is likely to be proportionate to provide the police with details of the patient, the attacker, the attack and the patient's injuries.

Scenario 3: One day during surgery hours a GP notices Mr. Smith arrive, park his car and enter the surgery building. Mr. Smith had attended an appointment

in the previous month with the GP. At a previous appointment, the GP had prescribed Mr. Smith with drugs and informed him that they were likely to make him drowsy, and that he should avoid driving. During the consultation Mr. Smith had assured the GP that he'd "be fine!" when accepting the prescription. The GP knows Mr. Smith well, and that he might ignore advice not to drive, and so has some concern over whether Mr. Smith was fit to drive. What action should the GP take?

Decision 3: In principle, Mr. Smith could cause serious harm to others by continuing to drive. The GP should speak to Mr. Smith and try to establish whether his medication is having the effect of making him drowsy and unfit to drive, and if so, to encourage him once more to stop driving. Discussion with colleagues may assist the GP in assessing the risk posed to the public from the effect of Mr. Smith's medication, and in weighing up whether a breach of confidence is justified. If Mr. Smith is unfit to drive but nevertheless persists in driving, it would be justifiable in the public interest to inform the Driver and Vehicle Licensing Agency.

Scenario 4: A patient has been arrested on suspicion of robbery and the police have asked a consultant psychiatrist for a 'background' report based on prior knowledge. The police do not explain any more about the nature of the alleged crime but say they will use the report when preparing the papers for the Crown Prosecution Service. The consultant has not been asked to assess the patient and is not convinced that the patient would consent to the disclosure of information. Should the consultant provide the report?

Decision 4: The consultant's decision hinges on whether robbery is a serious crime. Were the police to not provide further details (e.g., as to whether it is robbery with violence), it would be reasonable for the consultant to assume this does not constitute a serious crime. Without a court order, the police cannot force the consultant to provide a report. However, in this case, the police disclose that the robbery was with serious violence and the consultant judges this to be an investigation of a serious crime. The consultant consults the Caldicott Guardian and another colleague. They consider whether the public interest in disclosure outweighs the potential damage from the disclosure. In this case, they feel that the patient's relationship with the psychiatrist (and with any future psychiatric services the patient may receive) would be seriously damaged by a disclosure. Furthermore, the patient receives services through an outreach Centre, and the doctors fear that this may lead to other patients withdrawing from the outreach services. They judge that no report should be provided without the patient's consent.

Scenario 5: Following a series of complaints to a Member of Parliament from local residents, all of whom suffer from a particular disease and live close to a nuclear power station, a project is set up to investigate whether the proximity to the power station could contribute to the onset of the disease. The investigation team from the Public Health Observatory seeks access to confidential information within approximately two thousand paper case notes in Newtown Hospital Trust in order to discover the prevalence of relevant symptoms. The team argues that it is not feasible to seek consent from patients within the

timescales of the enquiry and that their work can be justified in the public interest.

Decision 5: The Newtown Hospital Trust Caldicott Guardian considers that the risk of serious harm is not sufficient to breach the confidence of thousands of patients. However, she feels there is a strong public interest in the investigation. In order to minimize the potential detriment caused, she offers to assist the investigation by providing local clinical coding staff to extract relevant data from the case notes and provide it to the investigation team. Nevertheless, the data to be provided could still reveal patient identity, and so she instructs the investigation team that the information provided must be stored and processed securely, and that no identifiable patient information will be published without explicit patient consent.

APPENDIX 4

Data Protection Impact Assessment Screening Questionnaire

The completed screening questionnaire must be submitted to the Data Protection Officer:
Kirstie.macmillan@nhs.net or bsmhft.informationgovernance@nhs.net

Basic information:

Your name	
Your team and directorate	
Your location	
Your telephone number	
Your email address	
Date Screening Questionnaire Submitted to Data Protection Officer	

Screening questions:

If the answer to any of these questions is 'yes' please complete the full data protection impact assessment available from the Data Protection Officer.

What type of system is the screening tool for:	Software <input type="checkbox"/> Hardware (including office cabinets) <input type="checkbox"/> Information Sharing Protocol <input type="checkbox"/>
Does this system hold any clinical data?	Yes <input type="checkbox"/> No <input type="checkbox"/>
Give a brief description of the system	

Screening Question	Yes / No
Will identifiable personal data of vulnerable natural persons, in particular of children, be processed? This includes patients, service users or staff. You must enter yes if any data points identifying an individual are used (eg names).	Yes <input type="checkbox"/> No <input type="checkbox"/>
Will the processing involve a large amount of personal data and affect a large number of data subjects?	Yes <input type="checkbox"/> No <input type="checkbox"/>
Will the project involve the use of a novel technology(ies)? A novel technology is one that is experimental or is not well established.	Yes <input type="checkbox"/> No <input type="checkbox"/>

Is there the risk that the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy (e.g. health records), unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage?	Yes <input type="checkbox"/> No <input type="checkbox"/>
Is there the risk that data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data?	Yes <input type="checkbox"/> No <input type="checkbox"/>
Will there be processing of genetic data, data concerning health or data concerning sex life?	Yes <input type="checkbox"/> No <input type="checkbox"/>
Are the data to be processed revealing racial or ethnic origin, political opinions, religion or philosophical beliefs, or trade union membership?	Yes <input type="checkbox"/> No <input type="checkbox"/>
Will there be processing of data concerning criminal convictions and offences or related security measures?	Yes <input type="checkbox"/> No <input type="checkbox"/>
Will personal aspects be evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles?	Yes <input type="checkbox"/> No <input type="checkbox"/>
Will the project include a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person (e.g. a recruitment aptitude test which uses pre-programmed algorithms and criteria)?	Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>
Will there be a systematic monitoring of a publicly accessible area on a large scale (e.g. CCTV)?	Yes <input type="checkbox"/> No <input type="checkbox"/>
<p>Motivated Intruder Test:</p> <p>If you are using anonymised data and there were to be a breach of that anonymised data – would it be possible for someone to work out the identity of any individual the data belongs to? This could be by using the data directly, using it with other data that is publicly available or by using investigative techniques. You should assume that you are not looking just at the means reasonably likely to be used by an ordinary person, but also by a determined person with a particular reason to want to identify individuals. For example, intruders could be investigative journalists, estranged partners, stalkers, or industrial spies</p>	Yes <input type="checkbox"/> No <input type="checkbox"/>

Health and care: Template data protection impact assessment (DPIA)

Background

A [data protection impact assessment \(DPIA\)](#) will help you to identify and mitigate potential data protection risks to an acceptable level before using or sharing (processing) data that identifies individuals (personal data).

A DPIA will also help you meet a number of data protection legal requirements including:

- [Data protection by design](#) - privacy and data protection issues must be considered at the start, or in the design phase, of a new system, product or process, then continuously while it exists.
- [Accountability](#) - your organisation is responsible for showing how it complies with data protection laws.
- [Transparency](#) - personal data must be used and shared in a transparent way.
- [Security](#) - adequate measures need to be in place to protect data. This can range from policies and procedures to technical security measures such as encryption of data.

DPIAs are mandatory when there is a high risk to individuals, such as when using the health and care data of a large number of people. However, health and care organisations are strongly advised to complete a DPIA when using and sharing personal data in a new or substantially changed way.

A DPIA involves a risk assessment. If a high-level risk remains after applying mitigations, then you must consult with the Information Commissioner's Office (ICO) for further advice before starting to collect, use or share the data.

A DPIA is a live document - you must update it if there are any changes to:

- the purpose - why you are proposing to use or share personal data
- the manner - how you will use or share the data
- who is involved - the organisations using and sharing personal data

This is a template DPIA for health and care organisations. We encourage organisations to adopt it. The template is written so that it is easy to use without needing expertise in data protection. It is the responsibility of the organisation which is deciding on why and how the data is being used and shared (known as the controller), to ensure that the DPIA is completed appropriately.

In the case of research, the sponsor is the controller. See Health Research Authority (HRA) guidance on [controllers](#) and research. HRA guidance on [DPIAs](#) sets out that sponsors should complete a DPIA for the broad range of health and care research they sponsor and ensure that individual research projects are designed in accordance with the DPIA. Individual DPIAs should only need to be completed for individual research projects that involve activities beyond the generic research DPIA. Where the study deviates from the established processes (for example, where it is intended that a project uses a new technology for the processing of personal data, or requires that safeguards set out in standing policies cannot be applied), the

sponsor should consider whether a study specific DPIA is appropriate to address the level of risk, or whether updating existing DPIA(s) will be sufficient. Research sites should not complete DPIAs or request researchers to complete individual DPIAs for each research project, as they are not the controller.

Text in [square brackets and green highlight] is guidance only and should be removed for the final version.

Text in yellow highlight is sample wording and should be edited according to your local circumstances.

Table of contents

Data protection impact assessment (DPIA)	48
SECTION 1 – Screening questions	49
SECTION 2 – Why do you need the data?	49
SECTION 3 – What data do you want to use or share?	50
SECTION 4 – Where will data flow?.....	54
SECTION 5 – Is the intended use of the data lawful?	55
SECTION 6 – How are you keeping the data secure?	58
SECTION 7 – How long are you keeping the data and what will happen to it after that time? ..	61
SECTION 8 – How are people’s rights and choices being met?	62
SECTION 9 – Which organisations are involved?	65
SECTION 10 – What data protections are there and what mitigations will you put in place? ..	67
SECTION 11 – Review and sign-off	69

Data protection impact assessment (DPIA)

Data protection impact assessment (DPIA) title:	
[Please provide any other reference numbers as needed]	

Background Information			
Lead Organisation:		Project/Activity/ Asset Leads Contact Details:	
Name of individual submitting this PIA/Key contact:			

If Information is to be shared with any external organisation has an Information Sharing Protocol (ISP) been completed? This will also be needed if a software supplier will have access to Trust data for maintenance or repair reasons.	
Has this system/ software been approved by (or is it planned to go to) the System Strategy Group and/or ICT CAB?	Yes/No N/A
If applicable, has the Clinical Safety Officer approved the implementation of the software?	Yes/No N/A
Is the organisation you will share information with or purchase software from registered with the Information Commissioners Office? What is the ICO Registration Number and date of expiry?	Yes/ No

Does this organisation have in date, Information Governance, and Information Security Policies / Procedures?	Yes/ No
--	---------

SECTION 1 – Screening questions

1. Do you need to do a DPIA?

Background

Add background.

a. Summary of how data will be used and shared

[For example, data is collected from our services, and aggregated. We will then share the aggregated data with Company A to gain improved insights to enable us to improve service provision.]

b. Description of the data

[Put an ☒ next to all that apply.]

<input type="checkbox"/>	Personal data [individuals can be identified]
<input type="checkbox"/>	Pseudonymised data [identifiers, for example name or NHS number, are replaced with a unique number or code (a pseudonym)]
<input type="checkbox"/>	Anonymous data [not identifiable, for example trends or statistics]

[Provide details of any pseudonymised data, including which organisation holds the key that allows the data to be re-identified. Describe the way the data has been anonymised and whether it is anonymised in the hands of those you will be sending it to. This should include detail of whether the data has been aggregated with small numbers suppressed. For example, if only two people in the area have a rare condition it could be possible to identify them so this data would need to be removed.]

Where a DPIA is not required but you are documenting your decision and the risks, [skip to section 10](#) and [11](#) – the other sections do not need completing.]

SECTION 2 – Why do you need the data?

2. What are the purposes for using or sharing the data?

[Give a high-level description of the purpose(s) for example, the purpose is to look at overall health of the people in our area to ensure we have the right services in the right places.]

Multiple related purposes are acceptable for one DPIA, but where these are unrelated, a separate DPIA should be completed for each one.]

3. What are the benefits of using or sharing the data?

[Set out the benefits of using and sharing the data. This should cover the benefits to the individuals whose data is being used, the benefits to the organisation(s), the wider public, or other groups if applicable.]

For example, installing a new telephony system will help deliver a better service to patients because they will be able to get through to the organisation faster and the organisation will also have an audit trail to ensure better management.]

SECTION 3 – What data do you want to use or share?

4. Can you use anonymous data for your purposes? If not, explain why.

[Put an ☒ next to the one that applies.]

<input type="checkbox"/>	Yes
<input type="checkbox"/>	No
<input type="checkbox"/>	Unsure [try to provide an explanation of what you think]

[Anonymous data does not identify individuals, for example trends or statistics. You should use anonymous data whenever possible. This may not always be possible, for example if your intended use of data is to provide individual care.]

For example, we intend to use analytical tools to identify which individuals in our local population are at high risk of diabetes so that their GP can offer them early intervention treatments.]

5. Which types of personal data do you need to use and why?

[Put an ☒ next to all that apply.]

<input type="checkbox"/>	Forename	<input type="checkbox"/>	Physical description, for example height	<input type="checkbox"/>	Photograph / picture of people
<input type="checkbox"/>	Surname	<input type="checkbox"/>	Phone number	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	Location data e.g. <ul style="list-style-type: none">• IP address• Other [please state]
<input type="checkbox"/>	Address	<input type="checkbox"/>	Email address	<input type="checkbox"/>	Audio recordings

<input type="checkbox"/>	Postcode full	<input type="checkbox"/>	GP details	<input type="checkbox"/>	Video recordings
<input type="checkbox"/>	Postcode partial	<input type="checkbox"/>	Legal representative name (personal representative)	<input type="checkbox"/>	Other [please state]
<input type="checkbox"/>	Date of birth	<input type="checkbox"/>	NHS number	<input type="checkbox"/>	None
<input type="checkbox"/>	Age	<input type="checkbox"/>	National insurance number		
<input type="checkbox"/>	Gender	<input type="checkbox"/>	Other numerical identifier [please state]		

[State why you need this personal data and embed a description of the dataset if available.]

6. Data protection laws mean that some data is considered particularly sensitive. This is called special category data. Data that relates to criminal offences is also considered particularly sensitive. Which types of sensitive data do you need to use or share?

[Put an ☒ next to all that apply.]

Type of data		Reason why this is needed (leave blank if not applicable)
<input type="checkbox"/>	Information relating to an individual's physical or mental health or condition, for example information from health and care records	[be specific where possible, for example diagnostic data, care plans, medication details, test results, vitals readings are needed in order to...]
<input type="checkbox"/>	Biometric information in order to uniquely identify an individual, for example facial recognition	

	Genetic data, for example details about a DNA sample taken as part of a genetic clinical service	
	Information relating to an individual's sexual life or sexual orientation	
	Racial or ethnic origin	
	Political opinions	
	Religious or philosophical beliefs	
	Trade union membership	
	Information relating to criminal or suspected criminal offences	
	None of the above	

[Embed a description of the dataset if available, unless special category data is covered in your embedded description in response to [question 5](#)]

7. Who are the individuals that can be identified from the data?

[Put an ☒ next to all that apply.]

<input type="checkbox"/>	Patients or service users
<input type="checkbox"/>	Carers
<input type="checkbox"/>	Staff
<input type="checkbox"/>	Wider workforce

<input type="checkbox"/>	Visitors
<input type="checkbox"/>	Members of the public
<input type="checkbox"/>	Other [please state]

8. Where will your data come from?

[This may be directly from the individuals or from a third party, such as another health and care organisation. Note this should be a brief summary - full details of the data flows are covered in [section 4.](#)]

9. Will you be linking any data together?

[Put an ☒ next to the one that applies.]

<input type="checkbox"/>	Yes [provide an explanation below and then go to question 9a]
<input type="checkbox"/>	No [skip to question 10]
<input type="checkbox"/>	Unsure [try to provide an explanation of what you think then go to question 9a]

[For example, combining data received from a local authority with data from NHS organisations. If so, provide details of why this is necessary, for example local authority data needs to be linked with data from local NHS organisations so that we can understand admissions to care homes from different organisations.]

a. Will it become possible, as a result of linking data, to be able to identify individuals who were not already identifiable from the original dataset?

[Put an ☒ next to the one that applies.]


<input type="checkbox"/>	Yes [provide details below]
<input type="checkbox"/>	No
<input type="checkbox"/>	Unsure [try to provide details below]

[Standalone datasets may not be identifiable when all identifiers, such as NHS number, are replaced with a code. However, if you link the dataset with other data, it could become identifiable data. For example, if once linked, you could look up which code is associated with which NHS number. You will need to factor this in when you complete [section 5.](#)]

SECTION 4 – Where will data flow?

10. Describe the flows of data.

[You can use this table - some examples have been provided. Alternatively, you can use a data flow map or a written description of the data flow. A simple example of a map could be: patient - inputs blood pressure reading into app X - reading uploaded into patient's hospital record.]

Data flow name	Going from	Going to	Data description
Admission data	Hospital	Local authority	Demographic data of patients admitted to hospital from local authority commissioned care homes
Diabetic data	Ambulance Trust	Hospital	Demographic data of patients with diabetes requiring an ambulance
Please complete the attached Data Flow Sheet  Data Flow Sheet.xlsx			

11. Confirm that your organisation's information asset register (IAR), record of processing activities (ROPA) or your combined information assets and flows register (IAFR) has been updated with the flows described above.

[Put an ☒ next to the one that applies.]

<input type="checkbox"/>	Yes
<input type="checkbox"/>	No

<input type="checkbox"/>	Unsure [add as a risk in section 10 with an action to find out]
--------------------------	---

[Your organisation is required to keep a record of the types of data processing it undertakes and any information assets it holds. The template [Information Asset and Flows Register \(IAFR\)](#) allows you to record both of these in one register. Alternatively, you can record them separately, with types of data processing recorded in a ROPA and information assets recorded in an IAR.]

12. Will any data be shared outside of the UK?

[Put an ☒ next to the one that applies.]

<input type="checkbox"/>	Yes [go to question 12a]
<input type="checkbox"/>	No [skip to question 13]
<input type="checkbox"/>	Unsure [add as a risk in section 10 with an action to find out then skip to question 13]

- a. If yes, give details, including any safeguards or measures put in place to protect the data whilst outside of the UK.

[An example of a safeguard is an up to date international data transfer agreement ([IDTA](#)). This should be included in your contract with the overseas organisation. For countries without [UK adequacy in place](#), further checks on the organisation must be made before providing them access to data to ensure the data will be handled appropriately.]

SECTION 5 – Is the intended use of the data lawful?

[You should consider seeking advice to help you complete this section if you are not an IG professional.]

13. Under Article 6 of the UK General Data Protection Regulation (UK GDPR) what is your lawful basis for processing personal data?

[The list below contains the most likely conditions applicable to health and care services. Put an ☒ next to the one that applies. If a different lawful basis applies for a different party, clearly indicate which lawful basis applies to which party by adding in brackets after the selected lawful basis which party it applies to e.g.]

☒ e) **We need it to perform a public task** (GP practice)]

<input type="checkbox"/>	(a) We have consent [this must be freely given, specific, informed and unambiguous. It is not appropriate to rely on consent for individual care or research, even if you have obtained consent for other reasons, but is likely to be needed for the use of cookies on a website]
<input type="checkbox"/>	(b) We have a contractual obligation [between a person and a service, such as a service user and privately funded care home]

<input type="checkbox"/>	(c) We have a legal obligation [the law requires us to do this, for example where NHS England or the courts use their powers to require the data. See this list for the most likely laws that apply when using and sharing information in health and care.]
<input type="checkbox"/>	(e) We need it to perform a public task [a public body, such as an NHS organisation or Care Quality Commission (CQC) registered social care organisation, is required to undertake particular activities. See this list for the most likely laws that apply when using and sharing information in health and care. This is mostly likely to be relevant for the provision of NHS and social care services regulated by the CQC. See HRA guidance on legal basis for processing data for research]
<input type="checkbox"/>	(f) We have a legitimate interest [for example, a private care provider making attempts to resolve an outstanding debt for one of its service users. This cannot be relied on by public bodies in the performance of their tasks.]
<input type="checkbox"/>	Other [please state]

14. If you have indicated in question 6 that you are using special category data, what is your lawful basis under Article 9 of the UK GDPR?

[The list below contains the most likely conditions applicable to health and care services. Put an ☒ next to the one that applies.]

<input type="checkbox"/>	(b) We need it to comply with our legal obligations for employment [for example, to check a person's eligibility to work in the NHS or a local authority. See this list for the most likely laws that apply when using and sharing information in health and care.]
<input type="checkbox"/>	(f) We need it for legal claims, to seek legal advice or judicial acts [the information is required to exercise, enforce or defend a legal right or claim, for example a person bringing litigation against a health or care organisation.]
<input type="checkbox"/>	(g) We need to comply with our legal obligations to provide information where there is a substantial public interest, as set out in this list [for example, safeguarding of children and individuals at risk.]
<input type="checkbox"/>	(h) We need it to comply with our legal obligations to provide or manage health or social care services [providing health and care to a person, or ensuring health and care systems function to enable care to be provided. See this list for the most likely laws that apply when using and sharing information in health and care.]
<input type="checkbox"/>	(i) We need it to comply with our legal obligations for public health [using and sharing information is necessary to deal with

	threats to public health, or to take action in response to a public health emergency (such as a vaccination programme). See this list for the most likely laws that apply when using and sharing information in health and care.]
<input type="checkbox"/>	(j) We need it for archiving, research and statistics where this is in the public interest [for example, health and care research, with relevant safeguards in place for the use of the participant's health and care information. See this list for the most likely laws that apply when using and sharing information in health and care. See HRA guidance on legal basis for processing data for research. Processing must be in the public interest to rely on this lawful basis.]
<input type="checkbox"/>	Other [please state]
<input type="checkbox"/>	Not applicable [the use of special category data is not proposed]

15. What is your legal basis for using and sharing this health and care data under the common law duty of confidentiality?

[The common law duty of confidentiality says that health and care information about a person cannot be disclosed without that person's consent. Implied consent can be used when sharing relevant information with those who are directly involved in providing care to an individual. Explicit consent is normally required for purposes beyond individual care unless one of the other conditions set out below applies, for example you have section 251 support.]

[Put an ☒ next to the one that applies.]

<input type="checkbox"/>	Implied consent [for individual care or local clinical or care audits. Skip to question 16]
<input type="checkbox"/>	Explicit consent [a very clear and specific statement of consent. Go to question 15a]
<input type="checkbox"/>	Section 251 support [this means you have support from the Secretary of State for Health and Care or the HRA following an application to the Confidentiality Advisory Group (CAG). CAG must be satisfied that it isn't possible or practical to seek consent. Go to question 15a]
<input type="checkbox"/>	Legal requirement [this includes where NHS England has directed an organisation to share the data using its legal powers. State the legal requirement in the further information section. Go to question 15a]
<input type="checkbox"/>	Overriding public interest [for example to prevent or detect a serious crime or to prevent serious harm to another person. The justification to disclose must be balanced against the public interest in maintaining public confidence in health and care services. Routine use of this is extremely rare in health and care, as it usually applies to individual cases where decisions are made to share data. Go to question 15a]
<input type="checkbox"/>	Not applicable [you are not proposing to use identifiable health and care data. Skip to question 16]

a. Please provide further information or evidence.

[Provide evidence as follows depending on your selection in [question 15](#)]

- A record of the explicit consent is stored in
- The CAG reference number is...
[for research the DPIA should cover multiple projects, so signpost to the sponsor's list of research projects with relevant CAG reference numbers]
- The legal requirement is...
[for example directed by NHS England under the Health and Social Care Act 2012]
- The overriding public interest justification we are relying upon is...

SECTION 6 – How are you keeping the data secure?

16. Are you collecting information?

[Put an ☒ next to the one that applies.]

<input type="checkbox"/>	Yes [go to question 16a]
<input type="checkbox"/>	No [skip to question 17]

a. How is the data being collected?

[You should describe the method for the collection, for example it is collected by a team going through records and extracting relevant information.]

17. Are you storing information?


[Put an ☒ next to the one that applies.]

<input type="checkbox"/>	Yes [go to question 17a]
<input type="checkbox"/>	No [skip to question 18]

a. How will information be stored?

[Put an ☒ next to all that apply.]

Storage location		Details (leave blank if not applicable)
<input type="checkbox"/>	Physical storage, for example filing cabinets, archive rooms etc	[provide details including whether the facility is operated by your organisation or a third party]

<input type="checkbox"/>	Local organisation servers	[provide details]
<input type="checkbox"/>	Cloud storage  health_and_social_care_data_risk_model	If you are using a public cloud, please complete the embedded Cloud Risk Assessment spreadsheet and go to Q17.b
<input type="checkbox"/>	Other	[please state]

b. If you are completing the risk assessment spreadsheet, please consider the following:

Understand the data you are dealing with

Assess the risks associated with the data

Implement appropriate controls

Monitor the implementation and ongoing risks

If you completed the risk assessment, enter the Class you Scored:

If you scored Class 3 or 4, answer the following questions:

- **How does the cloud provider meet the required security standard?** (eg, Cyber Essentials Plus, ISO27001, Digital Marketplace, Encryption)
- **What security controls are your responsibility?**
- **What security controls are the cloud providers responsibility?**
- **How will you monitor, review and implement any changes to cloud security for yourself and the cloud provider?**

18. Are you transferring information?

[Put an ☒ next to the one that applies.]

<input type="checkbox"/>	Yes [go to question 18a]
<input type="checkbox"/>	No [skip to question 19]

a. How will information be transferred?

[For example, will the information be physically moved as required, sent electronically by email, or uploaded into a shared system. Provide details of security measures to ensure the transfer is secure, for example using secure email (such as NHSmail).]

19. How will you ensure that information is safe and secure?

[You need to have measures in place to ensure that the data is safe and it won't be used, either on purpose or accidentally, in ways that are unlawful. The measures needed will be dependent upon, and proportionate to, the data which is being used.]

[Put an ☒ next to all that apply.]

Security measure		Details (leave blank if not applicable)
<input type="checkbox"/>	Encryption	[specify the level of encryption, such as AES 256]
<input type="checkbox"/>	Password protection	
<input type="checkbox"/>	Role based access controls (RBAC)	[where users only have access to the data held digitally which is needed for their role (this includes setting folder permissions)]
<input type="checkbox"/>	Restricted physical access	[where access to personal data is restricted to a small number of people, such as access cards or keys to a restricted area]
<input type="checkbox"/>	Business continuity plans	
<input type="checkbox"/>	Security policies	[embed these]
<input type="checkbox"/>	Other	[please state]

20. How will you ensure the information will not be used for any other purposes beyond those set out in [question 2](#)?

Specify the measures below which will be used to limit the purposes the data is used for.

[Put an ☒ next to all that apply and provide details.]

Security measure		Details (leave blank if not applicable)
<input type="checkbox"/>	Contract	[a legally binding contract]
<input type="checkbox"/>	Data processing agreement	[this sets out the arrangements between a controller and processor and is legally binding]
<input type="checkbox"/>	Data sharing agreement	[this sets out the arrangements for sharing data between the organisations involved – it may or may not be legally binding depending on the content]
<input type="checkbox"/>	Data sharing and processing agreement (DSPA)	[where appropriately completed, this is a legally binding agreement that sets out the arrangements for processing and/or sharing data, and/or joint controller arrangements]

<input type="checkbox"/>	Audit	[provide details, for example there will be an audit trail of those who access health and care records, which is reviewed monthly]
<input type="checkbox"/>	Staff training	
<input type="checkbox"/>	Other	[please state]

SECTION 7 – How long are you keeping the data and what will happen to it after that time?

21. How long are you planning to use the data for?

We intend to start using the data on [add date] and will finish using the data on [add the contract/project/programme end date or indicate if it is ongoing.]

22. How long do you intend to keep the data?

[The time you keep the data for may differ from the period of time you intend to use the data, for example adult health records need to be kept for a minimum of 8 years from the time they were last used. The [Records Management Code of Practice](#) sets out the retention period for health and care records. Appendix 2 of the Code also includes guidance about setting a retention period for a record not covered in the retention table of the Code.]

23. What will happen to the data at the end of this period?

[Put an ☒ next to all that apply.]

Action		Details (leave blank if not applicable)
<input type="checkbox"/>	Secure destruction (for example by shredding paper records or wiping hard drives with evidence of a certificate of destruction)	[provide details of who will do this]
<input type="checkbox"/>	Permanent preservation by transferring the data to a Place of Deposit run by the National Archives	[provide details of who will do this]
<input type="checkbox"/>	Transfer to another organisation	[provide details]
<input type="checkbox"/>	Extension to retention period	[with approved justification]
<input type="checkbox"/>	It will be anonymised and kept	[provide details of how this will be done and by who]
<input type="checkbox"/>	The controller(s) will manage as it is held by them	

<input type="checkbox"/>	Other	[please state. For research, explain the exemptions applicable to research. Explain the safeguards as set out in HRA guidance on safeguards]
--------------------------	-------	---

[The [Records Management Code of Practice](#) provides detail about what happens once a retention period has been reached.]

SECTION 8 – How are people’s rights and choices being met?

24. How will you comply with the following individual rights (where they apply)?

[For joint controllers, indicate anything you have agreed, such as designating one controller as a point of contact for patients and service users (data subjects).]

These rights will not always apply so you should review each one to see if it applies. In particular, some rights do not apply when data is being used for research purposes. The HRA has published guidance on [research exemptions](#).]

Individual right	How you will comply (or state <i>not applicable</i> if the right does not apply)
The right to be informed The right to be informed about the collection and use of personal data.	We have assessed how we should inform individuals about the use of data for [state initiative/project/programme] . We consider the communications methods below meet this obligation because [add reasons to justify your decision] [Put an <input checked="" type="checkbox"/> next to all that apply.]
	Privacy notice(s) for all relevant organisations [provide a link or describe where it will be displayed and embed a copy]
	Information leaflets
	Posters
	Letters
	Emails
	Texts

		Social media campaign
		DPIA published (best practice rather than requirement)
		Other [please state]
		Not applicable
The right of access The right to access details of data use and receive a copy of their personal information - this is commonly referred to as a subject access request.		
The right to rectification The right to have inaccurate personal data rectified or completed if it is incomplete.		
The right to erasure The right to have personal data erased, if applicable. [This will not apply if you have selected legal obligation, public task or legal claims in question 13, or if you have selected health and care services, public health or archiving, research or statistical purposes in question 14.]		
The right to restrict processing The right to limit how their data is used, if applicable. [For example, that it can be held by the organisation, but restrictions placed on how it is used. This is unlikely to apply to health and care organisations.]		

<p>The right to data portability The right to obtain and re-use their personal data, if applicable.</p> <p>[This only applies where you are processing under UK GDPR consent, or for the performance of a contract; and you are carrying out the processing by automated means, therefore excluding paper files.]</p>	
<p>The right to object The right to object to the use and sharing of personal data, if applicable.</p> <p>[This applies where you are carrying out a task in the public interest or for your legitimate interests, but there are exceptions. It is unlikely that an objection would be upheld where the data is processed for individual care, but each request must be considered on a case-by-case basis. However, it is important to note that there are other routes in which an individual can raise an objection to processing.]</p>	

25. Will the national data opt-out need to be applied?

[Put an ☒ next to the one that applies.]

<input type="checkbox"/>	Yes [provide details of how this is applied]
<input type="checkbox"/>	No [provide details of why this is not applicable]
<input type="checkbox"/>	Unsure [add as a risk in section 10 with an action to find out]

[The [national data opt-out](#) applies to the use of confidential patient information for purposes beyond individual care, for planning and research. It will only apply if your answer to [question 15](#) is section 251 support, although there are some [exceptions](#) in which it would not apply to programmes with section 251 support.]

26. Will any decisions be made in a purely automated way without any human involvement (automated decision making)?

[Put an ☒ next to the one that applies.]

<input type="checkbox"/>	Yes [go to question 26a]
<input type="checkbox"/>	No [skip to question 27]
<input type="checkbox"/>	Unsure [add as a risk in section 10 with an action to find out]

[An example of where automated decision making may be used is staff rostering.]

- a. Where the effect of the automated decision on the individual is substantial, how will you uphold an individual's right not to be subjected to a decision solely made by automated means)?

[For example, you provide people with an option to ask for a human review of the decision. If the effect on people is not legally significant, for example it will only have a minor impact upon them, state this here to confirm this right is not applicable.]

- b. Are you using any special category data as part of automated decision making?

<input type="checkbox"/>	Yes [we are not currently aware of any examples in health and care. If this is the case contact england.igpolicyteam@nhs.net for advice.]
<input type="checkbox"/>	No

27. Detail any stakeholder consultation that has taken place (if applicable).

[For example, if your processing will have a significant impact on partner organisations or the public, you may have approached them for their views and incorporated them into the design of your data use. Include any consultation with the Information Commissioner's Office (ICO) if applicable. For research, you should include information about the sponsors policies and procedures for [public involvement in research](#), and additional specific involvement relating to use of confidential patient information without consent under section 251 support.]

SECTION 9 – Which organisations are involved?

28. List the organisation(s) that will decide why and how the data is being used and shared (controllers).

[The organisation(s) listed here will be making the decisions for example:

- to collect the data in the first place
- what data is being collected

- what it is being used for
- who it is being collected from

The organisation(s) will also be likely to have a direct relationship with those the data is being collected from, for example patients, service users or employees.

There may be more than one organisation listed here. They may be controllers for their own data, for example care homes would usually only be controller for their own residents' information even if they were all using the same software supplier to manage their care records. In some instances, organisations may be joint controllers. For example, this may apply where organisations are using the data for the same purpose, where you share a dataset with another organisation, or where you have designed a new collection with another organisation. An example of where there may be joint controllers in some instances is shared care records, where multiple health and care organisations are contributing data for the same purpose.

In the case of research, the sponsor is the controller. See HRA guidance on [controllers](#) and [research](#)

29. List the organisation(s) that are being instructed to use or share the data (processors).

[The organisation(s) listed here will be under instruction from those listed in [question 28](#), for example they are likely to be told:

- what data to collect
- who to collect data from
- how the collection is legal
- the purpose for the collection
- who to share the data with
- how long to keep the data

Where processors are not being used, state not applicable.

For research, explain the sponsor's policies and procedures for managing the use of data by research sites]

30. List any organisations that have been subcontracted by your processor to handle data

[Your processor listed in [question 29](#) can only sub-contract an activity to another organisation with your authorisation. The organisation which has been sub-contracted is known as a sub-processor.

Where sub-processors are not being used, state not applicable.]

31. Explain the relationship between the organisations set out in [questions 28](#), [29](#) and [30](#) and what activities they do

[Describe here how it has been agreed that the organisations (controllers, processors and sub-processors) will work together. For example:

- Controller A has instructed Processor B to provide an IT system. Processor B sub-contracts the IT service desk function to sub-processor C; or
- Controllers A, B and C are controllers of their own data, which is shared between them. They all use processor D's app

Where no other organisations are used, state not applicable.]

32. What due diligence measures and checks have been carried out on any processors used?

[Put an ☒ next to all that apply. Where multiple processors are used, indicate which option applies to which processor]

Due diligence measures		Details (leave blank if not applicable)
<input type="checkbox"/>	Data Security and Protection Toolkit (DSPT) compliance	[applicable to all organisations that have access to NHS data and systems. Use the organisation search to check the latest DSPT score for any organisation required to complete DSPT]
<input type="checkbox"/>	Registered with the Information Commissioner's Office (ICO)	[any organisation using and sharing data should be registered - add the registration number]
<input type="checkbox"/>	Digital Technology Assessment Criteria (DTAC) assessment	[you should ask the processor for this - see question 29]
<input type="checkbox"/>	Stated accreditations	[for example, ISO accreditation]
<input type="checkbox"/>	Cyber Essentials or any other cyber security certification	[you can check the National Cyber Security Centre's list of organisations that have this]
<input type="checkbox"/>	Other checks	[please state]

SECTION 10 – What data protections are there and what mitigations will you put in place?

33. Complete the [risk assessment table](#). Use the [risk scoring table](#) to decide on the risk score.

[Some examples have been added below. These should be amended and added according to your local set up.

This should include:

- Confidentiality risks - for example unauthorised or accidental disclosure of or access to personal data.
- Integrity risks - for example unauthorised or accidental alteration of personal data. Consider also how you will ensure data is accurate and up to date.
- Availability risks - for example unauthorised or accidental loss of access to, or destruction of personal data.

You must consider risks at each stage, for example when data is being transferred, when it is stored and when it is no longer needed.

Consider whether there are any responses to questions in this DPIA that are either inconclusive or insufficient.]

Risk assessment table

Risk ref no.	Description	Risk score* (L x I)	Mitigations	Risk score* with mitigations applied
01	Power outage affecting Trust servers leading to loss of availability of data	10	Backup generators kick in if main system fails	2
02	Information is stored in unrestricted network areas leading to inappropriate access to data	8	Ensure project team have dedicated network space with access restricted to team members	2
03	Data is not up to date	12	Controller A will send out daily notifications of updates	4
04				
05				

***Risk scoring table**

		Impact (I)				
		Negligible (1)	Low (2)	Moderate (3)	Significant (4)	Catastrophic (5)
Likelihood (L)	Rare (1)	1	2	3	4	5
	Unlikely (2)	2	4	6	8	10

	Possible (3)	3	6	9	12	15
	Likely (4)	4	8	12	16	20
	Almost certain (5)	5	10	15	20	25

34. Detail any actions needed to mitigate any risks, who has approved the action, who owns the action, when it is due and whether it is complete.

Risk ref no.	Action needed	Action approver	Action owner	Due date	Status e.g. outstanding /complete

SECTION 11 – Review and sign-off

[Ensure the relevant staff review or sign off the DPIA according to your governance structure. For example, this may be a more senior member of staff for higher risk processing. Add additional entries for multiple reviewers / approvers.]

Reviewer sign-off	
Reviewer name:	
Reviewer job title:	[For example, Senior Information Risk Owner, Caldicott Guardian, Information Governance Lead, Information Asset Owner, IT lead, Data Protection Officer]
Reviewer contact details:	
Date of review:	
Comments:	
Date for next review:	

Approver sign-off	
Approver name:	
Approver job title:	
Approver contact details:	
Date of approval:	
Comments:	

APPENDIX 6 – ROOT CAUSE ANALYSIS TOOLS

Five Why's

What is it?

By repeatedly asking the question 'why?' (use five as a rule of thumb), you can peel away the layers of a problem to get to the root cause. Five whys can help you determine the relationship between different root causes of a problem. It is a simple tool and can be completed without statistical analysis.

When to use it

You can use this tool either in isolation or to complement a root cause analysis. Because it quickly helps identify the source of an issue or problem, you can focus resources in the correct areas and ensure you are tackling the true cause of the problem, not just its symptoms. How to use it 1. Write down the specific problem. This helps you formalise the problem and describe it accurately. It also helps a team focus on the same problem.

You can use brainstorming to ask why the problem occurs then, write the answer down. If this answer doesn't identify the source of the problem, ask 'why?' again and write that answer down. Loop back until the team agrees that they have identified the problem's root cause. This may take fewer or more than five 'whys?'

The cause-and-effect diagram (fish bone) helps you explore all potential or real causes that result in a failure or problem. Once you have established all the inputs on the cause-and-effect diagram, you can use the five whys technique to drill down to the root causes. The key is to avoid assumptions and encourage the team to keep drilling down to the real root cause. If you try to fix the problem too quickly, you may be dealing with the symptoms not the problem, so use five whys to ensure that you are addressing the cause of the problem.

Remember, if you don't ask the right questions, you won't get the right answers.

Example

An example of root cause analysis using five whys would be: The patient was late in theatre; it caused a delay.

Why? There was a long wait for a trolley.

Why? A replacement trolley had to be found. Why? The original trolley's safety rail was worn and had eventually broken. Why? It had not been regularly checked for wear.

Why? The root cause is that there is no equipment maintenance schedule. Setting up a proper maintenance schedule helps ensure that patients are not late due to faulty equipment.

Another example of root cause analysis using five whys would be: The patient's diagnosis of skin cancer was considerably delayed.

Why? The excision biopsy report was not seen by the surgeon.

Why? The report was filed in the patient's notes without being seen by the surgeon.

Why? It was the receptionist's job to do the filing.

Why? The junior doctors were busy with other tasks.

Why? The root cause is that the doctor's other tasks were seen as more important than filing. The system has now been changed. A copy of all biopsy reports are sent to the consultant surgeon responsible for the patient and no reports are filed unless they have been signed by a doctor. Once you have identified the root cause of the issue, the next suggested step is to complete the cause-and-effect diagram to help identify potential solutions. You will need to communicate the outcomes to others to ensure that the root cause of the problem is understood and that everyone is focused on working on the correct problem area, not treating its symptoms.

Cause and Effect Diagram

What is it?

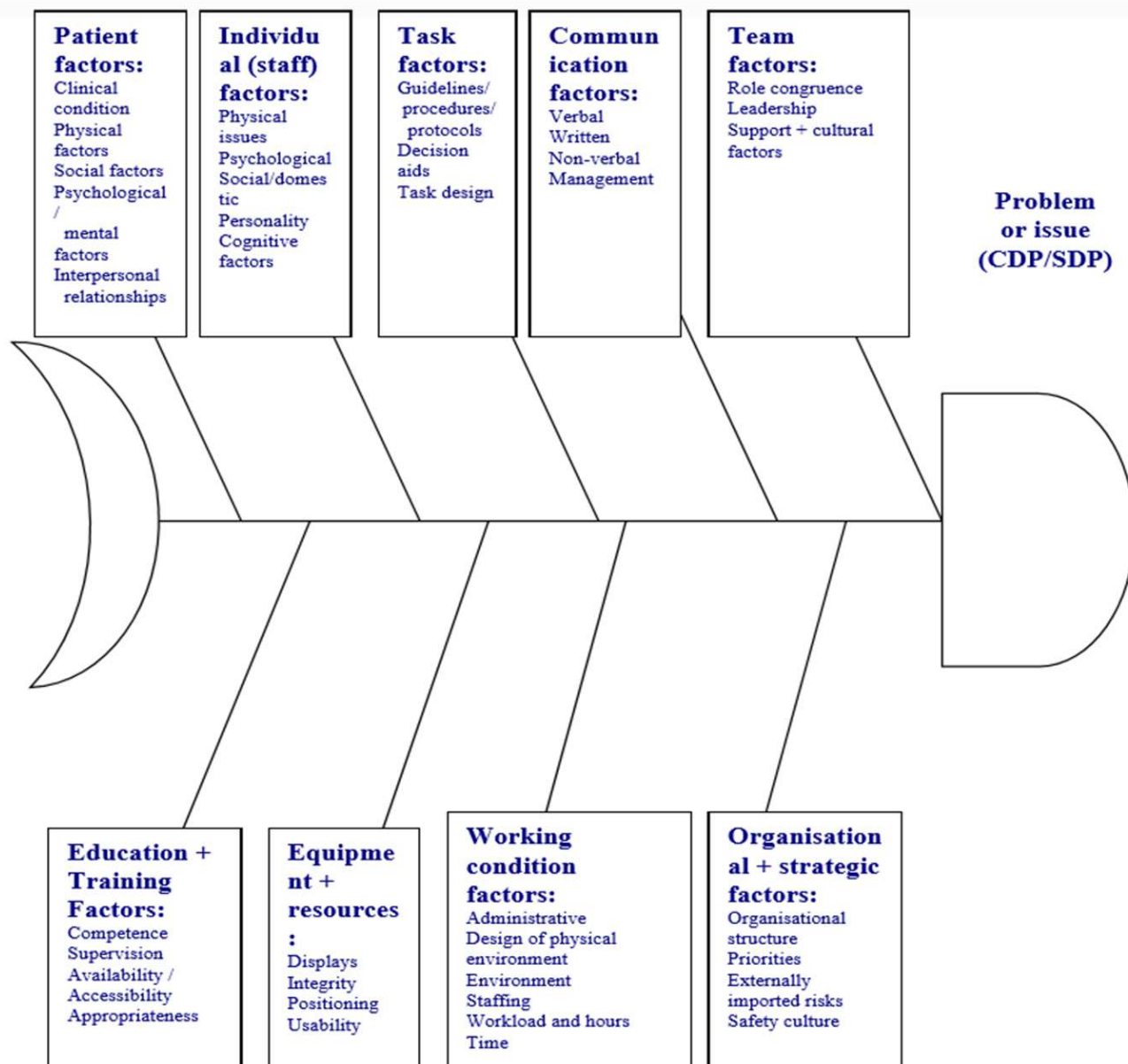
Cause and effect analysis helps you to think through the causes of a problem, including possible root causes, before you start to think of a solution – not just symptoms. By identifying all possible causes and not just the most obvious, you can work towards removing the problem. Working through cause-and-effect analysis enables those involved to gain a shared insight into the problem, develop possible solutions and create a snapshot of the team's collective knowledge.

When to use it

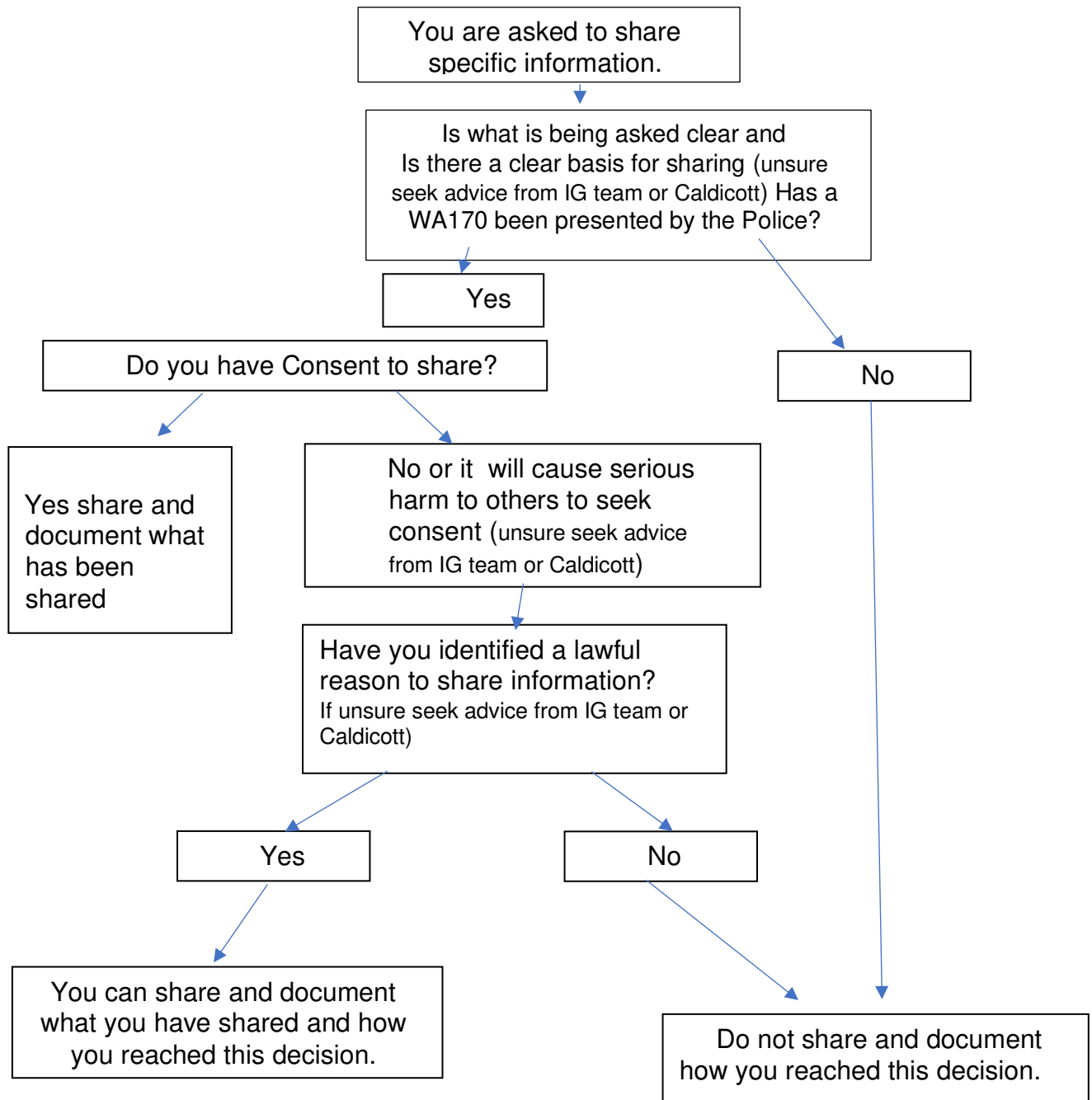
Use this tool when you are trying to determine why a particular problem is occurring. It will help you to fully understand the issue and to identify all the possible causes – not just the obvious.

How to use it

1. Identify the problem and consider it in detail: who is involved, when and where it occurs. Write the problem in a box and draw an arrow pointing towards it.
2. Identify the major factors, draw four or more branches off the large arrow to represent main categories of potential causes and label each line. Categories could include equipment, environment, procedures and people



APPENDIX 7 – FLOW CHART FOR SHARING INFORMATION WITH THE POLICE



Sharing information:

- identify how much information to share and what to share.
- Distinguish fact from opinion , share factual information only as far as possible
- Ensure that you are giving the right information to the right individual
- Ensure where possible, you are sharing the information securely
- Inform the patient that the information has been shared if they were not aware of this as long as this would not create or increase risk of serious harm
- If unsure regarding sharing information or what to share, please seek advice from the Caldicott for the trust or IG team

