NHS
South West
Yorkshire Partnership
NHS Foundation Trust

Document name:	Service User Confidentiality and Data Protection Policy, incorporating Information Sharing
Document type:	Policy
What does this policy replace?	Update of Service User Confidentiality and Data Protection Policy, incorporating Information Sharing v3
Staff group to whom it applies:	All staff within the Trust
Distribution:	The whole of the Trust
How to access:	Intranet
Version:	Version 3.1
Issue date:	January 2009 Revised September 2010 Revised February 2013 Reviewed January 2016 Revised May 2017 May 2018
Next review:	May 2019
Approved by:	Executive Management Team 17 May 2018
Developed by:	Information Governance Manager
Director leads:	Director of Nursing and Quality, Director of Finance and Resources
Contacts for advice:	Information Governance Manager

Contents

CONFIDENTIALITY AND DATA PROTECTION POLICY, INCORPORATING INFORMATION SHARING

1. Introduction

In order to provide high quality care, operate effectively and be accountable to the public the Trust must hold and process personal and sensitive personal data about services users in both electronic and paper formats.

The Chief Executive, supported by the Caldicott Guardian and SIRO, is accountable for ensuring the Trust meets its legal obligations and corporate responsibilities to ensure personal data remains confidential and is only used and shared in accordance with the data protection principles.

The Trust is registered as a data controller with the ICO and its level of confidentiality and data protection assurance is monitored as part of the data security and protection toolkit.

The Trust's data protection practices may also be subject to scrutiny by the ICO in the event of a consensual of compulsory audit.

2. Scope and Purpose

This policy applies to all service user personal data held and processed by the Trust and sets out the strategic governance arrangements for all such information that is created and received by the Trust in accordance with agreed best practice and with statutory and mandatory requirements.

This policy applies to service user personal data, from creation through to disposal, and to sharing of personal data from one or more organisations to one or more other organisations or to sharing data between different parts of the Trust.

This policy does not apply to personal/ service user data that is the responsibility of a health professional who acts as a data controller in their own right, such as those providing private healthcare services. Nor does it apply to sharing of information that doesn't involve personal data.

This policy does not apply to staff personal data that is obtained and held for the purpose of employment: a separate policy, Staff Confidentiality and Data Protection Policy, incorporating Information Sharing, is available.

This policy applies to personal data about employees who are or have been in receipt of healthcare from the Trust's services who have shared sensitive personal information for that purpose.

The information in this policy applies to all persons processing personal data in the course of discharging Trust functions. This includes but is not limited to:

- Full and part-time Trust employees
- Non-executive directors
- Medical locum staff
- Students and trainees

- Secondees and staff on temporary placements in the Trust
- Volunteers
- Governors
- Visiting professionals or researchers
- Employees of partner organisations that have approved access to Trust information
- Contracted third parties, including agency staff
- Contracted organisations and companies providing support services to the Trust

Where partnership arrangements exist with local authorities and other health service providers, this policy applies to all services and locations applicable to the Trust.

The overall purpose of this policy is to contribute to the achievement of the Trust's mission and values, performance targets and strategic objectives, which means recognising the value and importance of personal data as a corporate resource for the delivery of high quality services.

The policy will facilitate communication to all Trust employees of their roles and responsibilities in maintaining legal compliance and best practice in using and sharing personal data.

3. Definitions

Anonymised Information
Does not identify an individual directly and cannot be reasonably used to determine identity: requires the removal of names, addresses, full post codes and any detail or combination of details that might support identification

Caldicott Guardian
A senior person responsible for protecting the confidentiality of service user information and enabling information sharing; following a recommendation developed in the first Caldicott Report, which was mandated by the NHS Executive, every NHS organisation must have a Caldicott Guardian

Clinical Audit
The evaluation of clinical performance against standards or through comparative analysis with the aim of informing the management of services

Confidentiality
The state of keeping or being kept secret
Consent
Agreement that is freely given, specific, informed, explicit and verifiable; and involves a clear, affirmative action: it cannot be inferred from silence or inactivity

Data Controller
A person who, either alone or jointly or in common with other persons, determines the purposes for which and the manner in which personal data is processed

A data controller must be a "person" recognised in law:

- An individual,
- An organisation, or
- Another corporate or unincorporated body of persons

Data Processor
A person, other than an employee of the data controller, who processes personal data on behalf of the data controller

A data processor must be a "person" recognised in law:

- An individual,
- An organisation, or
- Another corporate or unincorporated body of persons

Data Security and Protection Toolkit (the toolkit)
A Department of Health (DH) policy delivery vehicle that draws together the legal rules and central guidance set out by DH policy and presents them in a single standard as a set of information governance requirements. Organisations within the scope of the Toolkit are required to carry out self-assessments of their compliance against the requirements.

Data Subject
An individual who is the subject of personal data

Disclosure
The divulging of or provision of access to information

European Economic Area (EEA)
The EEA consists of the member states of the EU plus certain other countries that are part of the EU's single market. A full list of EEA countries is available on the following webpage: https://www.gov.uk/eu-eea

Healthcare Purposes
All activities that directly contribute to the diagnosis, care and treatment of an individual and the audit and assurance of the quality of the healthcare provided; does not include teaching, financial audit and other management activities

Human Rights Act 1998 – Article 8: Right to Respect for Private and Family Life
Everyone has the right to respect for his private and family life, his home and his correspondence.

There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Inaccurate Data
Personal data is inaccurate if it is incorrect or misleading as to any matter of fact; personal data is not inaccurate if it faithfully represents someone's opinion about an individual, even if the opinion proves incorrect, for example, a health professional's opinion about an individual's condition. If the data subject disagrees with the opinion

the data would not need to be “corrected” but the data controller may have to add a note stating the subject’s disagreement.

Information Commissioner’s Office (ICO)
The UK’s independent body, sponsored by the Government Department for Media, Culture and Sport, for upholding information rights in the public interest: every organisation that processes personal information must register as a data controller with the ICO and failure to do so is a criminal offence. The ICO’s key responsibilities are to:

- address concerns raised by members of the public about the information rights practices of data controllers
- take actions to change the behaviour of data controllers, including undertakings, enforcement notices, consensual or compulsory audits, monetary penalties and individual prosecutions

The ICO is the UK’s supervisory authority for compliance with the General Data Protection Regulation.

Information Sharing Protocols – Inter Agency
Documented rules and procedures for the disclosure and use of personal information that specifically relate to security, confidentiality and data destruction, between two or more organisations

Personal Data
Information that can identify an individual directly or indirectly, including personal identifiers such as IP addresses

Data protection impact Assessment (DPIA)
A process that assists organisations in identifying and minimising the privacy risks of project plans and proposals to ensure risks are minimised while allowing the aims of a project to be met wherever possible

Processing
Processing in relation to information or data means obtaining, recording or holding the information or data or carrying out any operation or set of operations on it, including:

a. organisation, adaptation or alteration of the information or data,
b. retrieval, consultation or use of the information or data,
c. disclosure of the information or data by transmission, dissemination or otherwise making available, or
d. alignment, combination, blocking, erasure or destruction of the information

Pseudonymised Information
In the possession of the holder it cannot reasonably be used to identify an individual, however, the original provider of the information may retain a means of identifying individuals by attaching codes or unique references so that the information is only identifiable to those who have access to the key or index

Public Interest
Exceptional circumstances that justify overruling the right of an individual to confidentiality in order to service a broader, societal interest: public interest decisions are complex and must take account of the potential harm that disclosure may cause

and the interest of society

Recipient
Any person to whom personal data is disclosed, including any person to whom it is disclosed in the course of processing the data for or on behalf of the data controller; does not include any person to whom disclosure is or may be made as a result of, or with a view to, a particular inquiry by or on behalf of a person who has the legal power to make it, e.g.: the police, revenue and customs.

Relevant Filing System
Non-automated records that are structured in a way that allows ready access to information about individuals: a relevant filing system is considered to exist where records relating to individuals, such as health or employment records, are held in a sufficiently systematic, structured way as to allow ready access to specific information about those individuals

Senior Information Risk Owner (SIRO)
An executive or senior manager who is familiar with information risk and the organisation's response to risk: all NHS organisations must have a SIRO who takes overall ownership of the information risk policy, acts as champion for information risk at Board level and provides advice to the Chief Executive on the content of the Statement of Internal Controls in regard to information risk

Social Care
The support provided for vulnerable people, whether children or adults, including those with disabilities and sensory impairments: it excludes "pure" healthcare (hospitals) and community care, e.g.: district nurses; but may include services such as respite care

Special Category Data
Information about an individual's:

- race
- ethnic origin
- politics
- religion
- trade union membership
- genetics
- biometrics
- health
- sex life
- sexual orientation

Third Party
Any person other than:

a. the data subject,
b. the data controller, or
c. a data processor authorised to process personal data for the data controller

4. Duties

Overall responsibility for data protection and confidentiality of personal data held by the Trust lies with the Chief Executive. This responsibility extends to legacy data of preceding and obsolete organisations.

Executive Management Team (EMT)

- Approving this policy and ensuring it is reviewed and monitored
- Ensuring resources are available to support this policy

Director Leads

- Providing confidentiality and data protection assurance to the Trust Board
- Overseeing the development of this policy
- Ensuring a process is in place to monitor the compliance and effectiveness of this policy
- Ensuring formal and standardised risk management processes are followed in relation to confidentiality and data protection
- Advising the EMT on issues affecting service delivery
- Acting as an escalation point for discussion and resolution of issues

Caldicott Guardian

- Ensuring service user identifiable information is used, transferred and shared appropriately and securely
- Acting as the "conscience" of the Trust, providing advice on options for the lawful and ethical processing of service user identifiable information
- Providing advice on service user confidentiality
- Making final decisions on proposed breaches of service user confidentiality within the framework of this policy

Senior Information Risk Owner (SIRO)

- Reporting risks associated with personal data to the Trust Board
- Ongoing development and day to day management of risk management for the security of personal information

Data Protection Officer

- Acting as the main point of contact for communications with the ICO
- Acting as the contact point for any issues pertaining to confidentiality, data protection or information sharing
- Monitoring and taking a risk-based approach to organisational compliance with the data protection principles
- Providing regular compliance reports to the SIRO
- Providing advice on compliance to Trust staff
- Providing training and raising awareness
- Providing advice on data protection impact assessments
- Maintaining expert knowledge of data protection
- Monitoring data protection breaches and recommending appropriate action
- Reporting personal data breaches to external bodies as required

Information Management &Technology Task & Action Group (IM&T TAG)

- Reviewing the content of the Trust's IM&T Strategy to ensure it remains "fit for purpose" meeting local priorities and national guidance
- Developing, for EMT approval, an action plan to meet the ongoing requirements of the IM&T Strategy
- Ensuring achievements against the requirements of the plan are reported to and reviewed by the TAG on a quarterly basis

Improving Clinical Information Group (ICIG)

- Providing assurance over this policy and the resultant risk to EMT
- Monitoring risks associated with confidentiality and data protection
- Ensuring the principles set out in this policy are complied with when changes to processes and systems are planned
- Reviewing the recommendations of audit reports and progress of action plans
- Providing performance reports and assurance to the Clinical Governance & Clinical Safety Committee
- Monitoring and reviewing this policy
- Commissioning audits to ensure the effectiveness of this policy
- Ensuring policy requirements are communicated

Managers

- Ensuring staff are briefed on policy requirements
- Enabling policy implementation locally
- Ensuring staff are adequately trained in confidentiality and data protection as appropriate to their role, providing guidance and overseeing compliance with this policy

All staff

Adherence to the requirements set out in this policy and associated documents

5. Principles

This section of the policy sets out the requirements for confidentiality, data protection and information sharing in respect of personal data. The final subsection covers other legislative provisions and requirements that impact on confidentiality, data protection and information sharing.

Where applicable, the Trust will adhere to codes of practice or other guidance that has been published by the government and the ICO.

5.1 Confidentiality

Trust service users entrust us with, or allow us to gather, sensitive information about them as part of their seeking treatment: they do so in confidence with the legitimate expectation that their privacy will be respected and staff will act appropriately. In certain circumstances individuals may lack the competence to extend this trust but this does not diminish the duty of confidentiality.

The Trust must make records to support healthcare, to meet legal requirements and for the trust of service users to be retained; however, the Trust will not use or disclose information that can identify individuals for purposes other than healthcare without the

individual's explicit consent, some other legal basis or where a robust public interest or legal justification to do so exists.

5.1.1 Disclosing and Using Confidential Information: No Surprises

Service users must be made aware of information disclosures that must take place in order for the Trust to provide them with high quality care, in particular, clinical governance and clinical audits, which are components of healthcare provision that might not be obvious to service users so must be drawn to their attention.

The Trust will take steps to inform service users that information needs to be shared between members of care teams and between different organisations involved in their healthcare provision: this is particularly important where disclosure extends beyond NHS bodies.

Many current uses of confidential information do not contribute to or support the healthcare that a service user receives but are extremely important and provide benefits to society, for example, medical research, protecting public health, health service management and financial audit. These uses are not directly associated with healthcare and the Trust will not assume that service users seeking healthcare are content for their information to be used for these purposes.

Further information on sharing information that identifies an individual where the information is held under a legal obligation of confidentiality is included in Annex B of the Confidentiality - NHS Code of Practice.

5.1.1.1 Legal Considerations

The disclosure and use of Trust-held confidential information must meet the minimum standard set out by law and also the requirements of the government and professional, regulatory bodies.

There are a range of statutory provisions that limit or prohibit the use and disclosure of confidential information in specific circumstances or require information to be used or disclosed: details of current legal requirements and permissions can be found in Appendix A of this policy.

Key questions for confidentiality decisions and examples of confidentiality decisions for health care purposes, for medical purposes other than healthcare and for non-medical purposes are included in Annex C of the Confidentiality - NHS Code of Practice.

5.1.2 Consent to Disclosure

Service users have a right to object to the use and disclosure of confidential information that identifies them and the Trust has a duty to make them aware of this right. If service users choose to prohibit information being disclosed to other health providers involved in providing their care it may mean the care that can be provided is limited: service users must be informed if their decisions about disclosure could have implications for the provision of their care or treatment as clinicians may be unable to treat service users safely or provide continuity of care without relevant information and medical history.

Where the Trust has informed service users of the information listed in section 5.4.1, then consent is not usually required for information disclosures needed to provide health or social care or treatment; however, the Trust will pay special attention to issues around child consent. Further information on consent issues pertaining to children and young people is included in Annex B of the Confidentiality - NHS Code of Practice.

Where the purpose is not directly concerned with the health or social care or treatment of a service user, consent cannot be assumed and the Trust will make additional efforts to gain consent or identify an alternative lawful basis for processing.

When situations arise where consent cannot be obtained for the use or disclosure of person identifiable information the Trust will ensure the public interest in this use outweighs issues of privacy: further information on public interest disclosures can be found in Appendix A of this policy.

5.1.2.1 Deceased Service Users

The duty of confidentiality persists after a service user has died: an exception exists where disclosure of personal data is required by statute or is ordered by a court. Further information on statutory provisions and other circumstances where the duty of confidentiality can be overridden is provided in Appendix A of this policy.

5.1.3 Obligations on Individuals Working in or Under Contract to the NHS

All staff must meet the standards outlined in the Confidentiality - NHS Code of Practice as well as their contractual obligations and, where applicable, their professional codes of conduct.

Where organisational systems and processes are not yet in place Trust staff must demonstrate that they are working within the spirit of the Confidentiality - NHS Code of Practice and are making every reasonable effort to comply.

If the need for change to Trust systems and processes arises the information governance team must be informed of any specific problems or barriers to change.

5.1.3.1 Providing a Confidential Service

The confidentiality model outlines the requirements that Trust employees must meet in order to provide service users with a confidential service:

a. Protect – look after service users' information;
b. Inform – ensure service users are aware how their information is used;
c. Provide choice – allow service users to decide if their information can be disclosed or used in particular ways;
d. Improve – always look for better ways to protect, inform and provide choice.

Detailed requirements for providing a confidential service are included in Annex A of the Confidentiality - NHS Code of Practice.

5.1.3.1.1 The Caldicott Principles

Everyone who handles confidential, service user data must follow the Caldicott principles:

i. Justify the purpose
Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed by an appropriate guardian.

ii. 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 service users to be identified should be considered at each stage of satisfying the purpose(s).

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

iv. 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 they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

v. Everyone with access to personal confidential data should be aware of their responsibilities
Access should be taken to ensure that those handling personal confidential data – both clinical and non-clinical staff – are made fully aware of their responsibilities and obligations to respect confidentiality.

vi. Comply with the law
Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

vii. The duty to share information can be as important as the duty to protect confidentiality
Health and social care professionals should have the confidence to share information in the best interests of their service users within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

5.2 Data Protection

The Trust has a legal duty under the General Data Protection Regulation to control how personal information about living individuals is used.

Article 5 of the Regulation lists six data protection principles that must be adhered to when personal information held by the Trust is processed.

Personal data must 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, for scientific or historical research purposes or for 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 it is processed
d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay
e) Kept in a form that permits identification of a data subject for no longer than is necessary for the purposes for which is processed; personal data may be stored for longer periods insofar as it will be processed solely for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR to safeguard the rights and freedoms of individuals
f) Processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures

5.2.1 Exemptions and derogations

Exemptions from the General Data Protection Regulation's transparency obligations and individuals' rights that will be introduced in the UK are set out in the Data Protection Bill. Areas that may be safeguarded by the introduction of exemptions are listed in Appendix D.

Derogations in relation to specific processing activities that will be provided in the UK are set out in the Data Protection Bill. Processing activities that may have derogations provided for are listed in Appendix D.

5.2.2 Anonymisation

The General Data Protection Regulation controls the use of 'personal data', which is data that allows individuals to be identified. Anonymisation is the process of turning personal data into a form that does not identify individuals and where identification is not likely to take place and, therefore, it is outside the scope of the Act and this policy.

5.2.3 Closed Circuit Television (CCTV)

CCTV cameras involve intrusion into individuals' lives and can raise privacy concerns: images of individuals are covered by the General Data Protection Regulation, as is information derived from images, such as vehicle registration numbers.

The Trust will ensure the potential impact on individuals' privacy is identified and taken into account when installing an operating a CCTV system.

Information on retaining and storing images, image quality and security in included in the Trust's Closed Circuit Television Policy.

A CCTV Code of Practice is available from the ICO.

5.2.4 Data protection impact Assessments (DPIAs)

A DPIA will be undertaken for any major project that involves the processing of personal data, for all types of processing listed in appendix E and for any other processing that is likely to result in a high risk to individuals' interests.

The information in appendix E will assist in determining if a DPIA is required: if a DPIA is not carried out the reason will be documented in the project or risk management process to which it is applicable.

The Data Protection Officer must be consulted when a DPIA is undertaken as well as appropriate individuals and experts who can assist in its completion.

Where high risk processing is identified the Data Protection Officer will consult the ICO, which will issue written processing advice, a warning not to process or a ban on the processing.

A DPIA template is available from the Data Protection Officer.

5.2.5 Deceased Individuals' Data

The General Data Protection Act does not cover data about deceased individuals; however, the duty of confidentiality persists after death: refer to sections 5.1 and 5.1.2.1 of this policy.

5.3 Information Sharing

For the purpose of this policy information sharing is defined as:

- the sharing of personal data between the Trust and one or more third party organisations, or,
- the sharing of personal data between different parts of the Trust.

It can take the form of:

- A reciprocal exchange of personal data
- One or more organisations providing personal data to a third party or parties
- Several organisations pooling personal data and making it available to each other
- Several organisations pooling personal data and making it available to a third party or parties
- Exceptional, one-off disclosures of personal data in unexpected or emergency situations
- Different parts of the Trust making personal data available to each other for different purposes

It will be one of the following types:

- Systematic sharing – regular, routine sharing of the same data sets shared or pooled between the same organisations for specific and established purposes
- Exceptional sharing – ad-hoc or one-off decisions to share in conditions of real urgency

5.3.1 Sharing with a Data Processor

Where the Trust uses a data processor:

- the data processor will only act on the Trust's instructions, and,
- the data processor will have security in place that is equivalent to that imposed on the Trust by the data protection principle set out in Article 5f, and,
- the data processor's data protection responsibilities will all be imposed on it through its contract with the Trust.

5.3.2 The Trust as Data Processor

Where the Trust acts as a data processor on behalf of a data controller:

- the Trust will only act on the data controller's instructions, and,
- the Trust will have security in place that is equivalent to that imposed on the data controller by the data protection principle set out in Article 5f, and,
- the Trust's data protection responsibilities will all be imposed on it through its contract with the data controller.

5.3.3 Sharing within the Trust

The data protection principles apply to sharing of information within the Trust where there is a difference in purpose.

5.3.4 Legislative Requirements

As the NHS derives its powers from statute, relevant legislation exists that may permit data sharing that is required for the NHS's functions but does not mention data sharing explicitly:

- Express obligations – legal obligations to share particular information with a named organisation in highly specific circumstances
- Express powers – often referred to as 'gateways', permit disclosure of information for certain purposes
- Implied powers – where legislation is silent on the issue of data sharing but the proposed sharing would be 'reasonably incidental' to an express power that the Trust has to engage in another activity

5.3.5 Deciding to Share

When deciding whether to enter into an arrangement to share personal data as a provider, a recipient or both, the Trust will identify the objective that it is meant to

achieve, consider the potential benefits and risks to individuals or society and assess the likely results of not sharing.

5.3.6 Fairness

The Trust will ensure that people are generally aware that their personal data is shared and what it is being used for, whether this is routine data sharing or a single, one-off disclosure.

5.3.6.1 Privacy Notices (Fair Processing Notices)

The Trust will provide a privacy notice leaflet when first collecting an individual's personal data and a privacy notice is also available on the Trust's Internet site or from the Data Protection Officer.

5.3.6.2 Sharing without the Individual's Knowledge

Under the General Data Protection Regulation individuals have a right to be informed that personal data about them has been or is going to be shared even if their consent for the sharing is not needed.
Exemptions from the General Data Protection Regulation's transparency obligations and individuals' rights are set out in the UK's Data Protection Bill.

5.3.6.2.1 Ad-hoc or 'One-off' Sharing

Where it is proposed that very sensitive information is shared, with or without the individual's knowledge, the Trust will seek appropriate professional judgement to ensure it is processed fairly.

5.3.6.2.2 Emergency Response Situations

The General Data Protection Regulation does not prevent sharing of personal data when it is appropriate to do so: where the Trust is required to make a judgement about whether personal data can be shared, the risks involved in not sharing will be considered.

5.3.6.3 Security Measures

Security requirements that are specific to the type of personal data will be included in individual data sharing agreements.

5.3.7 Responsibility

The Trust expects that every other organisation involved in a data sharing initiative will take responsibility and accept liability for the information disclosed or received and that a senior, experienced person in each of the organisations will take on overall responsibility for information governance, legal compliance and providing advice to staff faced with making decisions about data sharing. For NHS organisations the senior, responsible person will be the Caldicott Guardian.

5.3.7.1 Data Sharing Agreements

Where the Trust is involved in a data sharing arrangement with other organisations, a common set of rules to be adopted by all parties must be set out. A standalone agreement will not always be required, for example, information sharing arrangements may be written into contracts between parties; however, sharing of service user data outside of the Trust must be approved by the Caldicott Guardian.

The Trust accepts that drafting and adhering to a sharing agreement does not provide any form of indemnity from legal action but supports the justification of the sharing and demonstrates awareness of the relevant compliance issues.

A data sharing agreement template is available from the Data Protection Officer.

all parties are signatories to the Inter-Agency Information Sharing Protocol the data sharing agreement in appendix III of the protocol can be used in conjunction with it. Current signatories are listed in appendix V.

5.3.7.2 Data Protection Impact Assessments (DPIAs)

Before entering into any data sharing arrangement the Trust will carry out a DPIA to assess the benefits that the sharing will bring to individuals or society and assess any risks or negative effects that may harm individuals or the reputation of the Trust that may arise if data is shared inappropriately. E

A DPIA template is available from the Data Protection Officer.

5.4 Individuals' Rights

The Trust accepts that the rights individuals have under the General Data Protection Regulation must not be affected by any data sharing arrangements.

5.4.1 Right to be informed

The Trust will provide individuals with information on the following at the time their personal data is collected:

a. its name and contact details (as the data controller)
b. the Data Protection Officer's contact details
c. why the information is needed and what it will be used for
d. the lawful basis for each use
e. any sharing of the information and, where applicable, the recipients
f. details of any international transfers
g. the retention periods
h. rights of access, rectification and erasure
i. rights to object or restrict processing
j. the right to data portability
k. the right to withdraw consent where it is the lawful basis for processing
l. the right to complain to the ICO
m. rights in relation to automated decision making

This information will usually be provided via the Trust's privacy notice, which is available from the Data Protection Officer.

If the Trust obtains personal data from a source other than the individual it relates to, the individual will be informed of the source of the data, in addition to the information listed above, when the first communication with the individual takes place or, if the data is to be shared, when it is disclosed.

5.4.2 Right of Access

Individuals have a right of access to their personal data and to supplementary information, which is the information listed in 5.4.1.

The process for managing such requests is set out in the Trust's Access to Health Records Policy.

When several organisations are sharing data it may be difficult for an individual to determine who they should make a request to: the Trust will ensure that clear information is provided in sharing agreements about how such requests can be made and include the process for receiving subject access requests in data sharing agreements so all parties know their responsibilities when a request is received.

5.4.3 Right to Rectification

Where an individual notifies the Trust that their personal data is inaccurate or incomplete, the Trust will ensure that it is rectified or is completed as appropriate within one month.

If the Trust identifies that personal data that has been shared with any recipient is inaccurate the recipient will be notified: where the sharing is covering by a sharing agreement, the agreed process for notification will be documented in it.

5.4.4 Right to Erasure

The Trust recognises that individuals have the right to have personal data erased, also known as 'the right to be forgotten; but that it is not an absolute right and it only applies in certain circumstances.

It must be noted that the right to erasure does not apply to special category data where the processing is necessary for:

- the purposes of preventative or occupational medicine, e.g.: assessing the working capacity of an employee, medical diagnosis, providing health or social care and managing health and social care systems or services
- public health purposes in the public interest, e.g.: protecting against cross-border health threats and ensuring high standards of quality and safety of health care, medicinal products and medical devices

The Trust will comply with requests to erase personal data if:

- It is no longer necessary for the purpose for which it was originally collected and processed for
- Consent is the lawful basis for processing and the individual withdraws consent

- Legitimate interests is the lawful basis for processing and there is no overriding legitimate interest to continue the processing
- It has been processed unlawfully, i.e.: in breach of the data protection principle set out in Article 5a
- It must be done to comply with a legal obligation
- It has been processed to offer information society services to a child

If personal data that has been shared with any recipient will be erased the recipient will be notified: where the sharing is covering by a sharing agreement, the agreed process for notification will be documented in it.

The Trust will not comply with requests to erase personal data if the processing is necessary:

- To exercise the right of freedom of expression or information
- To comply with a legal obligation
- For performing a task carried out in the public interest or in the exercise of official authority
- For archiving purposes in the public interest, for scientific or historical research purposes where erasure is likely to render impossible or seriously impair the achievement of that processing
- For the establishment, exercise or defence of legal claims

5.4.5 Right to Restrict Processing

The Trust recognises that individuals have the right to request the restriction of their personal, insofar as the data will continue to be stored but its uses are limited; but that it is not an absolute right and it only applies in certain circumstances.

The Trust will restrict the processing of personal data if:

- The individual contests the accuracy and the Trust is verifying the accuracy
- It has been processed unlawfully, i.e.: in breach of the data protection principle set out in Article 5a; but the individual requests restriction rather than erasure
- The Trust no longer needs it but the individual requires it to be retained in order to establish, exercise or defend a legal claim
- The individual is exercising the right to object and the Trust is considering if there are legitimate grounds that override those of the individual

The Trust will not process restricted data unless:

- The individual has consented
- It is necessary for the establishment, exercise or defence of legal claims
- It is necessary for the protection or rights of another person
- It is necessary for reasons of important public interest

5.4.6 Right to Data Portability

The Trust recognises that individuals have the right to obtain and reuse their personal data for their own purposes across different services.

Where it is technically feasible, the Trust will take a reasonable approach to requests to securely transmit personal data in a structured, commonly used and machine-readable format if:

- The data was provided to the Trust by the individual, and,
- The lawful basis is consent, and.

- It is being processed by automated means, i.e.: it is not in paper form

5.4.7 Right to Object

The Trust accepts that individuals have a right to object to the following where they grounds relating to their particular situations:

- Processing for the performance of a task in the public interest or in the exercise of official authority
- Processing based on legitimate interests
- Direct marketing
- Processing for scientific and historical research or statistical purposes

The Trust will stop processing personal data immediately unless:

- There are demonstrable and compelling legitimate grounds for the processing that override the interests, rights and freedoms of the individual, or,
- The processing is necessary for the establishment, exercise or defence of legal claims.

The Trust will attempt to avoid objections by providing individuals with clear information about why their personal data is shared and what it will be used for.

5.4.8 Rights in Relation to Automated Decision Making, including Profiling

The Trust will only carry our automated decision where the decision is:

- Based on the individual's consent, or,
- Authorised by a UK law that is applicable to the Trust

Where the Trust identifies automated decision making it will:

- Notify individuals of the processing
- Advise how human intervention may be requested or automated decisions may be challenged
- Regularly check its decision making systems to ensure they are working as intended

6 Equality Impact Assessment

	Equality Impact Assessment Questions:	Evidence based Answers & Actions:
1	**Name of the document that you are Equality Impact Assessing**	Confidentiality and Data Protection Policy, incorporating Information Sharing
2	**Describe the overall aim of your document and context?** **Who will benefit from this policy/procedure/strategy?**	To give assurances to the EMT that the relevant legislation and standards are adhered to when personal information is processed All staff and service users
3	**Who is the overall lead for this assessment?**	Director of Nursing and Quality/ Director of Finance and Resources
4	**Who else was involved in conducting this assessment?**	Information Governance Manager
5	**Have you involved and consulted service users, carers, and staff in developing this policy/procedure/strategy?** **What did you find out and how have you used this information?**	Yes N/A
6	**What equality data have you used to inform this equality impact assessment?**	None
7	**What does this data say?**	N/A
8	**Taking into account the information gathered above, could this policy/procedure/strategy affect any of the following equality group unfavourably:**	**Yes/No**
8.1	**Race**	No
8.2	**Disability**	No
8.3	**Gender**	No
8.4	**Age**	No
8.5	**Sexual Orientation**	No
8.6	**Religion or Belief**	No
8.7	**Transgender**	No
8.8	**Maternity & Pregnancy**	No

8.9	**Marriage & Civil partnerships**	No
8.10	**Carers *Our Trust requirement***	No
9	**What monitoring arrangements are you implementing or already have in place to ensure that this policy/procedure/strategy:-**	
9a	**Promotes equality of opportunity for people who share the above protected characteristics;**	N/A
9b	**Eliminates discrimination, harassment and bullying for people who share the above protected characteristics;**	N/A
9c	**Promotes good relations between different equality groups;**	N/A
9d	**Public Sector Equality Duty – "Due Regard"**	N/A
10	**Have you developed an Action Plan arising from this assessment?**	No
11	**Assessment/Action Plan approved by**	N/A
12	**Once approved, you must forward a copy of this Assessment/Action Plan to the Equality and Inclusion Team: inclusion@swyt.nhs.uk** **Please note that the EIA is a public document and will be published on the web.** **Failing to complete an EIA could expose the Trust to future legal challenge.**	

7 Dissemination and Implementation Arrangements

All staff	• Legal and statutory duties • Responsibilities under this policy	• Annual, mandatory IG and data security essentials training • Induction and supervision
Caldicott Guardian	Confidentiality and data protection skills, knowledge and experience	Caldicott masterclass to be attended at least three-yearly; online training to be completed annually otherwise
Information Asset Owners (IAOs)/ Administrators (IAAs) and other identified staff as required	Requirements for data protection impact assessments and data sharing arrangements	One-off, in-house understanding data protection impacts and data sharing training

8 Monitoring Compliance and Effectiveness

Information governance incident numbers, categories and learning are reported to the Improving Clinical Information Group (ICIG), which reports to the Clinical Governance Committee.

Breaches of confidentiality are reported to the Trust Board via the Information and Performance Report.

The Information Governance Manager provides a monthly report to EMT, via the Director of Finance and Resources, which includes incident hot spots and actions taken.

A standing agenda item is included at the IM&T TaG for attendees (IAOs/ IAAs) to communicate key messages regarding incident hot spots and required actions to their relevant areas.

	Standard	**Monitoring process - evidence:**
1.	This document is reviewed and updated in accordance with Trust policy	The document on the intranet is up-to-date
2.	Relevant staff will be made aware of the policy and offered support and training	• Document is on the intranet • Reference in team brief • Record of meetings where implementation discussed • Content of and attendance at relevant training • Audit of staff awareness
3.	ICIG will use the number of incidents to monitor the effectiveness of the policy	ICIG to monitor incident numbers, categories and teams to report to Clinical Governance and recommend action plans
4.	IM&T TaG will use the categories of incidents to monitor the effectiveness of the policy and identify issues and training needs	IM&T TaG to monitor incidents types to report to ICIG
5.	Review of action plans	ICIG to review recommendations and action plans where appropriate.

9 Review and revisions

Following a recommendation made by ICO in their report on the Trust's 2016 data protection audit, information governance policies will be reviewed annually in line with the recommendations made in the IG Toolkit.

Revisions will be made if a risk is identified or in accordance with changes to legislation, standards or other Trust policies that have an impact on this policy.

10 References

Department of Health Guidance and Publications

- Caldicott Committee Report on the Review of Patient-Identifiable Information (December 1997)
  https://nationalarchives.gov.uk/www.dh.gov.uk/caldicott1.pdf
- Confidentiality: NHS Code of Practice
  https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice
- Information: To Share or Not To Share? The Information Governance Review ('Caldicott 2', April 2013)
  https://www.gov.uk/government/publications/the-information-governance-review

ICO Guidance

- Anonymisation: Managing Data Protection Risk Code of Practice
  https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf
- Code of practice for surveillance cameras and personal information
  https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf
- Conducting Privacy Impact Assessments Code of Practice
  https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf
- Data Sharing Code of Practice
  https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf

Legislation

- General Data Protection Regulation
- Human Rights Act 1998
  http://www.legislation.gov.uk/ukpga/1998/42/contents

NHS Digital Publications

- Disclosure of Personal Information to the Police
  https://www.igt.hscic.gov.uk/Resources/DisclosureofPersonalInformationtothePolice.pdf
- Information Governance Toolkit
  https://www.igt.hscic.gov.uk/
- NHS Care Record Guarantee
  http://systems.digital.nhs.uk/rasmartcards/strategy/nhscrg
- Public Interest Disclosures of Confidential Personal Information
  http://systems.digital.nhs.uk/infogov/iga/consultations/publicinttdisc.pdf
- Records Management Code of Practice for Health and Social Care 2016
  http://systems.digital.nhs.uk/infogov/iga/resources/rmcop/index_html
- Statutory Provisions that Override the Common Law of Confidentiality
  http://systems.digital.nhs.uk/infogov/iga/consultations/statprov.pdf

11 Associated Documents

Trust policies and procedures (Document Store):

- Access to Health Records Policy
- Closed Circuit Television Policy
- Data Quality Policy
- Health Records Management Policy
- Information Governance Policy
- Interpreting, Translation and Transcription Policy, incorporating the Accessible Information Standard
- Procedure for Permanent Removal of Information in a Patient Record
- Safe Haven Policy
- Staff Confidentiality and Data Protection Policy

Inter-Agency Information Sharing Protocol

12 Appendices

Appendix A - statutory provisions that override the common law duty of confidentiality

Exceptional circumstances apply when person identifiable information may be used or shared without the consent of the data subject, even if the data subject has previously objected to such use or sharing.

These exceptional circumstances are:

- Public interest disclosures
- Statutory requirements
- Statutory permissions
- Implied necessity
- Miscellaneous

Even where there is a statutory requirement to disclose information to a third party, the General Data Protection Regulation still applies and, unless doing so would undermine the purpose for which the information was shared, the obligation to inform an individual about who their information is shared with remains in force.

Public Interest Disclosures
The public interest justification in using or sharing the information outweighs the duty of confidentiality: circumstances are usually limited to circumstances where a third party is at risk or serious crime is involved.

A public interest justification for disclosure can be considered in situations where:

- Disclosure would be in the public interest, and,
- The purpose for the disclosure cannot be achieved with anonymised information, and,
- There is no statutory basis for disclosure, and,
- Consent has not been given because:
    - It is not practical to ask an individual for consent, e.g. the matter is urgent or the individual cannot be contacted, or,
    - It would be inappropriate to ask the individual for consent, e.g. they lack capacity to give consent or they are suspects who should not be informed they are under investigation, or,
    - The individual has been informed about a proposed disclosure and has objected

A disclosure of confidential, personal information might be justified in the public interest in the following circumstances:

To prevent serious harm
The Trust must distinguish between serious harm to the individual to whom the information relates and serious harm to other individuals: confidential information can be disclosed in the public interest without consent to prevent serious harm to others.

Where the individual concerned is an adult lacking capacity the best interests of the individual can be sufficient to justify disclosure.

If the individual concerned has the capacity to decide for themselves their best interests are not sufficient to justify disclosure: there has to be an additional public interest justification, which may or may not be in the service user's best interests.

In certain circumstances, such as where parents refuse to allow disclosure of information about a child who lacks capacity; healthcare professionals must act in the best interest of the child.

Where there is a risk of significant harm to a child, relevant confidential information can be released to social services in the public interest.

To prevent, detect or prosecute for serious crime

"Serious crime" is not defined in law but, in respect of disclosing confidential personal information in the public interest, it includes crimes that cause serious physical or psychological harm to one or more individuals, e.g.: murder, manslaughter, rape, kidnapping, child abuse and neglect.

Other crimes, such as theft or fraud, may not warrant breaching an individual's confidentiality but it may be possible to disclose some information about an individual's involvement in crime in the public interest without disclosing any healthcare information.

The Trust will assess whether the crime is sufficiently serious to warrant disclosure, for example, a prolonged period of incidents may be considered serious even though none might be significant in isolation.

Where there is insufficient information available to determine whether a disclosure may serve to prevent or detect a serious crime, the Trust will engage appropriate healthcare professionals to establish if concerns are justified and sharing of information is required.

The Trust will ensure only the minimum necessary information is disclosed where the public interest is engaged.

Further information is available in the IG Alliance's Disclosure of Personal Information to the Police guidance.

To serve another public interest

The Trust acknowledges that 'public interest' does not mean 'of interest to the public'.

The Trust's decision to disclose will take account of the likelihood of detriment to the individuals concerned: a proportionate disclosure will be considered where there is a clear benefit to the public but there would be little or no detriment to Trust service users.

The competing interests of the public, the individual(s) concerned and society must be balanced: the public interest achieved by the disclosure must be weighed against the potential damage to the individual(s) and society's interest in the Trust's provision of a confidential service.

Another relevant factor that will be considered is the potential damage to the relationship between the service users and the health professional and the risk of the service user terminating that relationship, therefore, the Trust will involve the health professional in decisions whether to share or not to share confidential information.

Account will also be taken of the risk of a breakdown in trust between the service user and the Trust and the loss of public confidence Trust services.

Statutory Requirements
A statutory requirement is a clear information provision that sets out the type of information and the circumstances in which it must be shared with or used by another party.

It is the responsibility of the Trust to ensure that only information that is absolutely necessary to satisfy the purpose is used or shared.

The Trust will ensure that a statutory requirement is correctly applied in that:

- The person making the request is empowered to do so
- All conditions specified in the legislation have been satisfied

The main statutory requirements that are likely to present in the health and social care sector are included in the table below.

Statutory Permissions
A statutory permission does not impose a requirement that information must be disclosed; it is permissive in that information may be disclosed when the service user has given consent or there is an overriding public interest. Objections may only be overridden where the public interest is significant, e.g.: detecting or preventing serious crime.

If a request is received where a statutory permission is claimed, the Trust will ensure that the provision is clearly identified and does what the requestor claims.

Examples of permissive statutory provisions that may present in the health and social care sector are included in the table below.

Implied Necessity
Where a specific statutory function cannot be delivered without access to confidential personal information it is possible to imply necessity, which has the force of statute and can, therefore, override confidentiality.

The body attempting to obtain or use Trust information will need to provide assurances in respect of the necessity of providing the information and the relevance of a related statutory function.

If the Trust receives a request for confidential personal information where implied statutory necessity is stated as the legal basis, legal advice will be sought.

Miscellaneous

There are a number of other ways in which information sharing may be authorised with sufficient force to override confidentiality and any objections made by individuals that are not strictly resulting from statutory provisions, e.g. court proceedings and coroners' investigations.

Further information is included in the table below.

Statutory Requirements	Description	Notes
Care Quality Commission (CQC)	The CQC is empowered by the Health & Social Care Act 2008 to require documents and information	S.76 and s.79 of the Health & Social Care Act 2008 govern the CQC's use and disclosure of confidential personal information
General Medical Council (GMC) investigations of a doctor's fitness to practise	S.35 of the Medical Act 1983 empowers the GMC to request access to a health record for the purposes of an investigation	
Health & Social Care Act 2012	Empowers NHS Digital to require that information, including confidential personal information, is provided to it	• NHS Digital may only use their powers when directed by the Health Secretary or NHS England • NHS Digital works under restrictions on when information collected can be passed onto others
Health & Social Care (Safety & Quality) Act 2015 s.115	Health and social care commissioners and providers have a duty to share information where it may result in improved outcomes for individuals	Explicitly requires objections to be respected and common law duty of confidentiality requirements to be met
NHS Act 2006 s.251	Empowers the Health Secretary to set the common law duty of confidentiality aside and enable confidential information to be used without consent	To date has only been used in relation to public health emergencies
NHS Counter Fraud investigations	Investigators are empowered by the NHS Act 2006 to require the disclosure of relevant parts of a health record if they believe it is needed for the investigation	
Public Health (Control of Disease) Act 1984/ Public Health (Infectious Diseases) Regulations 1988	Health professionals are required to notify local authorities of the identity, gender and address of any person suspected of having a notifiable disease	
Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1985	The following must be reported: • deaths, major incidents and	Refer to the legislation for further details re the reportable diseases and dangerous occurrences

	accidents resulting in more than three days off work • certain diseases and dangerous occurrences	http://www.legislation.gov.uk/uksi/1985/2023/made
Road Traffic Act 1988	Health professionals are required to provide to the police, on request, any information that may identify a driver alleged to have committed an offence	
Terrorism Act 2000/ Terrorism Prevention & Investigation Measures Act 2011	All persons must inform police immediately of information that may help: • to prevent an act of terrorism, or, • in apprehending or prosecuting a terrorist	

Permissive Statutory Provisions	**Description**	**Notes**
Crime & Disorder Act 1998	Permits disclosure to the police for strategic, cross-organisational planning to detect, prevent or reduce crime and disorder that an individual may be involved in	There is no clear statutory requirement to disclose: information may be shared if there is an overriding public interest
NHS Act 2006 s.251	Empowers the Health Secretary to make regulations that provide statutory permissions, explicitly setting the common law duty of confidentiality aside and enabling confidential personal information to be used without consent	S.251 enables the Health Secretary to make regulations that can be statutory requirements or provide statutory permissions
Police & Criminal Evidence Act 1984	Permits information to be disclosed to the police if it is believed that someone may be seriously harmed or death may occur if they are not informed	There is no clear statutory requirement to disclose: information may be shared if there is an overriding public interest

Miscellaneous	**Description**	**Notes**

Coroners' investigations	Health and social care organisations are obliged to disclose any information they hold about the deceased that is relevant to the investigation	The duty of confidentiality survives the death of an individual but the provision of confidential information to the coroner is a justifiable public interest exception
Courts and litigation	The judge or presiding officer of a civil, criminal or coroner's court can require the disclosure of personal information that is relevant to the proceedings	Information pertaining to what appear to be irrelevant matters must only be disclosed with consent: attempts to force disclosure must be objected to

Appendix B – Lawful bases for processing personal data

- Consent of the data subject
- It is necessary for the performance of a contract with the data subject or to take steps to enter into a contract with the data subject
- It is necessary for compliance with a legal obligation
- It is necessary to protect the vital interests of a data subject or another person
- It is necessary for the performance of a task carried out in the public interest or in exercise of the official authority vested in the data controller
- It is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject

N.B. public authorities can only use legitimate interests as a basis where the processing activity is **not** in the performance of its official tasks, e.g.: managing a car parking permit database

Appendix C – Conditions for processing special category data

At least one of the lawful bases for processing personal data (Appendix C) must be met whenever personal data is processed; however, if the data is special category data, at least one of other condition must also be met before processing can comply with the data protection principle set out in Article 5a:

- The data subject has given explicit consent to the processing of the data for one or more specified purposes

- It is necessary for the purposes of carrying out the obligations and exercising specific rights of the data controller or the data subject in the field of employment and social security and social protection law insofar as it is authorised by a UK or EU providing for appropriate safeguards for the fundamental rights and the interests of the data subject

- It is necessary to protect the vital interests of the data subject or of another person, where the data subject is physically or legally incapable of giving consent

- It is carried out in the course of the legitimate activities, with appropriate safeguards, by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that processing relates solely to members or former members, or to persons in regular contact with it in connection with its purposes, and the data is not disclosed outside the body without the consent of the data subject

- It relates to personal data that has been manifestly made public by the data subject

- It is necessary for the establishment, exercise or defense or legal claims or whenever courts are acting in their judicial capacity

- It is necessary for reasons of substantial public interest, or the basis of EU or UK law that is proportionate to aim the pursued, respects the essence of the right to data protection and provides for suitable and specific measures to safeguard the fundamental rights and interests of the data subject

- It is necessary for the purposes of preventative or occupational medicine, the assessment of the working capacity of an employee, medical, diagnosis, the provision of health or social care or treatment, or the management of health and social care systems and services on the basis of EU or UK law or pursuant to a contract with a health professional

- It is necessary for reasons of public interest in the area of public health, such as protecting against cross-border threats or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis on EU or UK law, which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular, professional secrecy

- It is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes based on EU or UK law that is proportionate to aim the pursued, respects the essence of the right to data

protection and provides for suitable and specific measures to safeguard the fundamental rights and interests of the data subject

Appendix D – exemptions from the transparency obligations and individuals' rights under the General Data Protection Regulation

Exemptions may be introduced to safeguard:

- National security
- Defense
- Public security
- The prevention, investigation, detection or prosecution of criminal offences
- Other important public interests, such as, economic or financial interests, public health and security
- The protection of judicial independence and proceedings
- Breaches of ethics in regulated professions
- Monitoring, inspection or regulation connected to the exercise of official authority regarding security, defense, crime prevention, ethics prevention or other important public interests
- The protection of the individual or of the rights and freedoms of others
- The enforcement of civil law matters

Derogations may be introduced that cover processing activities including:

- Freedom of expression
- Freedom of information
- Public access to official documents
- National identification numbers
- Employee data
- Archiving
- Scientific and historical research
- Statistical purposes
- Secrecy obligations
- Churches and religious associations

Appendix E – data protection impact assessment

Screening questions

A DPIA will always be undertaken where any of the following apply:

- A change to the nature, scope, context or purposes of processing
- Processing of special category data on a large scale
- Processing personal data that could result in the risk of physical harm in the event of a security breach
- Processing criminal offence data on a large scale
- Use of new technology
- Combining, comparing or matching data from multiple sources
- Systematically monitor a publicly accessible place on a large scale
- Use of special category data, profiling or automated decision making to help make decisions on someone's access to a service, opportunity or benefit
- Processing personal data without providing a privacy notice directly to the individual
- Use of systematic and extensive profiling or automated decision-making to make significant decisions about people
- Profiling on a large scale
- Processing biometric or genetic data
- Processing personal data in a way that involves tracking individuals' online of offline location or behaviour
- Processing children's data for profiling or automated decision making, for marketing purposes or for offering online services directly to them

A DPIA may be undertaken where any of the following apply

- A major project involving the use of person data
- Processing of sensitive or highly personal data
- Processing of data about vulnerable individuals
- Use of innovative technological or organisational solutions
- Processing that involves preventing a data subject from exercising a right or using a service or contract
- Large scale processing
- Evaluation or scoring
- Automated decision making with significant effects
- Systematic monitoring:

Appendix F – checklist for review and approval of procedural document

	Title of document being reviewed: Confidentiality & Data Protection Policy	Yes/No/ Unsure	Comments
1.	**Title**		
	Is the title clear and unambiguous?	YES	
	Is it clear whether the document is a guideline, policy, protocol or standard?	YES	
	Is it clear in the introduction whether this document replaces or supersedes a previous document?	YES	
2.	**Rationale**		
	Are reasons for development of the document stated?	YES	
3.	**Development Process**		
	Is the method described in brief?	YES	
	Are people involved in the development identified?	YES	
	Do you feel a reasonable attempt has been made to ensure relevant expertise has been used?	YES	
	Is there evidence of consultation with stakeholders and users?	YES	Health Records Sub Group, Improving Clinical Information Group, IM&T TaG
4.	**Content**		
	Is the objective of the document clear?	YES	
	Is the target population clear and unambiguous?	YES	
	Are the intended outcomes described?	YES	
	Are the statements clear and unambiguous?	YES	
5.	**Evidence Base**		
	Is the type of evidence to support the document identified explicitly?	YES	
	Are key references cited?	YES	
	Are the references cited in full?	YES	
	Are supporting documents referenced?	YES	
6.	**Approval**		
	Does the document identify which committee/group will approve it?	YES	
	If appropriate have the joint Human Resources/staff side committee (or equivalent) approved the document?	N/A	

	Title of document being reviewed: Confidentiality & Data Protection Policy	Yes/No/ Unsure	Comments
7.	**Dissemination and Implementation**		
	Is there an outline/plan to identify how this will be done?	YES	
	Does the plan include the necessary training/ support to ensure compliance?	YES	
8.	**Document Control**		
	Does the document identify where it will be held?	YES	
	Have archiving arrangements for superseded documents been addressed?	YES	
9.	**Process to Monitor Compliance and Effectiveness**		
	Are there measurable standards or KPIs to support the monitoring of compliance with and effectiveness of the document?	YES	
	Is there a plan to review or audit compliance with the document?	YES	
10.	**Review Date**		
	Is the review date identified?	YES	
	Is the frequency of review identified? If so is it acceptable?	YES	
11.	**Overall Responsibility for the Document**		
	Is it clear who will be responsible implementation and review of the document?	YES	

Appendix G – version control

Version	Date	Author	Status	Comment / changes
1	Feb 2006	Nicola Smith	Final	Confidentiality Policy
2	Dec 2007	Nicola Smith	Final	Data Protection Policy.
1	Jan 2009	Nicola Smith	Final	Confidentiality and Data Protection Policy
1.2	Sept 2010	Nicola Smith	Final	Information Sharing, Confidentiality and Data Protection Policy
2	Feb 2013	Nicola Smith	Final	Revised
2.1	Jan 2016	Caroline Britten	Final	Reviewed
3	May 2017	Rachael Smith	Final	Confidentiality & Data Protection Policy incorporating Information Sharing
3.1	May 2018	Rachael Smith	Final	