Ashford and St. Peter's Hospitals
NHS Foundation Trust

Confidentiality & Data Protection Policy

Author: Mark Gubby
Information Governance Manager

Executive Lead: Simon Marshall
Director of Finance & Information

Status

Ratified by: Information Governance Steering Group

Last reviewed: Feb 2019

Next review due: Mar 2022

History

Issue	Date Issued	Brief Summary of Change	Author
1	28 Jan 14	Redraft of 'Confidentiality Policy'	Mark Gubby, Information Governance Manager
2	24 Jul 15	Updates throughout	Mark Gubby, Information Governance Manager
2	26 Feb 2019	Updates throughout to incorporate GDPR / DPA18	Jane Townsend, Information Governance Manager

For more information on the status of this document, please contact:	
Policy Author	Information Governance Manager
Department/Directorate	Digital Services
Date of issue	Jul 2019
Review due	Mar 2022
Ratified by	Information Governance Steering Group
Audience	All staff

Executive summary

The Trust has legal obligations to protect the confidentiality and privacy of all persons whose data it holds and uses. These legal obligations apply individually to every person working for or on behalf of the Trust.

This policy sets out the principles to which Trust working practices should conform, in order to help staff comply with the law and protect the rights and freedoms of Trust patients and staff.

Key Points

- The General Data Protection Regulation (GDPR) came into force on 25th May 2018, and is the biggest change to data protection legislation in 20 years, fundamentally changing the way organisations must handle and look after people's information.
- All information held in either manual or electronic format that identifies an individual must be processed (held, obtained, recorded, used and shared) in accordance with the six principles of the Data Protection Act 2018.
- All staff have a legal obligation to keep information secure and to protect confidential information from disclosure under the Common Law Duty of Confidentiality.

- Individuals are entitled to ask the Trust for copies of information that is held about them.

- All staff must receive Information Governance Training on an annual basis to ensure they are up to date on Trust policies and procedures.

All staff are individually responsible for complying with the law.

CONTENTS

Enclosure:
Equality Impact Assessment

1 INTRODUCTION

Ashford & St Peter's Hospitals NHS Foundation Trust ("**the Trust**") has legal obligations to protect the confidentiality and privacy of all persons whose data it holds and uses.

These legal obligations apply individually to every person working for or on behalf of the Trust.

The Trust has committed[1] to keep confidential all personal data relating to staff, patients and all other persons, using and sharing it only in accordance with the law and in the best interests of individual patients and the public.

1.1 Aim

The aim of this policy is:

(a) To identify and detail the roles and responsibilities associated with confidentiality and data protection throughout the Trust.

(b) To provide a framework within which the Trust will comply with the law.

(c) To set out the practices which staff are required and expected to follow, with the support of additional policies, procedures and guidance as may be published from time to time.

1.2 Scope

This policy applies to:

(a) All employees of the Trust, including but not limited to permanent, temporary, bank, contract, honorary and volunteer staff, and all other persons and organisations carrying out any function or work directly for or on behalf of the Trust.

(b) All data falling within the definition of either "personal data" or "confidential data" below, where the Trust has any role in determining the purposes for which or the manner in which the data are processed.

1.3 Non-personal data which may be commercially or otherwise sensitive to the Trust as a business are not included within the scope of this policy, but many of the principles may be applied equally.

2 DEFINITIONS

2.1 **Personal data.** "'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person" (GDPR - Article 4, paragraph 1)[2].

2.2 **Special Category data.** "Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data and biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation" (GDPR Article 9, paragraph 1).

[1] ASPH Information Governance Policy – Jun 2015.
[2] GDPR – Article 4, Definitions

2.3 **Confidential data.** Any personal data which were given in confidence, or to which a duty of confidence is otherwise owed under the common law or professional obligations. This includes all healthcare information held by the Trust, for living and deceased patients.

2.4 **Processing.** "'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction" (GDPR-Article 4, paragraph 2).

2.5 **Data subject.** Any person about whom the Trust processes personal data, whether a member of staff, patient, member of the public or any other person.

2.6 **Data controller.** "'Controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law" (GDPR-Article 4, paragraph 7).

2.7 **Data processor.** "'Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller (GDPR Article 4, paragraph 8).

2.8 **Data breach.** A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.[3]

2.9 **Disclosure.** Any release of personal or confidential data to any person or organisation, other than the data subject or a data processor, for the recipient to use for their own purposes.

2.10 **Information Asset Owner.** The senior member of staff ultimately responsible for the secure and proper operation of any physical or electronic system which processes information of value to the Trust (an "**information asset**"). This role is defined fully in the Information Security Policy.

2.11 **Data Protection Officer (DPO).** The DPO assists the Trust to monitor internal compliance, inform and advise on its data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority.

3 ROLES & RESPONSIBILITIES

3.1 **Caldicott Guardian.** The Medical Director is appointed as the Caldicott Guardian[4], whose duties are:[5]

(a) Champion confidentiality issues at Board and senior management level, acting as the

[3] ICO "Personal Data Breaches" - https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/
[4] UK Caldicott Guardian Council - https://www.gov.uk/government/groups/uk-caldicott-guardian-council
[5] Manual for Caldicott Guradians - https://www.gov.uk/government/groups/uk-caldicott-guardian-council#manual-for-caldicott-guardians

'conscience' of the organisation.

(b) Ensure that confidentiality and data protection issues are appropriately reflected in organisational strategies, policies and working procedures.

(c) Oversee all arrangements, protocols and procedures where confidential patient information may be shared with external bodies, both within and outside the NHS.

(d) Provide a focal point for patient confidentiality and information sharing issues.

3.2 **Senior Information Risk Officer (SIRO).** The Director of Finance and Information is appointed as SIRO, whose duties are:

a) To have overall responsibility for an organisation's information risk policy.

b) To be accountable and responsible for information risk across the organisation.

c) To ensure that everyone is aware of their personal responsibility to exercise good judgement, and to safeguard and share information appropriately.

d) To provide the focus for the management of information risk at Board level.

e) To provide the CEO with assurance that information risk is being managed appropriately and effectively across the organisation and for any services contracted for by the organisation.

3.3 **Chief Executive Officer** (CEO). The CEO, with the support of the Trust Board, duties are:

a) To have overall responsibility for ensuring that information risks are assessed and mitigated to an acceptable level.

b) To ensure that staff are aware of the need to comply with the GDPR/DPA 18/DPA 18, in particular with the rights of patients wishing to access personal information and or their health records.

c) To ensure that staff are aware of requirements of the common law duty of confidence as set out in Confidentiality: NHS Code of Practice

d) To ensure that arrangements with third parties who process personal data on behalf of the Trust are subject to a written contract which stipulates appropriate security and confidentiality.

3.4 **Data Protection Officer (DPO).** The DPO is the Information Governance Manager whose duties are:

a) To have overall responsibility for managing and effectively implementing all activities necessary to achieve compliance with the GDPR/DPA 18/DPA 18 throughout the Trust.

b) To inform and advise the organisation and its employees about their obligations to comply with the GDPR/DPA 18 and other data protection laws

c) To monitor compliance with the GDPR/DPA 18 and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; and conduct internal audits

d) To be the first point of contact for supervisory authorities and for individuals whose data is processed (patients/staff).

3.5 **Information Governance Manager.** The Information Governance Manager is appointed as the Data Protection Lead for the Trust, whose duties are:[6]

(a) Promote compliance with relevant legislation and NHS policy.

(b) Formulate and maintain policies, procedures and guidance materials as may be necessary.

(c) Provide specialist advice and guidance to any staff member on request, on any aspect of this policy.

(d) Maintain the Trust's data protection registration with the Information Commissioner's Office, and liaise with the Information Commissioner's Office as may be required.

3.6 **Service, Department and Line Managers.** All managers will:

(a) Enforce the requirements of this policy, and have due regard to confidentiality and data protection, when implementing working processes within their service areas and departments.

(b) Promote this and other related policies and procedures, as both mandatory requirements and good professional practice.

(c) Monitor confidentiality practices within their service areas and departments, provide support and guidance to their staff, and escalate to senior managers and specialist data protection roles where appropriate.

(d) Ensure all their staff comply with confidentiality and data protection training requirements.

3.7 **All staff.** All staff will:

(a) Comply with the common law duty of confidence, the Data Protection Act 2018, and other relevant legislation.

(b) Comply with NHS[7,8] and relevant professional[9,10] requirements.

(c) Comply with this and other related policies and procedures.

(d) Report all identified and suspected breaches in accordance with the Incident Management Policy, in order to contribute to improvement of practice.

---

[6] ASPH Information Governance Manager job description – May 2015.
[7] DH "Confidentiality: NHS Code of Practice" – Nov 2003; https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice
[8] NHS Digital "A guide to confidentiality in health and social care", v1.1 – Sep 2013; https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/a-guide-to-confidentiality-in-health-and-social-care
[9] GMC "Confidentiality: good practice in handling patient information" – 2018; https://www.gmc-uk.org/ethical-guidance/ethical-guidance-for-doctors/confidentiality
[10] NMC "Professional standards of practice and behaviour for nurses, midwives and nursing associates" – Mar 2015; http://www.nmc.org.uk/standards/code/

(e) Seek advice from senior colleagues, or the Information Governance Manager, if in doubt of any part of this policy or confidentiality requirements.

(f) In summary, **keep confidential the personal information of patients, staff and all other persons, only using it where strictly necessary and where a legitimate relationship or other lawful basis exists.**

Failure to comply with the law or Trust policy may lead to disciplinary or professional regulatory action, dismissal, fines, or criminal prosecution.

4 LEGAL CONTEXT

The legal requirements described in this section are a summary of the core obligations which will normally need to be assessed for each collection, use or disclosure of personal or confidential data.

4.1 Caldicott Guidelines

In 1997 the Caldicott Committee Report found that confidentiality and security compliance was patchy across the NHS. In response to this patchy compliance across the NHS, the Caldicott Committee developed 6 principles which staff must apply when using patient information. The 2013 Information Governance Review, amended the 6 Caldicott principles to include a seventh Caldicott principle:

1. Justify the purpose(s);
2. Don't use personal confidential data unless it is absolutely necessary;
3. Use the minimum necessary personal confidential data;
4. Access to person confidential data should be on a strict need-to-know basis;
5. Everyone with access to personal confidential data should be aware of their responsibility;
6. Comply with the law;
7. The duty to share information can be as important as the duty to protect patient confidentiality.

4.2 NHS Confidentiality Code of Practice

The Department of Health Confidentiality Code of Practice published in 2003 states its implementation will enable an NHS organisation to achieve a confidential service in which all patient information is processed fairly, lawfully and as transparently as possible.

The Department of Health Confidential model has 4 main elements:

4.3 PROTECT – look after patient's information

In order to provide a confidential service, the Trust needs to ensure that it protects patient information at all times, so only staff who have a need to access the confidential information can do so.

Staff should check that any callers, by telephone or in person, are correctly identified.

There could be a significant risk of harm to a patient through impersonation by those seeking information improperly.

Staff should share the minimum information necessary to provide safe care or to satisfy other legitimate purposes, bearing in mind that missing information can harm patient care.

A patient's confidentiality must be respected in response to enquiries from external individuals or organisations (e.g., media, police, and insurance companies). In these circumstances express consent must be obtained from the patient and/or proper (legal) authority demonstrated before any disclosure is made.

Staff must not use any of the Trust's IT systems to make an unauthorised disclosure or copy of confidential information belonging to the Trust.

INFORM – ensure that patients are aware of how their information is used
The Trust must inform patients of the intended use of their information, giving them the choice to give or withhold their consent and protect their identifiable information from unwarranted disclosure.

PROVIDE CHOICE – allow patients to decide whether their information can be disclosed or used in particular ways.
Patients have different needs and values – this must be reflected in the way that they are treated, both in terms of their medical condition and the handling of their personal information. Staff must:

- Seek the patient's consent prior to using their information in ways that do not directly contribute, or support the delivery of their care;
- Respect a patient's decisions to restrict the disclosure or use of their information, other than where exceptional circumstances apply;
- Communicate effectively with patients to ensure they understand the implications if they choose to agree or restrict the disclosure of their information.

IMPROVE – always look for better ways to protect, inform and provide choice
The Trust accepts that technology changes, therefore the Trust will continually review its processes to ensure that the 4 elements of the Department of Health Confidentiality is protecting patient information to the highest level at all times.

4.4 **Common law duty of confidence**
The Trust considers that information relating to its patients' physical and mental health or condition is given in confidence, in the expectation that the information will not be disclosed outside the health professionals providing direct care or the administrative staff directly supporting them (collectively "the care team").

Any disclosure of confidential data outside the care team is therefore subject to the common law duty of confidence, and can only occur where there is:

(a) A legal obligation; or

(b) Explicit consent of the data subject.

Whilst the Data Protection Act 2018 only covers living individuals' information, the Common Law Duty of Confidentiality ensures that a patient's right to confidentiality continues after their death.

4.5 **Section 251**
Section 251 of the NHS Act 2006 allows the common law duty of confidence to be set aside

in certain circumstances.[11]

"Section 251 approval" is granted either by the Health Research Authority (for research purposes) or the Secretary of State (for non-research purposes), following a successful application to the Confidentiality Advisory Group.[12]

All activities carried out under Section 251 approval must demonstrably comply with DPA18.

Section 251 approval is normally granted only if there is sufficient justification to process confidential patient information without consent.[13] Any proposal for a new use of data involving common law disclosure should therefore exhaust other lawful bases before considering an application for Section 251 approval.

Any use of data reliant on Section 251 should be referenced against a specific, in-date approval decision published by the Health Research Authority.[14]

4.6 **General Data Protection Regulations (GDPR)**
GDPR adds in new concepts of Accountability and Demonstrability for the processing of personal data on organisations, as well as increasing the rights of an individual to how organisations process their personal data.

4.7 **UK Data Protection Act 2018**
The Data Protection Act 2018 mirrors the GDPR and will remain in force until GDPR no longer applies once the UK has exited the EU. The purpose of the Act is to enhance and protect the rights and privacy of individuals, and to ensure that data about them cannot be processed without their knowledge or consent wherever possible. The Act covers personal data relating to living individuals.

4.8 **Regulatory Authority - Information Commissioner**
Data Protection (Charges and Information) Regulations 2018 requires every organisation who processes personal information to pay a data protection fee to the ICO. The Trust will continue to keep this registration up to date, details of this registration can be found on the Information Commissioner's website.

Under Article 30 of the GDPR, the Trust is required to keep a record of processing activities and will review this register on an annual basis, to ensure all processing of personal data is recorded and kept accurate and up to date.

4.9 **Legal Basis for Processing Personal / Special category Data**
"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 the information or data, including:

- Organisation, adaptation, alteration of the information or data;

[11] Approval is given under section 251 of the NHS Act 2006.
[12] NHS Health Research Authority "Section 251 and the Confidentiality Advisory Group"; https://www.hra.nhs.uk/about-us/committees-and-services/confidentiality-advisory-group/
[13] NHS Health Research Authority "General Data Protection Regulation"; https://www.hra.nhs.uk/planning-and-improving-research/policies-standards-legislation/data-protection-and-information-governance/gdpr-guidance/gdpr-and-use-confidential-patient-information-without-consent/
[14] NHS Health Research Authority "Confidentiality Advisory Group registers"; https://www.hra.nhs.uk/planning-and-improving-research/application-summaries/confidentiality-advisory-group-registers/

- Retrieval, consultation or use of the information or data;
- Disclosure of the information or data by transmission, dissemination or otherwise making available;
- Blocking, deletion/erasure or destruction of the information or data, also
- The Trust advocates the method of remembering the definition of "Processing" by using the acronym HORUS – Holding, Obtaining, Recording, Using and Sharing.

The Trust has identified its legal basis for processing personal data under the GDPR / Data Protection Act 2018 as;

Type of data	Patients/Customers	Staff
Personal Data (Article 6)	Processing is necessary for the performance of a task carried out in the public interest or in the exercise of the official authority vested in the controller (Article 6(e)).	Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract of employment (Article 6(b)).
Special Category Data (Article 9)	We will use your information to provide preventive medicine, medical diagnosis, the provision of health care/treatment (Article 9(h)).	We will use your information for preventive or occupational medicine, for the assessment of the working capacity of the employee (Article 9(h)).

In line with Caldicott 2 recommendations, information will only be shared for the purposes of direct care with registered and regulated health care professionals who have a legitimate relationship with the patient.

5 FAIR AND LAWFUL PROCESSING

Before collecting, storing or otherwise processing personal data, the Trust will:

- Identify the purposes for which the data will be processed, and ensure that any new purposes are compatible with those for which the data were originally collected.
- Identify a valid lawful basis for processing from the GDPR Article 6 and Article 9 for special category data (as above).
- Determine whether the processing would be fair to the data subjects, and in so doing take account of the reasonable expectations of individuals.
- The senior member of staff directing any new collection or use of personal data is responsible for ensuring it is fair and lawful, and that these requirements of the GDPR are identified and met.
- All processing activities should be regularly reviewed, and must be ceased when the purpose, fairness or condition for processing are no longer met.

Purposes for processing are outlined below:

5.1 **Healthcare purpose.** Any purpose which directly contributes to the safe health and social care of an individual patient, including care, diagnosis, referral and treatment processes

together with relevant supporting administrative processes, such as clinical letters and patient administration, patient management on a ward, and managing appointments for care. This may also be known as "**direct care**". It includes clinical audit only where conducted by the care team for the purpose of assurance of the quality of care provided to individual patients.

5.2 **Non-healthcare medical purpose.** Any medical purpose which does not directly contribute to the safe care of a specific patient, but rather to the overall provision of services to a population or group of patients. This may also be known as "**indirect care**". Non-healthcare medical purposes include medical research, health service management, preventative medicine, financial audit, and risk stratification.

Patient data may be used for non-healthcare medical purposes by the care team which provided care to the patient, provided that patients have been informed, given an opportunity to opt out, and have not opted out. Most clinical audit falls into this category.

Disclosure of confidential data outside the care team will require a specific lawful basis under Article 6 and Article 9 of the GDPR.

5.3 **Non-medical purpose.** Use of patient data for non-medical purposes will require a lawful basis for processing from Article 6 and Article 9 or with the explicit consent of the patient.

5.4 **Individuals Rights.** The Trust will provide comprehensive information to all data subjects about the uses of their personal data, in order to ensure that such usage is fair and transparent. This shall include:

Written material such as patient leaflets, posters, and the Trust website.

Active communication with patients, which shall be **an individual responsibility of all staff with direct patient contact**, ensuring that all patients:

- Are aware of how their data may be used or disclosed.
- Are aware of their rights to make decisions and choices in regard of such uses, and to have such decisions respected by the Trust.
- Understand the information made available to them, and have the opportunity to ask questions.
- Prompt, open and honest answers to all queries about the use of data, referring to specialist staff where appropriate.
- Departments directing the use of data for specific purposes are responsible for producing and distributing appropriate fair processing information about those purposes.

5.5 **Consent.** Defined in the GDPR Article 4 (11) as being "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

In general, the Trust shall not seek the consent of data subjects where another condition for processing provides a more robust lawful basis.

The Trust shall endeavour to build a relationship of mutual understanding with all data subjects by informing them fully about the uses of their personal data, and by ensuring that

all such uses are fair and reasonable.

Consent is not an all-encompassing justification for processing personal data, and does not obviate the Trust's obligations with regard to the fairness, necessity and proportionality of data processing. For the avoidance of doubt, processing data may not be lawful even where consent has been given.

Seeking consent only when required will ensure that it is used in the appropriate lawful context. Consent must not be sought unnecessarily, nor where there is no real choice.

When seeking consent from patients, staff should also refer to the Trust's Consent Policy and relevant professional guidance.[15,16]

5.6 **Capacity.** Where adult patients lack capacity to consent, decisions should be made in line with appropriate professional guidance and the Trust's Mental Capacity Policy.

5.7 **Children.** Any person aged 13 and over is presumed to be competent to give consent, unless there is reason to believe otherwise in the particular circumstances. Below that age, parents/guardians may only exercise the child's rights on their behalf until such time as the child acquires *"sufficient understanding and intelligence to enable him or her to understand fully what is proposed"* (Gillick competence).

Children aged under 12 may be presumed to lack sufficient understanding and intelligence.[17]

Clinical staff should make a decision of competence for each individual child between the ages of 12 and 15.

Non-clinical staff are to seek advice where required, but should normally consider independent consent from children aged 12 and over.[18]

Whenever any person aged under 18 is determined to be competent, the parents/guardians should nonetheless be kept involved in decisions where possible, but only to the extent that this is compatible with the rights and wishes of the child.

5.8 **Objections.** Consent may be given or withdrawn at any time. Where consent is relied upon as the condition for processing, and it is then withdrawn, the Trust must cease processing.

5.9 **NHS National Data Opt out**. The national data opt-out enables patients to opt out from the use of their data for research or planning purposes, in line with the recommendations of the National Data Guardian in her Review of Data Security, Consent and Opt-Outs.

Patients who object to their information being used for any purpose other than their own direct care must register with the National Data Opt-Out. Patients can view or change their national data opt-out choice at any time with the service. [19]

The use of any patient data for any non-healthcare purpose which is not also a legal requirement for the Trust, must take account of the National Data Opt-Out.

---

[16] NMC "Professional standards of practice and behaviour for nurses and midwives" – Mar 2015; http://www.nmc.org.uk/standards/code/
[17] Based on legally prescribed age of competence in Scotland; there is no fixed equivalent in English law.
[18] ICO 'what rights do children have?" - https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr/what-rights-do-children-have/
[19] National Data Opt-Out - https://digital.nhs.uk/services/national-data-opt-out-programme

The Trust will ensure that where patients have exercised their rights to "opt out" of their information being used for secondary purposes, this will be respected.

5.10 **Data Protection Impact Assessments (DPIA)**

A data protection impact assessment must be conducted on all new information asset projects. This will enable us to identify if the project collects new data, processes data for a new purpose, or processes data. The DPIA will enable us to identify and address any potential privacy issues.

The senior member of staff directing any new project or information asset is responsible for ensuring a DPIA is completed as part of the business planning process, in accordance with the guidance provided by the Information Commissioner.[20]

The Data Protection Officer (DPO) must be consulted to ensure that data protection principles are integrated into the new processing to protect the privacy rights of data subjects.

6 DATA PROTECTION PRINCIPLES

The Act stipulates that any organisation processing personal data must comply with 6 principles of good practice. The principles are legally enforceable. The Trust and its staff will take all necessary measures to ensure that personal data is:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date.
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

6.1 Data retention

NHS retention schedules[21] shall be used to determine the minimum retention periods for data. Data exceeding the minimum retention period must be either:

- Retained for a specified further period of time where there is a justifiable need to do so, which decision is to be made by an appropriately senior manager having regard to the individual rights and freedoms of data subjects, and such decision documented and noted in all relevant record systems. Retention may not, in any circumstance not specifically allowed for by legislation, exceed the time at which the data is considered a

[20] Information Commissioner's Office DPIAs- https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

[21] Records Management Code of Practice for Health & Social Care 2016: https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/records-management-code-of-practice-for-health-and-social-care-2016

'historical record'.22

- Transferred to an approved Place of Deposit, if likely to have historical or research value.

- Destroyed securely, in accordance with current Trust standards.

- Information Asset Owners are responsible for implementing these information standards in regard of the information within their asset, regardless of whether it is held in electronic or paper format.

7 DATA SUBJECT ACCESS RIGHTS

Requests for access to personal or confidential data may be made under:

- DPA18 section 45, which provides data subjects with the right to a copy of all personal data related to them which are held by the Trust ("right of access by the data subject").

- The Access to Health Records Act 1990, which provides access to the records of a deceased person by their personal representative, and which requests shall normally be handled by the Trust as if they were subject access requests.

The Trust will complete all subject access requests within the legal deadline of one month, and will endeavour to meet the recommended response time of 21 calendar days as far as is reasonably practicable. The time limit begins the day after the request is received and (working day or not) until the corresponding calendar date in the next month.

The Trust will treat all subject access requests equally and without prejudice.

The Trust will, as far as practicable and in accordance with current Trust policy, maintain information in a readily accessible state by maintaining and adhering to proper filing techniques, allowing information to be collated quickly and efficiently.

Subject access and equivalent requests shall be managed through Information Governance Standard Operating Procedure No. 3, "Subject Access Requests".

All staff are responsible for fulfilling subject access requests relevant to their specialty, area or department, in accordance with the above procedure.

The Information Governance Steering Group monitors all patient subject access requests to ensure that they are compiled within the defined timescales in the Data Protection Act 2018.

Where staff wish to make a request for a copy of the information held about them by the Trust, this must be sent to the HR Department to be processed.

8 INFORMATION SECURITY

All persons employed by the Trust, or otherwise carrying out work for or on behalf of the Trust, are to be subject to confidentiality agreements, which are to be contractually binding wherever possible.

[22] Public Records Act - https://www.nationalarchives.gov.uk/archives-sector/our-archives-sector-role/legislation/20-year-rule-and-records-of-local-interest/

An honorary contract does not provide a lawful basis for access to information.[23]

Individuals engaged in an honorary capacity to provide direct care may (like other care staff) infer patient consent to access information for the purpose of that direct care. Disclosures to individuals for audit or research purposes must have a lawful basis, as described in section 4 of this policy.

8.1 **Data processors.** Persons or organisations processing data on behalf of the Trust are to be selected, contracted and held to account in accordance with section 11 of this policy.

8.2 **User Access.** The process and controls for registering users on Trust information systems are detailed in Information Governance Standard Operating Procedure No. 4, "User Access Management", and in asset-specific documentation as may be published by Information Asset Owners in accordance with the Information Security Policy.

8.3 **Information handling.** All personal data held and processed by or on behalf of the Trust are to be managed in accordance with the Information Security Policy, and handled in such a way as to maintain the privacy and confidentiality of data subjects. This includes, but is not limited to:

- Secure storage, transport and tracking of physical records.
- Ensuring that Trust records remain under Trust control at all times and that, where lawful disclosure occurs, a copy of the relevant information is produced and disclosed.
- Appropriate access control and other security measures on electronic records, which are to be held and processed only on authorised Trust systems.
- Care when verbally discussing patients or staff.
- Verifying the identity and authorisation of persons to whom personal or confidential data are to be disclosed.
- Prompt reporting and action in regard to data breaches.

9 OVERSEAS TRANSFER

The Trust will, as far as is reasonably practicable, store and process personal data only within the UK.

9.1 **Transfers within EEA.** Transfers of personal data to or via any country outside the UK, but within the European Economic Area (EEA), should be notified to the Information Governance Manager. The UK government has stated that, on the UK's exit from the EU, transfers of data from the UK to the EEA will be permitted but this will be reviewed in due course.

9.2 **Transfers outside EEA.** Transfers of personal data to or via any country outside the EEA are considered a "restricted transfer". However, according to the GDPR, a restricted transfer can be made if it is covered by an adequacy decision, an appropriate safeguard or an exception.

The senior member of staff directing the transfer is responsible for ensuring a written

[23] National Institute for Health Research - https://www.myresearchproject.org.uk/help/hlphrgoodpractice.aspx

assessment of GDPR compliance, in accordance with ICO guidance,[24] is made and recorded.

The assessment should be approved by the senior person responsible for directing the use of the information.

A copy of the approved assessment is to be lodged with the Information Governance Manager.

Exceptionally, where an individual has given explicit consent to the transfer of their own personal data outside the EEA, after having been fully informed on the information security and data protection risks so incurred, the transfer may proceed without further assessment of GDPR. Consent is to be obtained as detailed within this policy.

10 DISCLOSURES & DATA SHARING (DATA CONTROLLERS)

A disclosure is defined by this policy as *"any release of personal or confidential data to any person or organisation, other than the data subject or a data processor, for the recipient to use for their own purposes."* This includes other health and social care organisations, public bodies, and **any person not employed by or under substantive contract to the Trust**.

Each disclosure must meet the six data protection principles of DPA18, as set out in section 4 of this policy, and (where relevant) the common law duty of confidence.

In practice, the common law duty provides a higher bar to disclosure than DPA18 and will typically define whether a disclosure can occur. Common scenarios are detailed in this section.

Compliance with the law is the responsibility of the person making the decision whether to disclose or to withhold, which should normally be the most senior member of staff available at the time.

10.1 **Statute.** Some organisations have statutory powers relating to the disclosure of personal data. In the majority of cases, such powers *allow* disclosure but do not *compel* it, and all requests are to be assessed in the particular circumstances against the common law, DPA18, and the individual rights and freedoms of the data subject.

10.2 **Court orders.** The Trust will comply with all court orders. Any member of staff receiving a court order is promptly to fulfil it or ensure it is passed to the appropriate person.

10.3 **Other legal obligations.** Certain information must be disclosed by law, such as (for example) notification of abortions, notifiable diseases, and obligations imposed by DHSC under HSCA12.

Nothing in this or any other policy shall prevent Trust staff from complying with their individual obligations to disclose information to appropriate agencies when required by law, provided that adequate authority is obtained and recorded.

However, the personal data disclosed must be the minimum necessary to meet the legal obligation, and data subjects must be informed unless inappropriate in the particular circumstances.

[24] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/

10.4 **Law enforcement.** This type of processing is subject to the rules in Part 3 of the DPA 2018. Part 3 only applies to competent authorities processing for law enforcement purposes. So, it applies, but is not limited, to:
•the police, criminal courts, prisons, non-policing law enforcement; and
•any other body that has statutory functions to exercise public authority or public powers for any of the law enforcement purposes.

Police forces and other agencies have no general right of access to health records. All requests should be challenged to identify the specific lawful basis.

Requests from police and coroners in relation to crime, taxation and deaths will be assessed against the specific legislative powers named by the agency in the particular case.[25]

Requests for confidential information relating to deceased patients shall be assessed against the common law duty of confidence, with disclosure only in the substantial public interest.

10.5 **Regulatory bodies.** Requests from professional regulatory bodies will be assessed under the particular body's statutory powers.[26]

10.6 **Section 251 support.** Disclosures relying on Section 251 should be referenced against a specific, in-date approval decision published by the Health Research Authority,[27] and must comply with DPA18 in all other regards.

10.7 **Explicit consent. Consent must be in accordance with the principles set out in this policy, ie. must normally be given explicitly for the specific disclosure. For Special category data, such as health records,** consent may be inferred only when disclosure is necessary for the patient's direct care**.**

For the avoidance of doubt, information can and should be shared with other health and social care professionals when necessary for direct patient care.

Controls for lawful disclosures are listed below.

10.8 **Data sharing agreements.** Regular or routine disclosures of personal data to other data controllers are to be supported by data sharing agreements in accordance with the ICO code of practice.[28] Where the recipient is not a public body, the agreement should be contractual.

The senior member of staff directing the disclosure is responsible for the data sharing agreement.

---

[25] ico "Guide to Law Enforcement Processing": https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/scope-and-key-definitions/
[26] See 'Disclosures to regulatory bodies'; http://trustnet/departments/infogov/guidance.html and See 'Disclosures to police & coroners'; http://trustnet/departments/infogov/guidance.html
[27] NHS Health Research Authority "CAG Advice and HRA/SofS Approval Decisions"; http://www.hra.nhs.uk/about-the-hra/our-committees/section-251/cag-advice-and-approval-decisions/
[28] ICO "Data sharing code of practice" – https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/ico-call-for-views-on-updating-the-data-sharing-code-of-practice/; http://www.ico.org.uk/for_organisations/data_protection/topic_guides/data_sharing

Copies of all data sharing agreements are to be lodged with the Information Governance Manager.

Data sharing agreements should include:

- The lawful basis for disclosure and use.
- The permitted purposes and manners in which the data are to be processed, including the terms of any permitted onward sharing, and including the terms of any permitted linkage to other data.
- Arrangements for data destruction.
- Requirements to ensure the reliability and training of staff authorised to access the data.
- A requirement for the receiving party to have regard to the NHS Digital's 'Code of practice on confidential information'.[29]
- Provision for audit of compliance to the agreement, and penalties for failure to comply.

10.11 **Information security.** All information disclosures must be conducted securely, in accordance with the Information Security Policy and current Trust standards and guidance. Where paper records are disclosed, the Trust is to retain possession of all original records and disclose only copies, as far as lawfully allowed in the circumstances.

10.12 **Recording.** All disclosures to other data controllers should be recorded, and the lawful basis documented.

11 SUPPLIERS (DATA PROCESSORS)

Organisations and individuals processing personal data on behalf of the Trust (data processors) may only do so under a contract, made or evidenced in writing, between the Trust and the data processor.

The Trust as data controller, must exercise control over the processing and carry data protection responsibility for it.

The Trust's contract signatory is responsible for ensuring compliance with DPA18 and this policy.

11.1 Contractual requirements

The contract must, as a legal minimum, require the data processor:

- Only to process the personal data in accordance with instructions given by the Trust.
- To put in place appropriate technical and organisational security measures to protect the data, so as to meet obligations equivalent to those imposed on the Trust as data controller under DPA18.

The contract should also:[30]

[29] NHS Digital Code of Practice on confidential information - https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/code-of-practice-on-confidential-information

[30] See also DSP Toolkit requirement 10.

- Indemnify the Trust without limitation against any action or inaction of the data processor in respect of unlawful or unauthorised processing of personal data.

- Provide the Trust with power of audit and inspection of the technical and organisational security measures applied to the processing of the personal data.

- Require the data processor not to transfer personal data outside the European Economic Area without the prior consent of the Trust.

- Require the data processor to ensure the reliability and adequate training of its staff.

- Require the data processor to report data breaches and other incidents and security events to the Trust.

- Define how the data processor should deal with subject access requests.

- Where subcontracting is permitted, require the data processor to procure that any subcontractors of the data processor comply with the same obligations.

- The use of national standard NHS terms & conditions,[31] as may be updated from time to time, is strongly recommended and shall be taken as satisfying the requirements of this policy. Advice should be sought from Procurement before using any other terms.

11.2 **Assurance**

Where the Trust engages with another company to undertake services, and the company will be processing the Trust's personal or special category data, the Trust will ensure that it has put in place a data processing agreement with the company/supplier. This agreement will outline the data protection responsibilities of both The Trust and the company/supplier.

Data processors should be selected with due regard to the guarantees provided in respect of the technical and organisational security measures governing the processing of Trust personal data.

In accordance with DH policy, all data processors should complete and publish an annual Data Security & Protection Toolkit assessment, and achieve a minimum of 'Standards Met' in all elements.

In exceptional cases, the Trust's Senior Information Risk Owner may accept alternative assurances to meet DPA18.

Data processors are to be monitored regularly for compliance with contractual requirements in regard of Trust personal data, such as by regular reports or inspections.

12 ANONYMISATION

Anonymisation is the process of rendering data non-identifiable, such that they no longer fall within the DPA18 definition of personal data.

In accordance with the law[32] and NHS guidance[33]:

[31] https://www.gov.uk/government/publications/nhs-standard-terms-and-conditions-of-contract-for-the-purchase-of-goods-and-supply-of-services
[32] DPA18 Principle 3 (*"Personal data shall be … not excessive"*).
[33] Caldicott Principles 2 (*"Don't use personal confidential data unless it is absolutely necessary"*)

Data shall always be anonymised to the fullest extent possible under the circumstances and the purpose for which they are processed.

Fully anonymised data cease to be personal data, and may be handled accordingly.

ISB1523: Anonymisation Standard for Publishing Health and Social Care Data: this is the process standard for publishing health and social care data which provides an agreed and standardised approach to anonymisation[34]. It shall be adopted as the basis for anonymisation processes within the Trust.

The senior staff member directing each use of data is responsible for ensuring appropriate anonymisation for that use.

Accessing personal data in order to anonymise the data is, in itself, a non-healthcare medical purpose, and must be done only by the care team which provided care to the patient (or under another lawful basis).

12.1 **'Motivated intruder' test & risk assessment**
Data are fully anonymised when a competent and motivated intruder could not identify any individual, taking into account all means likely reasonably to be used and any other data in the possession of (or likely to come into the possession of) that intruder.

Data may be personal data when held by one organisation, and not personal data when held by a second organisation, due to additional data which may be in the possession of either.

Before releasing data to any other person or organisation, the Trust shall consider the likelihood of other data being in the possession of the receiving party which may be used in conjunction with the released data to identify individuals, and thereby determine whether the data are adequately anonymised. If not, a lawful basis for the release of the data is required.

Even where data are fully anonymised, the risk of *misidentification* of data subjects should be assessed before disclosure occurs.

12.2 **De-identified data for limited disclosure**
In some cases, full anonymisation may be impossible or impractical to achieve without damaging the purpose for which the data are processed. Data may be partially anonymised (also known as "de-identified") for limited disclosure or limited access, but **such data still constitute personal data**, and all uses must therefore be supported by a lawful basis and adequate safeguards against further use or disclosure of the data – as detailed in the *'Controls for lawful disclosures'* section of this policy.

12.3 **Pseudonymisation.** Pseudonymisation is a particular type of partial anonymisation, where information is attributable to an individual, but that individual is not identifiable except by means of a pseudonym (eg. "Person A"). This may be used alongside or instead of other anonymisation measures, as may be appropriate in the particular circumstances and the purpose for which the data are processed.

[34] ISB1523: Anonymisation Standard for Publishing Health and Social Care Data: https://digital.nhs.uk/data-and-information/information-standards/information-standards-and-data-collections-including-extractions/publications-and-notifications/standards-and-collections/isb1523-anonymisation-standard-for-publishing-health-and-social-care-data

The preferred method of pseudonymisation is by means of a cryptographically-secure hashing algorithm, having due regard to current NHS good practice guidance, using a unique salt for each input value.

Where it is not practicable to use such an algorithm, an alternative method should be determined in accordance with current standards and codes of practice, in order to produce a dataset with an acceptably low residual risk of identification in the particular circumstances.

Pseudonymised data will still constitute personal data. All uses must be supported by a lawful basis compliant with DPA18, and adequate safeguards against further use.

13 AUDIT, RESEARCH AND SURVEYS (NON-HEALTHCARE MEDICAL PURPOSES)

As described in sections 4 and 5 of this policy, all uses of data for non-healthcare medical purposes must have a lawful basis to meet DPA18 and additionally, where data will be disclosed outside the care team which provided care to the patient, the common law duty of confidence.

The senior member of staff directing the use of data for any non-healthcare medical purpose is responsible for ensuring compliance with the law, including in particular (but not limited to):

Providing and distributing adequate information to patients before their data is used.

Meeting the specific requirements described in this section for typical use cases.

13.1 **Clinical audit.** In accordance with NHS and professional guidance:

13.2 **Local audit.** Local clinical audit, involving only those healthcare practitioners who provided care to the patient, or other Trust audit staff directly supporting them, may use personal data without explicit consent provided that patients have been fully informed that their data may be used for clinical audit, have been given an opportunity to opt out, and have not opted out.

13.3 **Non-local audit.** Non-local audit such as national audits will rely on the commissioning organisation having obtained the requisite permissions to request the data. Audits performed by auditors from other organisations will need to demonstrate to the Trust that they have the requisite permissions in place to view data where it is patient identifiable – such as external audit. Managers should take all reasonable steps to ensure that no information is released (or accessed) where these criteria are not assured as being met.

13.4 **Medical research.** The use of any identifiable NHS data for medical research requires explicit patient consent and ethical approval.

Ethical approval must be given by an authorised Research and Ethics Committee within the Research Ethics Service.

The lawful basis should be explicit consent, or Section 251 approval if consent is not practicable.

The Trust Research & Development Committee shall oversee all uses of Trust data for research purposes.

13.5 **National audits, collections and surveys.** National initiatives will normally rely on a legal obligation created for the purpose, or Section 251 approval, or explicit consent. Prior to disclosure, the particular lawful basis should be identified and recorded as part of departmental data flow mapping, and fair processing information provided to patients.

13.6 **Local initiatives.** The senior member of staff directing any new collection or use of data for a non-healthcare medical purpose is responsible for ensuring compliance with the law. A Data Protection Impact Assessment should be completed in the first instance.

14 POLICY MANAGEMENT

14.1 **Publication.** This policy will be published on the Trust website and intranet.

14.2 **Review.** This policy will be reviewed every three years, or more frequently as may be required.

14.3 **Archiving.** This is a Trust-wide policy. Current and archive versions will be managed in accordance with current Trust processes.

Enclosure to
Confidentiality & Data Protection Policy

EQUALITY IMPACT ASSESSMENT SUMMARY

Background

- *Description of the aims of the policy*
- *Context in which the policy operates*
- *Who was involved in the Equality Impact Assessment*

Policy describes aim and context.
Policy author conducted equality assessment.

Methodology

- *A brief account of how the likely effects of the policy was assessed (to include race and ethnic origin, disability, gender, culture, religion or belief, sexual orientation, age)*
- *The data sources and any other information used*
- *The consultation that was carried out (who, why and how?)*

Conducted by policy author by means of the template provided in the "Policies Procedures and Guidelines: Writing and Ratification" policy dated Dec 2010.

Key Findings

- *Describe the results of the assessment*
- *Identify if there is adverse or a potentially adverse impacts for any equalities groups*

No discrimination.

Conclusion

- *Provide a summary of the overall conclusions*

No discrimination.

Recommendations

- *State recommended changes to the proposed policy as a result of the impact assessment*
- *Where it has not been possible to amend the policy, provide the detail of any actions that have been identified*
- *Describe the plans for reviewing the assessment*

N/A