Imperial College Healthcare NHS
NHS Trust

Trust-Wide Policy	
Version:	V6.1
Policy Category:	Information Governance & Technology
Target Audience:	All Trust Staff
Review Date:	**22/08/2026**

Data Protection, Confidentiality and Information Sharing Policy

1. Introduction

1.1. As defined in the Data Protection Act 2018 (herein 'DPA') health information constitutes special category data which requires a higher level of protection due to its particularly sensitive nature. Patients have the legitimate expectation that Trust staff will respect their privacy and act appropriately. It is crucial that the Trust provides a confidential service to meet legal requirements and retain the confidence of patients and the public.

1.2. The Trust is registered with the Information Commissioner's Office (ICO). As a registered data controller, the Trust has a legal duty of confidentiality and an obligation to share, where necessary, personal information lawfully.

2. Data Protection Principles

2.1. The Trust must comply with the legal framework for the protection of personal and confidential information.

2.2. The UK General Data Protection Regulation ('UK GDPR') identifies seven **Data Protection Principles** that set out standards for information handling and personal data use. Data should be:

1. Processed fairly, lawfully, and transparently,
2. Collected for specified, explicit, and legitimate purposes, and not processed in a manner incompatible with those purposes,
3. Adequate, relevant, and limited to what is necessary,
4. Accurate and kept up to date,
5. Not kept for longer than is necessary,
6. Processed in a manner that ensures appropriate security, integrity, and confidentiality,
7. Processed in an accountable manner where data controllers take responsibility for their treatment of personal data and how they comply with the other principles.

2.3. **Personal identifiable data** is any data that can be used to directly or indirectly identify a specific individual.

2.4. Examples of personal identifiable data include but are not limited to;

- Name, address, full post code, date of birth,
- NHS number and local hospital numbers,
- Email address, phone numbers (mobile and/or landline) attributed to an individual,
- Photographs, videos, audio-tapes or other images of patients,
- Audio tapes or recordings of patients,
- Anything else that may be used to identify a patient directly or indirectly (e.g.: rare diseases, drug treatments or statistical analyses which have very small numbers within a small population may allow individuals to be identified).

2.5. Sensitive information is defined under Article 9 UK-GDPR as including any data revealing:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- Trade Union Membership;

Or any processing of:

- Genetic data;
- Biometric data for the purpose of uniquely identifying a natural person;
- Data concerning health;

- Data concerning sex life or sexual orientation.

2.6. Processing of special category data requires a lawful basis under both Article 6 and Article 9 UK GDPR (see section 5 below).

3. Common Law Duty of Confidentiality

3.1. Much of the personal identifiable data collected by the Trust is categorised as personal confidential data. This is any personal data over which a duty of confidence is owed from one party to another. The most common example is the duty of confidence which medical staff owe to their patients with regards to confidential health data, though this also includes certain staff information including occupational health and finance data.

3.2. The Common Law Duty of Confidentiality is a legal obligation distinct from, and in addition to, the obligations contained in the UK GDPR. This fundamental requirement, established via the British courts and referenced in professional codes of conduct, is also included within Trust employment contracts as a specific requirement sanctioned by disciplinary procedures.

3.3. The Duty of Confidentiality may be further extended via supplementary contractual arrangements. The Trust has two mechanisms in place: the **Honorary Contract** and the **Approved Associates process** designed to ensure that the duty can be enforced. Further information on the Approved Associates process can be found on the Trust Intranet. Advice on Honorary Contracts may be sought via the Human Resources Employee Relations Advisory Service.

3.4. In some circumstances, namely research, there is an alternative arrangement known as 'license to attend'. More information about license to attend can be obtained from the Joint Research Office / Joint Research Compliance Office. In any case, the duty of confidence will extend to such persons.

4. Caldicott principles (revised in light of Caldicott 2 and Caldicott 3)

4.1. All processing must also be in accordance the Caldicott Principles as set out below.

i. Justify the purpose(s) for using personal confidential data,
ii. Don't use personal confidential data unless it is absolutely necessary,
iii. Use the minimum necessary personal confidential data,
iv. Access to personal confidential data should be on a strict need-to-know basis,
v. Everyone with access to personal confidential data should be aware of their responsibilities,
vi. Comply with the law,
vii. The duty to share information can be as important as the duty to protect patient confidentiality,
viii. Inform patients and service users about how their confidential information is used.

5. Lawful Basis

5.1. The main purpose of patients' health records is to support the provision of healthcare. Information that can identify individual patients must not be used or disclosed without the individual's explicit consent or another legal basis as per **Articles 6 and 9** UK GDPR.

5.2. Implicit Consent and Direct Care

5.2.1. The Common Law Duty of Confidentiality also requires there to be a lawful basis for the use or disclosure of personal information held in confidence, such as:

- Valid informed consent
- Overriding public interest

- Statutory basis or legal duty to disclose.

Please note that the requirements under the Common Law Duty of Confidentiality and under the UK GDPR may differ.

5.2.2. Informed consent under the Common Law Duty of Confidentiality refers to reasonable and expected use of data, which includes the disclosure or sharing of health data with other healthcare providers for direct care. Indeed, the Health and Social Care (Safety and Quality) Act 2015 sets out the duty on healthcare providers to share information for a direct care purpose in this way.

5.2.3. Patients have the right to prohibit the use and disclosure of confidential information that identifies them, restrictions that can extend to other health professionals. Such an objection or prohibition may, by its nature, limit the care that can be offered by the Trust. Patients must be informed if their decisions about disclosure have implications for the provision of care or treatment.

5.2.4. If a patient objects to the sharing of any or all of their information, it must be highlighted that this may lead to the Trust not being able to provide the care required or potentially reducing the effectiveness of the care provided. Concerns raised by the patient on how the Trust utilises their information and the discussions regarding this should be recorded in the patient record. This is an on-going process. Consent to share in one instance is not the same as consent to share in all future instances and this should be revisited over time with the patient as appropriate.

5.3. Non-Direct Care Use of Personal Confidential Information

5.3.1. Non-direct care use of personal confidential information is the use of confidential information for purposes not directly concerned with providing direct care to the patient. Examples include, but are not limited to: administration, planning, audit, commissioning, payment by results, clinical research and education.

5.3.2. Personal confidential information may be accessed or disclosed for non-direct care uses, outside of the scope of informed consent under the Common Law Duty of Confidentiality, in the following circumstances:

- The patient has given explicit **consent**,
- There is a Confidentiality Advisory Group (**CAG**) authorised Section 251 exemption allowing disclosure of personal confidential information,
- The data is sufficiently de-identified to ensure that there is no breach of confidence to the patient.

Under the UK GDPR, personal data may be accessed or disclosed when:

- Disclosure is required by **a legal obligation (Article 6)**,
- Disclosure is necessary in a vested public authority's performance of a public task in the **public interest (Article 6)**,
- **Explicit consent** is given (**Article 9**),
- Processing is necessary for the purposes of preventive or occupational **medicine**, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services (**Article 9**),
- Processing is necessary for reasons of public interest in the area of **public health** (**Article 9**),
- Processing is necessary for **scientific research** purposes (**Article 9**).

5.3.3. Even where one of the above circumstances arises, all efforts should be taken to minimise the scope of confidential data to be disclosed, to ensure data is disclosed for a specific purpose and to implement the appropriate technical and organisational controls prior to the transfer being undertaken.

5.3.4. The Trust is accountable for any decisions made to pass on information to another agency or individual. Operationally, information disclosure decisions will be made by the clinical professional responsible for an individual's assessment, care or treatment or on the advice of a senior professional within the Trust, which may include the Caldicott Guardian.

5.3.5. Under the **National Data Opt Out**, patients have the right to opt out of the use of personal identifiable data for non-direct care purposes. Any proposals to use personal identifiable data for any purpose beyond direct care must be undertaken in compliance with the requirements of the National Data Opt Out.

5.3.6. Compliance with the National Data Opt Out is a requirement for all health and social care as of 31 July 2022. The Trust is implementing the National Data Opt Out technical solution within the ICT infrastructure, and the Data Protection Office may support any advice requests in regard to the applicability of the National Data Opt Out to any instance of data sharing.

5.4. Explicit Consent

5.4.1. Explicit consent must be obtained from the patient for any purpose where no other legal basis for disclosure of personal confidential information can be identified. In particular, explicit consent must be obtained and recorded before any disclosures to insurance companies, employers or organisations responsible for the assessment of benefit entitlements.

5.4.2. Patients should be encouraged to make disclosures considered necessary for their own protection. An example may be making contact with agencies that provide support to victims of domestic violence. A competent adult patient may refuse to consent to such a disclosure, even if this leaves them at risk of serious harm.

5.4.3. A data subject consents to processing if they clearly indicate their agreement either by a statement or a positive action. Silence, pre-ticked boxes or inactivity do not qualify as a valid consent under the UK GDPR.

5.5. Disclosures Required by Statute

5.5.1. Health professionals are required by law to disclose certain information with or without patient consent. The disclosure should consist of the minimum requirement of information for the purposes of disclosure. Although the patient has no right to refuse statutory disclosure, ideally they should be made aware of the disclosure and given assurance of the security of the disclosure to the relevant secure authority. Disclosure by statute also includes the legal provisions which provide for regulatory bodies to access Trust information.

Legislation	Disclosure	Recipient
Public Health (Control of Disease) Act 1984 and Public Health (Infectious Diseases) Regulations 1988	Identity, sex and address of any person suspected of having a notifiable disease including food poisoning	Local Authority

Abortion Regulations 1991	Reference number, date of birth and postcode of woman following termination of pregnancy	Chief Medical Officer
Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013	Deaths, major injuries, dangerous occurrences and accidents resulting in more than three lost working days, and certain diseases	Relevant enforcing authority
Road Traffic Act 1988	Information that may identify a driver alleged to have committed an offence	Police
The Prevention of Terrorism Act 2005	Any information that may prevent an act of terrorism or help to apprehend or prosecute a terrorist	Police
Information Sharing Index Regulations 2006	Provision of basic identifying information for every child up to the age of 18	Local Authority

Please note this is not an exhaustive list and other legislation applies in specific circumstances. If you have any doubt, please refer to the Information Governance team.

5.6. Requests for Disclosure Made by the Police

5.6.1. Requests from the police should be made via a formal Form 3022. These are to be forwarded to the Health Records Manager to process the request. If there is any uncertainty as regarding disclosure, these matters should be referred to the Data Protection Office.

5.6.2. Requests from the police for Closed Circuit Television (CCTV) and or Body Worn Camera (BWC) footage shall be processed in accordance with the Trust's CCTV and BWC Policy.

5.7. Court Orders

5.7.1. The courts have legal powers to require the disclosure of information. This does not require the consent of the patient, whose records are to be disclosed. Court orders must be followed precisely and in accordance with their instructions.

5.7.2. In circumstances where a court order is not clear or giving a direction that cannot be followed a variation may be sought. Any concerns with a court order or where a variation is required should be referred immediately to the Trust's Legal department.

5.8. Public Interest

Disclosures to a competent public authority may be necessary to prevent serious crime or risk of serious harm. The Trust might use the public task basis if it is performing a task in the public interest or for its official functions, including for public security and public health.

6. Disclosures relating to Genetic Information

Genetic information relating to one patient may also be patient information about blood relatives. Most patients will readily share information with relatives relating to genetics that may assist those relatives with actual or potential health problems. In cases where a patient may refuse to consent to disclosure about their genetic condition to a blood relative, advice should be sought from the Caldicott Guardian to determine what the next steps should be on a case by case basis.

7. Ability to Consent to Disclosures of Information

7.1. Seeking consent of patients may be difficult due to illness, disability or circumstances that may prevent understanding about the likely uses of patient information. The Mental Capacity Act 2005 protects people who lose the capacity to make their own decisions. The Act allows the person, while they still have capacity, to appoint someone (for example a trusted relative or friend) to make decisions on their behalf, in their best interests, for their health and personal welfare and not just about financial matters, once the patient has lost the ability to do so. The Mental Capacity Act 2005 introduces a Code of Practice for healthcare workers who support people who have lost the capacity to make their own decisions.

7.2. Staff should refer to this guidance when making decisions about access to information of patients who lack capacity to decide. Guidance on the use of the Mental Capacity Act Code of Practice is available via the web.

8. Multi Agency Public Protection Agreements (MAPPA)

The aim of a Multi-Agency Public Protection Arrangement (MAPPA) is to draft and co-ordinate a risk management plan for the most serious offenders based on the information, skills and resources provided by individual agencies. Three groups of people who might be referred to MAPPA are: registered sex offenders, all violent and non-registered sex offenders sentenced to 12 months or more in prison (This also includes patients on hospital orders) and any other offender posing a risk of serious harm. The Criminal Justice Act 2003 places a duty on NHS organisations to co-operate with MAPPA. Further information on MAPPA can be found at the Ministry of Justice website.

9. Statutory Restrictions on Disclosure

9.1. Gender Recognition Act 2004

This act makes it an offence to disclose information about a person's application to the Gender Recognition Panel and the person's gender history after that person has changed gender under the Act.

9.2. NHS Venereal Diseases Regulations (1974) and NHS Trust and PCTs (Sexually Transmitted Diseases) Directions 2000

This requires that any information capable of identifying an individual treated for a sexually transmitted disease (including HIV), shall not be disclosed other than to a medical practitioner in connection with treatment of the patient or the prevention of spreading the disease. In highly exceptional circumstances, for example where a patient with a sexually transmitted infection refuses to advise an ongoing sexual partner of their condition and refuses to modify their behaviour, then it may be appropriate to breach confidentiality and advise the contact. This is a highly exceptional circumstance and advice should be sought from the Caldicott Guardian before proceeding.

9.3. Fertilisation and Embryology Act 1990

Disclosure of information that identifies a patient undergoing treatment relating for fertilisation or embryology to another party without the patient's consent is a criminal offence.

9.4. Disclosure for Research and Audit

The Trust has an academic partnership with Imperial College London forming an Academic Health Sciences Centre (AHSC). All proposed research must be registered with the Joint Research Compliance Office and must accord to Good Clinical Practice Guidelines. All clinical governance audit projects must be registered and approved by the Clinical Governance Lead via the Clinical Safety and Effectiveness Team.

10. Transparency

10.1. All data subjects have the **right to be informed** about how and why the Trust collects, processes, stores and sometimes discloses their personal identifiable and confidential information under Articles 12 to 14 UK GDPR.

10.2. Processing personal data is an essential activity for care delivery and informing patients is the responsibility of all clinical staff when booking or referring patients to additional services and at regular intervals during and post treatment. During a medical emergency**, fair processing materials** should be provided to the patient's carers or representatives and then the patient should be informed at a suitable point during their treatment.

10.3. Such information and fair processing materials shall be provided:

- Where personal data is obtained directly from the patient, at the time such data is obtained,
- Where personal data is not obtained directly from the patient, within a reasonable period after obtaining the personal data, but at the latest within one month,
- if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

10.4. The obligation to provide detailed and specific information to data subjects applies whenever personal data is collected, including for HR or employment purposes.

10.5. Further information about **privacy notices** is published on the Data Protection Office page of the Trust intranet.

11. Subject Access Requests

11.1. Patients have the right to access their records upon request under Article 15 UK-GDPR. The Trust is subject to legal obligations to disclose or cite exemptions of the act to support partial disclosure or non-disclosure, within one calendar month of receiving the request.

11.2. There are several distinct subject access request processes operating within the Trust:

- Health Records – for all patients in all specialties including Imperial Private Healthcare,
- Imaging – for patients who request access to images,
- Human Resources – for all staff in all departments,
- Occupational Health – for staff who have utilised occupational health services,
- Sexual Health – for all patients using sexual health services.
- CCTV and Bodycams

11.3. The Data Protection Office can advise all staff on the rights of data subjects, including patients and employees, under the Data Protection Legislation. Please refer to the Data Subject Access Request Policy.

12. Data Protection Impact Assessments (DPIAs)

12.1. The Trust will conduct Data Protection Impact Assessments when:

- The planned implementation of new systems or a significant change in an existing system is likely to result in a high risk to the rights and freedoms of data subjects,
- Automated processing including profiling is conducted, or a
- Large-scale processing of special categories of personal data is conducted.

12.2. The purpose of undertaking a DPIA is to assess the particular likelihood and severity of the high risk, taking into account the nature, scope, context and purposes of the processing and the sources of the risk.

12.3. DPIAs should include, in particular, the measures, safeguards and mechanisms envisaged for mitigating that risk, ensuring the protection of personal data and demonstrating compliance with Article 35 UK-GDPR.

12.4. The DPO can advise on the completion of the Data Protection Impact Assessment. The procedure for completion of DPIAs is appended to this document. For further reference, the ICO Data Protection Impact Assessment guidance is available **here**.

12.5. Where a DPIA has been conducted and the risks cannot be mitigated, the Data Protection Officer or a delegate shall directly consult the ICO for advice.

13. Security, Integrity and Confidentiality

13.1. Personal data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

13.2. The Trust is responsible for developing, implementing and maintaining safeguards appropriate to the amount of personal data collected and processed, the scope and activities of processing, available resources and identified risks, including encryption and de-identification where applicable.

13.3. Particular care should be exercised in protecting special categories of personal data.

13.4. De-identification

13.4.1. **Anonymised data** can be created, whereby any item of data that could potentially identify an individual has been removed. Anonymisation is potentially complex, e.g. when dealing with statistical analyses of small populations. Care should be taken to ensure that identities of individual patients cannot be identified from this type of information as it is possible to identify individuals from limited data collections.

13.4.2. **Pseudonymised data** can be created, whereby patient identifiers are substituted with a pseudonym, code, or other unique reference so that confidential data will only be accessible to those who have the code or reference. This can often be more easily achieved than full anonymisation of data, and allows the re-identification of data by appropriate persons where necessary. Data is effectively anonymised to those data users who do not have the code and remains patient confidential to those who have the code. The Trust has an established pseudonymisation policy and procedure.

13.5. Role Based Access Controls

13.5.1. The Trust ensures that access to personal confidential information will be restricted to members of staff with a legitimate relationship requiring them to access this data on a need-to-know basis. This is achieved through setting permissions to access the data in accordance with the role that the member of staff performs.

13.5.2. Access to information systems containing personal confidential information should be via a security model incorporated as part of the system specific security policy and registered on the information asset register.

13.6. Data Processing Agreements (DPAs)

13.6.1. Under Article 28 UK-GDPR, processing undertaken by a third-party processor on behalf of the Trust as a data controller shall be governed by a contract or legal act, namely an Information or Data Processing Agreement. These documents are mandated to ensure the arrangements between the Trust and third parties are

documented and approved, in respect to information security and confidentiality. Typical examples include:

- Joint healthcare arrangements with commercial and NHS organisations for instances where Trust personal confidential information is being shared,
- Third party information processing services and /or shared care arrangements,
- Sub-contracted work of the Trust being carried out by third parties where there is processing of personal confidential information,
- Where Trust information is being submitted to clinical registers.

13.6.2. Research projects where personal confidential information is being transferred to or proceed by a third party organization are subject to detailed review of the informational relationships of the various parties. This may require an Information Processing Agreement and/or alternative arrangements for information sharing. All such projects must be communicated to the JRO/JRCO for their respective assessment.

13.6.3. Where a third party supplier is itself using a sub-contractor, the Trust must authorise this in specific terms through the IPA with the processor. Under Article 28(4) UK-GDPR, where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

13.6.4. Any project between the Trust and a third party involving the processing of personal data, including new systems, research, clinical audit, clinical registries, national projects, service evaluations, will require review by the Data Protection Office.

13.7. Confidential Paper Waste

Papers containing personal confidential information shall be disposed of securely using specially labelled blue confidential waste bins. A procedure is published on the Trust intranet.

13.8. Retention

The Trust works in accordance with the NHS X Records Management Code of Practice 2021 at all times.

14. Abuse of Authorised Access

14.1. All staff must comply with and not attempt to circumvent the administrative, physical and technical safeguards implemented in accordance with the UK GDPR and relevant standards to protect personal data.

14.2. Abuse of authorised access as per the terms set out below is considered to be a breach of this policy, the Information Security Policy and, in some circumstances, the Computer Misuse Act 1990, the UK-GDPR and the Common Law Duty of Confidentiality.

14.3. Personal information may only be accessed in pursuit of the Trust's activities. This is primarily for the purpose of direct care (which includes administrative work in support of that care), but may also include non-direct care purposes. Examples include, but are not limited to: administration, planning, audit, commissioning, payment by results, clinical research and education.

14.4. Even where access to personal confidential information for non-direct care purposes is legitimate, any further use of disclosure of personal confidential information must be subject to the technical and organisational controls set out in the terms of this Policy.

14.5. Users accessing or attempting to access medical or confidential information concerning themselves, family, friends or any other individual without a legal basis, a legitimate purpose and prior authorisation from senior management is strictly forbidden and shall be deemed a disciplinary offence.

14.6. Use of Trust or NHS information systems or data contained therein for personal gain, to obtain personal advantage or for profit is not permitted and shall be deemed a disciplinary offence.

14.7. Where misuse is identified it must be immediately reported to the Data Protection Office (imperial.dpo@nhs.net)

14.8. If identified misuse is considered a criminal offence this may be reported to the relevant authorities in accordance with legal requirements.

15. Supporting Information

Current Document Information	
Version:	V6.0
Document Lead:	Philip Robinson, Head of DPO Services
Responsible Executive Director:	Kevin Jarrold, Chief Information Officer
Approving Committee / Group:	Data Security and Protection Committee
Date Approved:	14.08.2023
Date Ratified by Executive Committee:	22.08.2023
Date Due for Review:	11/05/2024
Target Audience:	All Trust Staff
Category:	Data Protection

Current Document Replaces	
Previous Document Name:	Data Protection, Confidentiality and Information Sharing Policy
Previous Version Number:	V5.0
Previous Approval Date:	26.03.2019

Supporting References	
Keywords:	
Related Trust Documents:	Information Security Policy; Health Records Policy; Data Protection Compliance Policy

Contributing Authors	
Individuals:	Mansour Faez, Deputy Head of DPO Services

Consultation		
Sent to		**Date**
Committee / Groups:	Data Security and Protection Committee	06/06/2023
Team / Departments:		
Individuals:		

Version Control History			
Version	**Date**	**Policy Lead**	**Changes**
2.0	22.01.2019	Philip Robinson	Review and update
3.0	26.03.2019	Corporate Governance	Final ratified.
5.0	11/05/2022	Corporate Governance	Final ratified.
6.0	01/06/2023	Corporate Governance	TBC
6.1	05/07/2023	Corporate Governance	Review and update

Appendix 1 – DPIA Procedure

1. Purpose

1.1. Article 35 of the UK General Data Protection Regulation (UK-GDPR) introduces the concept of a Data Protection Impact Assessment (DPIA). A DPIA should describe the envisaged processing operations and the purposes of the processing assess necessity and proportionality of the processing, identify risks to the rights and freedoms of individuals and determine measures to mitigate these risks.

1.2. The DPIA acts as a demonstration of compliance by the data controller with the requirements under the UK-GDPR. By undertaking a DPIA for a processing activity or a new system, the data controller demonstrates mindfulness of the principles of data protection by design and data protection by default (Article 25). DPIAs are important tools for accountability, as they help controllers comply with requirements of the UK-GDPR and demonstrate that appropriate measures have been taken to ensure compliance with the Regulation (Article 24).

1.3. The DPIA is administered in two stages: the first stage is designed to identify whether the processing activity is likely to result in a high risk to the rights and freedoms of data subjects ('Threshold DPIA') and the second stage constitutes a full assessment, incorporating the requirements as stated in Articles 35 of the UKGDPR ('Full DPIA').

1.4. This document sets out the procedure under which DPIAs shall be undertaken where processing of personal identifiable data is undertaken by or behalf of the Trust.

2. Procedure

2.1. Whenever there is a materially new or changed processing activity, involving the processing of personal identifiable data, the Data Protection Office must be consulted as a matter of routine.

2.2. In the first instance a Threshold DPIA shall be administered to the responsible Information Asset Owner for the asset most closely associated to the processing activity.

2.3. If the processing activity is determined to present a high risk to the rights and freedoms of any Data Subject, a Full DPIA will be issued by the Data Protection Office. This document will identify and articulate any and all risks and mitigations involved in this processing activity.

2.4. The Data Protection Office shall review the risks and their mitigations as identified in the DPIA. This will allow the team to advise whether a processing activity should proceed, and articulate and conditions that should be satisfied or steps should be taken to allow it to do so in a manner compatible with all relevant legal and organisational requirements.

2.5. DPIA questionnaires shall be administered to project owners on the OneTrust Privacy Management Portal. The Threshold DPIA will be configured to automatically flag a risk scoring indicating a need for the completion of a Full DPIA where the processing activity may present a "high risk" to the rights and freedoms of the individual within the meaning of the UK-GDPR.

2.6. OneTrust assessments are designed to be clear and accessible to assist the respondent to undertake the assessment for review by the Data Protection Office.

3. Procedural Requirements and Legal Obligations

3.1. For the avoidance of doubt, all processing of personal identifiable data by or on behalf of the Trust must be undertaken lawfully and in accordance with Trust policy. This includes legal requirements to comply with the UK-GDPR and Data Protection Act 2018, the Common Law

Duty of Confidentiality, and all applicable Trust policies, including the Trust Information Security Policy.

3.2. Any high risk processing which has not been subjected to a DPIA should not begin or continue to be undertaken as per the terms of the Trust's Information Security Policy and the Confidentiality and Information Sharing Policy. Moreover, completion of a DPIA for instances of high risk processing is an explicit requirement under Article 35 UK-GDPR, and failure to complete such a document could leave the Trust in breach of its obligations to this extent.

3.3. It should be noted that the DPIA forms but one part of the Data Protection review. All new systems and processes shall be subject to full review and final approval by the Caldicott Guardian before they can be deemed to be "warranted" from a Data Protection perspective.

- Data Protection Act 2018;
- UK General Data Protection Regulation
- The Caldicott Principles;
- Common Law Duty of Confidentiality;
- The Freedom of Information Act 2000;
- The Mental Capacity Act 2005;
- Section 251 of the NHS Act 2006 (originally enacted under Section 60 of the Health and Social Care Act 2001);
- Health and Social Care (Safety and Quality) Act 2015
- Public Health (Control of Disease) Act 1984;
- Public Health (Infectious Diseases) Regulations 1988;
- The Gender Recognition Act 2004;
- Confidentiality: NHS Code of Practice 2003;
- IGA Records Management Code of Practice for Health and Social Care 2016;
- Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013;
- Abortion Regulations 1991;
- Road Traffic Act 1988;
- ICO Data Sharing Code of Practice;
- Confidentiality and Disclosure of Information Directions 2013;
- Health and Social Care Act 2012;
- The Criminal Justice Act 2003;
- The NHS Information Security Management Code of Practice 2007;
- The Computer Misuse Act 1990;
- The Electronic Communications Act 2000;
- The Regulation of Investigatory Powers Act 2000;
- The Prevention of Terrorism Act 2005;
- The Copyright, Designs and Patents Act 1988;
- The Re-Use of Public Sector Information Regulations 2005;
- The Human Rights Act 1998; and
- The NHS Care Record Guarantee 2007

Description of data processed

Health information, such as:

- A&E visits, hospital admissions or clinic appointments
- Scans, X-rays or tests
- Your diagnosis or treatment
- Any allergies or health conditions

from patients allow the Trust to administer healthcare, as listed in the privacy policy: https://www.imperial.nhs.uk/privacy.

Condition for processing

The conditions for processing, including official authority, public interest and research, are determined in the privacy policy: https://www.imperial.nhs.uk/privacy

Procedures for ensuring compliance with the principles

Accountability principle

- ✓ Appropriate documentation of our processing activities and appropriate data protection policies: The Trust has a plethora of policies and guidance which dictate how Trust's staff set and follow relevant guidance which are approved at Board level, such as the Information Security Policy, the Confidentiality Policy, the Password Policy, the Acceptable Use Policy, etc.
- ✓ DPIAs for use of personal data that are likely to result in high risk to individuals' interests are conducted in accordance with this Policy.

Principle (a): lawfulness, fairness and transparency

- ✓ Appropriate lawful basis for processing and a further Schedule 1 condition for processing SC data are documented in the relevant privacy policies and above.
- ✓ Appropriate privacy information is available with respect to the SC data, including online at: Imperial College Healthcare NHS Trust | My records.

Principle (b): purpose limitation

- ✓ Purpose(s) for processing the SC data include providing health and social care, service evaluation, planning and improvement and medical research. The specific purposes for dedicated projects or programmes are detailed in DPIAs as per the Policy above.
- ✓ Appropriate details of these purposes are further detailed in the patients privacy notice at: privacy-notice-patients.pdf (imperial.nhs.uk)
- ✓ Procedures and DPIAs are kept under regular review to ensure the purpose limitation principle is complied with. The Trust provides templates for DPIAs, screening questionnaires, and security impact assessments.

Principle (c): data minimisation

- ✓ Datasets are reviewed and adapted to each specific programme of work.
- ✓ The Trust applies the Records Management Code of Practice for Health and Social Care 2021 attached below and deletes data accordingly, or before if not necessary anymore.

Principle (d): accuracy

- ✓ Data is collected when patients attend one of the Trust's hospitals or services on paper or electronically. Trust's patients have summary care records and other NHS organisations may share information with the Trust when necessary for the provision of health and social care. The data sources are regularly updated.
- ✓ Patients may request changes to any data hold by the Trust that is incorrect or incomplete by contacting the Health Records Team. Such process is mentioned in the patient's privacy notice.

Principle (e): storage limitation

- ✓ Retention periods for research partners are set by the Trust.
- ✓ The Records Management Code of Practice for Health and Social Care 2021 is followed.
- ✓ Researchers do not have access to personal identifiable data unless data subjects have provided explicit and informed consent to such processing, or another legal justification allows to do so.

Principle (f): integrity and confidentiality (security)

- ✓ The Trust maintains an Information Security Policy, a Bring Your Own Device Policy, an Acceptable Use Policy, a Data Subject Access Request Policy, an IT & Cyber Security Risks and Issue Log.
- ✓ Privileged Users Groups are applied so that data is accessed on a need-to-know basis and depending on Role-Based Access Controls.
- ✓ The Trust obtained its Cyber Essentials Plus certificate.

Retention and erasure policies

NHS X Records Management Code of Practice 2021:
DPO - NHSX Records Management Code of Practice 2021 - The intranet (imperial.nhs.uk)

Description of data processed

Criminal Offence (CO) data from employees and potential employees may be processed.

Condition for processing

The conditions for processing are determined in the privacy policy for prospective employees at: prospective-employee.pdf (imperial.nhs.uk) and include assessing suitability to work and carrying out criminal record checks where applicable.

Procedures for ensuring compliance with the principles

Accountability principle

- ✓ Appropriate documentation of our processing activities and appropriate data protection policies: The Trust has a plethora of policies and guidance which dictate how Trust's staff set and follow relevant guidance which are approved at Board level, such as the Information Security Policy, the Confidentiality Policy, the Password Policy, the Acceptable Use Policy, etc.
- ✓ DPIAs for use of personal data that are likely to result in high risk to individuals' interests are conducted in accordance with this Policy.

Principle (a): lawfulness, fairness and transparency

- ✓ Appropriate lawful basis for processing and a further Schedule 1 condition for processing CO data are documented, and
- ✓ Appropriate privacy information is available with respect to the CO data, including online at: prospective-employee.pdf (imperial.nhs.uk)

Principle (b): purpose limitation

- ✓ Purpose(s) for processing the CO data include carrying out criminal record checks for prospective employees.
- ✓ Procedures and DPIAs are kept under regular review to ensure the purpose limitation principle is complied with. The Trust provides templates for DPIAs, screening questionnaires, and security impact assessments.

Principle (c): data minimisation

- ✓ The Trust applies the Records Management Code of Practice for Health and Social Care 2021 attached below and deletes data accordingly, or before if not necessary anymore.

Principle (d): accuracy

- ✓ Data subjects can take action to rectify any inaccuracies in the personal information hold by the Trust by contacting email as stated in the privacy policy: prospective-employee.pdf (imperial.nhs.uk).

Principle (e): storage limitation

- ✓ The Trust only retain CO data for as long as necessary for the purposes that the information was collected and for the purposes of meeting legal obligations.
- ✓ The Records Management Code of Practice for Health and Social Care 2021 is followed.

Principle (f): integrity and confidentiality (security)

- ✓ The Trust maintains an Information Security Policy, a Bring Your Own Device Policy, an Acceptable Use Policy, a Data Subject Access Request Policy, an IT & Cyber Security Risks and Issue Log.
- ✓ Privileged Users Groups are applied so that data is accessed on a need-to-know basis and depending on Role-Based Access Controls.

Retention and erasure policies

NHS X Records Management Code of Practice 2021:
DPO - NHSX Records Management Code of Practice 2021 - The intranet (imperial.nhs.uk)