Policy Document

Reference: DSP10

University Hospitals of North Midlands NHS Trust

Data Security, Protection and Confidentiality

Version:	**9**
Date Ratified:	**April 2024 by the Executive Digital and Data Security & Protection Group**
To Be Reviewed Before:	**April 2027**
Policy Author:	**Data Security & Protection Manager - Records**
Executive Lead:	**Chief Digital Information Officer**

Version Control Schedule

Version	Issue Date	Comments
1	October 2009	
2	March 2011	
3	May 2013	Approved by IGSG with minor changes, page 15 to 40 calendar days.
4	March 2015	Appendix added to provide IG guide for staff
5	June 2018	GDPR Updates
6	January 2019	Inclusion of Confidentiality replacing IG09
7	January 2022	Policy Review; updated title and reference to reflect change in the title of the DSP team Multiple pages to update document to meet DPA 2018/UK GDPR terminology Page 6 – inclusion of definition of SAR/PDR Page 8 – updated narrative to include new, forthcoming due diligence documentation which is referenced in appendix 1 Page 8 – updated Staff responsibilities to include the need to access data for business use only Page 9 – inclusion of the need to record all training on ESR (as a result of comments from PRG – December 2021) Page 10 – clarification of S170 of the DPA 2018 and instructions regarding securing data when off-sit Page 11 – Advice/guidance for legal requests Page 13 – inclusion of explanation around PDR Page 14 – further clarification of DPIA sign off
8	July 2022	Page 12 – reference to the Acceptable use of Electronic PID (DSP10 [S1]) SOP with regard to accessing the SCR Page 16 – clarification of the use of an MoU Page 22 - Acceptable use of electronic PID (S1) V1.0
9	April 2024	Page 6 – clarification on consent Page 7 – clarification on consent Page 9 – updated Roles & Responsibilities Page 15 - Consent to share and/ or Process Data added. Page 15 – Professional Activity Page 11 – Updated Monitoring arrangements and annual training removed Page 13 – updated purpose Page 15 – updated purpose Page 18 – Service Evaluations and Audits added. DSP10 [S2] SOP regarding consent to share/process data aligned to policy. DSP10 [S3] SOP Handling Requests under DPA Data subject rights aligned to policy.

Statement on Trust Policies

The latest version of 'Statement on Trust Policies' applies to this policy and can be accessed here

University Hospitals of North Midlands NHS Trust

Equality Impact Assessment (EIA)

The Trust aims to design and implement services, policies and measures that meet the diverse needs of our service, population and workforce, ensuring that none are placed at a disadvantage over others. The Equality Impact Analysis Form is designed to help consider the needs and assess the impact of each policy. To this end, EIAs will be undertaken for all policies.

Policy Reference, Title and Version Number	DSP10 (previously IG10) Data Security, Protection & Confidentiality
Summary of changes made on this review	Review/refresh
Please list which service users, staff or other groups have been consulted with, in relation to this	Records Management Group; HR consultations
Were any amendments made as a result? If yes, please specify	Updated according to current practices (see version control)
Which Executive Director has been consulted on?	Chief Digital Information Officer (via Executive Data Security & Protection Group)
Does this policy have the potential to affect any of the groups listed below differently - please complete the below. Prompts for consideration are provided, but are not an exhaustive list	

Group	Is there a potential to impact on the group? (Yes/No/Unsure)	Please explain and give examples	Actions taken to mitigate negative impact
Age (e.g. are specific age groups excluded? Would the same process affect age groups in different ways?)	No		
Gender (e.g. is gender neutral language used in the way the policy or information leaflet is written?)	No		
Race (e.g. any specific needs identified for certain groups such as dress, diet, individual care needs? Are interpretation and translation services required and do staff know how to book these?)	No		
Religion & Belief (e.g. Jehovah Witness stance on blood transfusions; dietary needs that may conflict with medication offered)	No		
Sexual orientation (e.g. is inclusive language used? Are there different access/prevalence rates?)	No		
Pregnancy & Maternity (e.g. are procedures suitable for pregnant and/or breastfeeding women?)	No		
Marital status/civil partnership (e.g. would there be any difference because the individual is/is not married/in a civil partnership?)	No		

Group	Is there a potential to impact on the group? (Yes/No/Unsure)	Please explain and give examples	Actions taken to mitigate negative impact
Gender Reassignment (e.g. are there particular tests related to gender? Is confidentiality of the patient or staff member maintained?)	No		
Human Rights (e.g. Does it uphold the principles of Fairness, Respect, Equality, Dignity and Autonomy?)	No		
Carers (e.g. is sufficient notice built in so can take time off work to attend appointment?)	No		
Socio/economic (e.g. would there be any requirement or expectation that may not be able to be met by those on low or limited income, such as costs incurred?)	No		
Disability (e.g. are information/questionnaires/consent forms available in different formats upon request? Are waiting areas suitable?) Includes hearing and/or visual impairments, physical disability, neurodevelopmental impairments e.g. autism, mental health conditions, and long term conditions e.g. cancer.	No		
Are there any adjustments that need to be made to ensure that people with disabilities have the same access to and outcomes from the service or employment activities as those without disabilities? (e.g. allow extra time for appointments, allow advocates to be present in the room, having access to visual aids, removing requirement to wait in unsuitable environments, etc.)		**Yes**	**No**
			✓
Will this policy require a full impact assessment and action plan? (a full impact assessment will be required if you are unsure of the potential to affect a group differently, or if you believe there is a potential for it to affect a group differently and do not know how to mitigate against this - please contact the Corporate Governance Department for further information)		**Yes**	**No**
			✓

CONTENTS **Page**

1. INTRODUCTION

The Trust, and the wider NHS, holds information about large numbers of people. Much of this information is personal, confidential, or sensitive/special category. Information is held about patients and staff. All Trust staff are responsible for the information held by the Trust and have a duty to ensure its secure and proper use.

Information considered identifiable, personal, confidential or sensitive/special category held by or on behalf of the Trust must be processed legally, securely and built on models of trust, confidentiality and best practice in accordance with the principles of the Data Protection Act (2018), the General Data Protection Regulation (2018), the UK General Data Protection Regulations; the common law duty of confidentiality, the Caldicott Principles, the Data Security & Protection Toolkit and NHS Codes of Practice on Confidentiality and Information Security Management. This policy and the associated staff DSP manual provides a guide to the key elements of the legal framework governing information handling and the responsibilities of all staff in relation to data security, protection and confidentiality.

Penalties can be imposed on the Trust and/or employees/contractors for non-compliance with relevant legislation and guidance. This includes a monetary penalty of up to €10-20 million for "reckless use of information" that can be imposed by the Information Commissioner's Office (ICO). Accessing or processing information for which staff have no legitimate reason a disciplinary offence that will result in disciplinary action.

Data security, protection and confidentiality is an integral part of information governance (IG), providing the legal basis for the processing of data. Data Security & Protection training is part of statutory and mandatory training and must be completed by all Trust staff on an annual basis. This requirement is set by the Department of Health to ensure staff are aware of their responsibilities including data security, protection and confidentiality.

Unlawful processing of data leaves the Trust open to complaint, external investigation, monetary penalties, and possible legal action. Data protection and Caldicott principles apply no matter what format the data is held in and by which method any sharing of that data may take place.

2. SCOPE

This document applies to all Trust staff, and third parties processing/ sharing data on behalf of the Trust.

This policy applies to all processing of personal or otherwise sensitive/special category data including but not limited to, electronic, paper based and verbal.

The manual provided via the appendix to this policy covers common topics within data security and protection but it is by no means exhaustive or all encompassing. Requests for use of data can often be sporadic and unique and staff should contact the DSP department if they require further advice – dspuhnm@uhnm.nhs.uk

3. DEFINITIONS

Anonymisation
Information amended in such a way that no individual can be identified from the information (whether directly or indirectly) by any means or by any person.

Consent to Process Information
Consent is the approval or agreement for something to happen after consideration. For consent to be legally valid, the individual must be informed, must have capacity to make the decision and must give

consent voluntarily. As stated, this relates to the process of personal identifiable data and does not relate to consent for clinical treatment.

Data Breach
A breach leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Data Controller
A 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.

Data Flow
A regular exchange of information, this may be between colleagues, between departments, or between the Trust and a third party.

Data Processor
A natural or legal person, Public Authority, Agency or other body which processes personal data on behalf of a Data Controller.

Data Protection Impact Assessment (DPIA)
A document to be completed when identifiable data is to be processed for the first time, or when significant changes are made to a current system. Assess the justification for using the data and the security in place.

Data Subject
The identified or Identifiable Natural Person to which the data refers.

Duty of confidence
A circumstance in which one person discloses information to another in a situation where it is reasonable for them to expect that information to remain confidential**.**

Encryption
The process of converting information or data into code, to prevent unauthorised access.

Explicit Consent to Process Information (NOT consent to clinical treatment)
Can be given in writing or verbally, or conveyed through another form of communication such as signing. Explicit consent is required when sharing information with parties who are not part of the team caring for the individual. It may also be required for a use other than that for which the information was originally collected for, or when sharing is not related to an individual's direct health and social care. For data protection purposes, this must clearly set out how the information is going to be used and how the person can withdraw that consent.

Identifiable Natural Person
Anyone 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 one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Implied Consent to Process Information (NOT consent to clinical treatment)
Is only applicable within the context of the direct care of an individual, instances where the consent of the individual patient can be implied without them having to take any positive action, such as a verbal agreement for a specific aspect of sharing information to proceed.

Information Sharing Agreement
An agreement what is in place between two or more parties, to justify and authorise the sharing of identifiable data.

Third Party
An external organisation that UHNM conducts business with.

Personal Identifiable Data (PID)
Items of data concerning a data subject that, if used singly or in conjunction with other data items, could lead to identification of the data subject. Data items include (but are not limited to) name, address, photographs and clinical images, telephone and email contact details. Also includes rare/unique information about a person that could identify them, even if their name is not present.

Personal, sensitive and confidential Data
Any information (including opinions and intentions) which relates to an identified or Identifiable Natural Person, patient or staff regardless of the format it is stored in.

Process, Processed, Processing
Any operation or set of operations performed on personal data or on sets of Personal Data, whether or not by automated means. Operations performed may include 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.

Profiling
Any form of automated processing of Personal Data where Personal Data is used to evaluate specific or general characteristics relating to an Identifiable Natural Person. In particular to analyse or predict certain aspects concerning that natural person's performance at work, economic situations, health, personal preferences, interests, reliability, behaviour, location or movement.

Pseudonymisation
Information amended in such a way that no individuals can be identified from the information (whether directly or indirectly) without a "key" that allows the data to be re-identified.

Service Evaluation
Service evaluation seeks to assess how well a service is achieving its intended aims.

Special Categories of Data
Personal Data pertaining to or revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data.

Subject Access Request (SAR)
An individual has the right under the Data Protection Act to ask to view or receive a copy of information held about them by an organisation. This is known as a "subject access request" and these are managed by either HR (in the case of staff requests for information) or Health Records (in the case of requests for information held in a patient's medical record).

Personal Data Request (PDR)
An individual has the right under the Data protection Act to ask to view or receive a copy of information held about them by an organisation. PDR requests are handled by the DSP Team and relate to information held by the Trust (on the Trust network or in e-mails) which do not sit within either the HR Record or a Patient's Medical Record.

Third Country
Any country not recognised as having an adequate level of legal protection for the rights and freedoms of Data Subjects in relation to the Processing of Personal Data.

4. ROLES AND RESPONSIBILITIES

The Trust Board is ultimately responsible for ensuring the Trust meets its legal responsibilities, and for the adoption of internal and external governance requirements. The Strategy & Transformation Committee will be updated on Data Security & Protection issues via the Executive Digital & DSP Group Highlight Report.

Chief Executive
The Chief Executive as the Accountable Officer for the Trust has overall accountability and responsibility for DSP throughout the Trust and is required to provide assurance that all risks to the Trust, including those relating to information, are effectively managed and mitigated.

Senior Information Risk Owner (SIRO)
The Trust SIRO is responsible to the Chief Executive for DSP and acts as an advocate for information risk on the Trust Board.

Caldicott Guardian
The Trust's Caldicott Guardian has a particular responsibility for reflecting patients' interests regarding the use of Personal Identifiable Data (PID). The Caldicott Guardian is responsible for ensuring PID is shared in an appropriate and secure manner.

Data Protection Officer (DPO)
The Data Protection Officer (DPO) will advise and monitor compliance with the GDPR. They are responsible for ensuring effective management, accountability, compliance and assurance for all aspects of the Trust's DSP agenda. They will also be the first point of contact with the Supervisory Authority – the Information Commissioner's Office

Information Asset Owner (IAO)
Designated Information Asset Owners (IAOs) are responsible for providing assurance to the SIRO that information risks, within their respective areas of responsibility, are identified and recorded and that controls are in place to mitigate those risks.

Information Asset Administrator (IAA)
Information Asset Owners can appoint Information Asset Administrators (IAAs) to support them in the delivery of their information risk management responsibilities. IAA ensure that policies and procedures are followed, recognise actual or potential security incidents and take steps to mitigate those risks, consult with their IAO on incident management and ensure that information asset registers are accurate and up to date. Where an IAA is not in place, this function is carried out wholly by the IAO.

Data Security & Protection Managers (Records & Assets)
The Trust's Data Security & Protection Managers are responsible for supporting the Data Protection Officer in the implementation of the Trust's DSP agenda.

Executive Digital & DSP Group (EDDSPG)
The Chief Digital Information Officer chairs the Trust's EDDSPG. This group is responsible for overseeing the day to day management of the individual components of the Trust's Data Security & Protection Framework and reports to the Trust's Strategy and Transformation Committee.

Information Security Manager (RA and Privacy)
Provides advice to the Trust, ensuring compliance, and conformance, with local and national requirements, and, generally, on information risk analysis/management incorporating the Privacy Officer role which focuses on ensuring privacy related alerts from electronic systems (e.g., Summary Care Record) are investigated for appropriateness, as well as other privacy compliance work as necessary.

Service Leads and Department Heads
Ensure that local staff inductions include all aspects of data security, protection and confidentiality. Ensure that staff are briefed on and kept aware of confidentiality and data security, protection initiatives and requirements. Enable implementation of the policies and procedures at local level and encourage reporting of breaches via the incident reporting procedure. They must identify and manage risks within the control of the Department/Directorate. Ensure that all staff within their department/directorates are up to date with their mandatory Data Security & Protection training, to ensure the national compliance target is achieved. Ensuring that their staff have only appropriate access to information and systems by advising Information asset owners and the IT department of staff changes.

Subject Access Team
To ensure timely processing of patient related subject access requests made under GDPR, Access to Health Records, and Access to Medical Reports. Ensure they have completed the necessary training to manage SARS requests, including processing requests, who to direct search queries to, applying exemptions to requests and redacting documents with third party or exempt information. The team must keep an accurate and up to date log of all data requests received by the Trust and fully trained on the adverse effects to the trust of any data breached or incidents, and know the process for reporting incidents on Datix.

Human Resources/Pathology and Local Security Management Specialist (for CCTV requests)
These departments must ensure timely processing of all subject access requests made under UK GDPR/DPA (including Staff requests), and that relevant staff within these departments are fully trained on processing requests, and know who to go to for searches and are competent on applying exemptions to requests made under UK GDPR/DPA. The department must keep an accurate and up to date log of all data requests received by the Trust

All Clinical Staff - Professional Activity
Although it is a requirement to keep a log of your professional activity e.g., procedures undertaken to demonstrate competence and development. If you make the decision to keep a physical logbook it is important to remember that no Personal Identifiable Information is to be captured. This is to ensure you and the Trust comply with the Data Protection Act 2018 as patients have not given their consent to have their information stored/used in this way for this purpose.

To avoid the use of a physical logbook, you can request an electronic audit of your activity, and this will be provided in an anonymous form with patient information removed. To make this request please email DSPUHNM@uhnm.nhs.uk

It is also important to remember that no patient information is removed from Trust premises in the event of you leaving the employment of UHNM. All patient information remains the property of the Trust and it is only used for the stated purpose in line with the Data Protection Act 2018.

If it is found that clinicians have used and stored patient identifiable information in this way, disciplinary action may be taken or a report may be made to the Information Commissioners Office (ICO) for them to take action against the clinician as an individual.

All Staff
All staff, via job roles and contracts of employment/professional registrations must comply with specific DSP related legal and ethical obligations and therefore must be aware of the related standards which impact within their area of responsibility. Individual staff must ensure that any personal and corporate information, is managed legally, securely, and efficiently in order to assist in the delivery of the best possible care/practice. Staff must keep up to date with DSP initiatives, keeping informed on policy and strategy requirements. Staff holding any spread sheets or databases containing personal identifiable information (PIL) must notify the DSP team to confirm legitimate purpose and review minimum data requirements. Staff involved with implementation of new services/ technologies and IT systems must

complete the appropriate DSP due diligence documentation (see appendix 1). All staff should be aware of the potential business risks and impacts associated with the use of blogging and social networking websites. This is further documented in **G06 Trust Media Policy.** Staff can email the DSP team on dspUHNM@uhnm.nhs.uk with any DSP related queries.

Staff should be aware that it is a criminal offence to access Personal Identifiable data (S.170 of the DPA 2018) without a valid business reason to do so, and that includes accessing staff's own records or those of family and friends, even with consent. The Trust views such actions as gross misconduct and disciplinary action, according to Trust procedures, may be taken if such access is identified.

Record Services Operational Group (RSOG)
The RSOG has responsibility for receiving issues raised and actions taken, to ensure the Trust meets its obligations under the legislation and that patient safety is maintained.

Service Evaluations/Audit
Staff may have a need to conduct service evaluations or audits to demonstrate the effectiveness of UHNM services upon patient care. Before any service evaluation or audits take place, they must be approved by the Data Security and Protection Team by emailing the request to DSPUHNM@uhnm.nhs.uk, where the requester will be asked to complete a screener detailing the purpose and process of the proposed activity. Once approval is given, the DSP team will register the service evaluation/audit with UHNM's audit team.

5. EDUCATION/TRAINING AND PLAN OF IMPLEMENTATION

Data Security & Protection training is a mandatory requirement for all staff employed within the Trust. The Data Security and Protection Toolkit requires that a minimum of 95% of staff are trained in Data Security & Protection.

Fundamental to the success of delivering the DSP framework is developing a positive DSP culture within the Trust. All staff utilise information in their day to day work. Awareness and training needs to be provided to everyone to promote this culture.

All staff, whether permanent, temporary or contracted, must be aware of their own individual responsibilities for the maintenance of information confidentiality, data protection, security and quality. To support this objective, all staff will receive training on commencement of employment and appropriately for their role on an annual basis. All training to be recorded on ESR.

In addition staff will be notified of changes by email, intranet display and any other mass coverage methods available.

6. MONITORING AND REVIEW ARRANGEMENTS

6.1 Monitoring Arrangements

Compliance with this policy will be monitored via review of reported incidents, together with a report produced to assess compliance with guidance re. timescales

6.2 Review

This policy will be reviewed three years after ratification, or sooner if changes to guidance/law requires.

7. REFERENCES

Department of Health: “Confidentiality: NHS Code of Practice” 2003. Data Protection Act (DPA) 2018
UK General Data Protection Regulation (as tailored by the DPA 2018)
Human Rights Act 2000
Regulation of Investigatory Powers Act 2000 Crime and Disorder Act 1998
Computer Misuse Act 1990
Access to Health Records Act 1990 Access to Medical Reports Act 1988 Health & Social Care Act 2001: Section 60
The Privacy and Electronic Communications (EC Directive) Regulations 2003 Department of Health: “Confidentiality: NHS Code of Practice” -November 2003. Information Commissioner’s Office: www.ico.org.uk
NHS Digital: www.digital.nhs.uk
Information Governance Alliance: https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/information-governance-alliance-iga

APPENDIX 1: –GUIDANCE ON MAINTAINING CONFIDENTIALITY

Using and disclosing patient confidential information

It is extremely important that patients are made aware of the way information will be used and how it may be disclosed in order to provide them with high quality care. In particular, patients may not be aware of clinical governance and clinical audits, even though they are wholly proper components of healthcare provision and therefore this should be drawn to their attention. Similarly, whilst patients may understand that information needs to be shared between members of care teams and between different organisations involved in healthcare provision, this may not always be the case and the efforts to inform them should reflect the breadth of the required disclosure. This is particularly important where disclosure extends to non-NHS bodies. For further guidance see the Trust's Overarching Information Sharing Protocol.

Accessing patient confidential information

In line with the Caldicott Principles and the Data Protection Act 2018, staff are permitted to access patient data/confidential information, FOR BUSINESS USE ONLY. It is NOT permitted to access data for any other reason – this includes accessing your own data. To do so is a criminal offence under S170 of the Data Protection Act 2018. The Trust regards this as gross misconduct, is in breach of the staff employment contract and will be the subject of appropriate disciplinary action, according to the Trust Policies & Procedures.

When accessing information contained within the Shared Care Record (SCR) staff must following the information provided in the Acceptable Use of Electronic PID SOP (ref: DSP10[S1]) which can be found on the Trust Intranet. In summary, the SOP advises staff of the need to seek the patient's explicit consent to access the data and provides guidance on how to achieve this.

Securing patient confidential information

Staff are reminded that they have individual responsibility for managing patient and staff confidential information and for ensuring that this information is handled appropriately, maintaining information security standards. Information must be kept securely at all times and when transporting information outside of the Trust site, where this is unavoidable, it must be kept securely and not left in a vehicle under any circumstances.

Follow any established information sharing protocols.

NHS organisations should have developed, or be in the process of developing, information sharing protocols that set out the standards and procedures that should apply when disclosing confidential patient information with other organisations and agencies. Staff must work within these protocols where they exist and within the spirit of this code of practice where they are absent.

Identify enquirers, so that information is only shared with the right people.

Staff should check that any callers, by telephone or in person, are who they say they are. There can be a significant risk of harm to a patient through impersonation by those seeking information improperly. Seek official identification or check identity by calling them back (**using an independent source for the phone number**). Check also that they have a legitimate right to have access to that information.

Ensure that appropriate standards are applied in respect of e-mails, and surface mail

Care must be taken, particularly with confidential clinical information, to ensure that the means of transferring it from one location to another are as secure as they can be.

Share the minimum necessary to provide safe care or satisfy other purposes

This must clearly be balanced against the need to provide safe care where missing information could be dangerous. It is important to consider how much information is needed before disclosing it. Simply providing the whole health record is generally needless and inefficient (for both parties), and is likely to constitute a breach of confidence. The Caldicott Principles should always be applied (see IG Staff manual).

Disclosing/sharing information with others
The key principle of the duty of confidence is that information confided should not be used or disclosed further in an identifiable form except as originally understood by the confider, without his or her permission.

Law Enforcement Requests & Disclosures
In certain circumstances, it is permitted that Personal Data be shared without the knowledge or Consent of a Data Subject. This is the case where the disclosure of the Personal Data is necessary for any of the following purposes:

- The prevention or detection of crime.
- The apprehension or prosecution of offenders.
- The assessment or collection of a tax or duty.
- By the order of a court or by any rule of law.

If the Processing of Personal Data is done for one of these purposes, then it may apply an exception to the Processing rules outlined in this policy but only to the extent that not doing so would be likely to prejudice the case in question. If staff are in any doubt, please contact the Data Security & Protection team for advice/guidance (dspuhnm@uhnm.nhs.uk).

GUIDANCE ON DATA PROCESSING, PROTECTION & SECURITY

Data Subject Notification
UHNM will provide Data Subjects with information as to the purpose of the Processing of their Personal Data via an online 'Privacy Notice'.

Consent to share and/ or Process Data
There may be some circumstances that UHNM will need to seek Explicit Consent for the purposes of sharing and/or processing personal and/ or special category data. UHNM will only share/process data once Explicit Consent has been obtained and recorded as part of it's due diligence processes. UHNM will ensure this Consent is reviewed regularly, up dated and withdrawn where applicable. See SOP, Appendix - Consent to Share and/ or Process Data

Professional Activity
Although it is a requirement to keep a log of your professional activity e.g., procedures undertaken to demonstrate competence and development. If you make the decision to keep a physical logbook it is important to remember that no Personal Identifiable Information is to be captured. This is to ensure you and the Trust comply with the Data Protection Act 2018 as patients have not given their consent to have their information stored/used in this way for this purpose.

To avoid the use of a physical logbook, you can request an electronic audit of your activity, and this will be provided in an anonymous form with patient information removed. To make this request please email DSPUHNM@uhnm.nhs.uk

It is also important to remember that no patient information is removed from Trust premises in the event of you leaving the employment of UHNM. All patient information remains the property of the Trust and it is only used for the stated purpose in line with the Data Protection Act 2018.

If it is found that clinicians have used and stored patient identifiable information in this way, disciplinary action may be taken or a report may be made to the Information Commissioners Office (ICO) for them to take action against the clinician as an individual.

Information Classification and Handling

Obligations regarding how a person deals with information depend on the nature of the information and its level of sensitivity. To help staff understand responsibilities, information within UHNM is categorised and defined as follows:

Public
Information in the public domain or designed for public use, i.e. Visible on the UHNM website.

Internal Use Only
Information that is not expected to be available to anyone outside the business e.g. internal communications, meeting minutes.

Restricted
Business critical or technically sensitive information likely to result in financial loss or serious harm.

Personal and Special Category
Person identifiable data (PID) - items of data concerning a data subject that, if used singly or in conjunction with other data items, could lead to identification of the data subject. Data items include (but are not limited to) name, address, photographs and clinical images, telephone and email contact details. Also includes rare/unique information about a person that could identify them, even if their name is not present.

UHNM uses Personal Data for the following broad purposes:

- Providing Direct Healthcare
- The general running and business administration
- On-going administration and management of Services to commissioners

UHNM will only process personal data where one of the following conditions applies:

- The Data Subject has given Consent to the Processing of their Personal Data for one or more specific purposes.
- Processing is necessary for the performance of a contract
- Processing is necessary for compliance with a legal obligation to which the Data Controller is subject to
- Processing is necessary in order to protect the vital interests of the Data Subject or of another natural person.
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller.
- Processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by a Third Party (except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject, in particular where the Data Subject is a child).

UHNM will only process special categories of data where one of the following conditions applies:

- Processing is necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement
- Processing is necessary to protect the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent
- Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent
- Processing relates to personal data manifestly made public by the data subject
- Processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity
- Processing is necessary for reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards
- Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care system/services and services on the basis of Union or Member State law or a contract with a health professional
- Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices
- Processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes

Data Retention

To ensure fair Processing, Personal Data will not be retained by UHNM for longer than necessary in relation to the purposes for which it was originally collected, or for which it was further processed.
The length of time for which UHNM need to retain Personal Data will be in accordance with national guidance. This takes into account the legal and contractual requirements, both minimum and maximum, that influence the retention periods set forth in the schedule.

UHNM will adopt physical, technical, and organisational measures to ensure the security of Personal Data. This includes the prevention of loss or damage, unauthorised alteration, access or Processing, and other

risks to which it may be exposed by virtue of human action or the physical or natural environment.

The minimum set of security measures to be adopted by UHNM is provided in the Information Security Policies. (IT01 & IT02).

Data Subject Requests
Data Subjects are entitled to obtain information held about them by UHNM, following a written request to the Trust via the Subject Access Team or HR department.

Personal Data Requests
Under the DPA 2018, data subjects have the right to access any and all information that an organisation holds about them. This includes e-mails and other data stored on the Trust network. To differentiate between a Subject Access Request relating to information held in a medical record (dealt with by Ministries) or information held about an employee held in a Personnel Record (dealt with by the H.R. team), requests for e-mails and other data stored on the Trust network are managed by the Data Security & Protection team and are referred to as a Personal Data Request (dspuhnm@uhnm.nhs.uk).

Informing individuals / patients effectively about the use of their information
Patients must be made aware that the information they give may be recorded and may be shared, in order to provide them with their care or any other legitimate processes. It may also be used to support clinical audit and other work to monitor the quality of care provided.

In order to inform patients effectively, staff must:

- Check where practicable that patients have received, read and understood relevant Trust patient information leaflets
- Make clear to patients the purpose of the health record and why and how the information is recorded
- Make clear to patients when Trust staff are or will be disclosing information to others and who these others may be.
- Check that patients are aware of the choices available to them in respect of how their information may be disclosed or used and emphasise that withholding their consent will not affect their healthcare or treatment
- Check that patients have no concerns or queries about how their information is disclosed and used
- Where possible, answer any queries personally or direct the patient to others who can answer their questions. In cases where staff are unsure of any aspect of confidentiality or for any advice on confidentiality, they should contact the Data Security & Protection team whose contact details will be available in the IG manual.
- Respect the rights of patients and facilitate them in exercising their right to have access to their health records
- Obtain and document Patient consent where necessary.

Data Protection by Design
To ensure that all Data Protection requirements are identified and addressed when designing new systems, services or processes and/or when reviewing or expanding existing systems, services or processes, each of them **MUST** go through a review and approval of the data impact prior to commencement process before continuing.

UHNM must ensure that a Data Protection Impact Assessment (DPIA) is conducted, in corporation with the DSP Team and the DPO, for all new and/or revised systems or processes for which it has responsibility. Once approved by the DPO, the DPIA and all associated documentation must be formally approved/signed off by the SIRO and the Caldicott Guardian, before the project can proceed.

Where applicable, the Information Technology (IT) department, as part of its IT system and application design review process, will cooperate with the DSP Team to assess the impact of any new or reused technology uses on the security of Personal Data.

Sharing/Transfers to Third Parties
UHNM will only transfer Personal and / or special category Data to, or allow access by, Third Parties when it is assured that the information will be processed legitimately and protected appropriately by the recipient. Where Third Party Processing takes place, UHNM will first identify if, under applicable law and regulations, the Third Party is considered a Data Controller or a Data Processor of the Personal Data being transferred.

Where the Third Party is deemed to be a Data Controller, UHNM will enter into, an appropriate sharing agreement with the Controller to clarify each party's responsibilities in respect to the Personal Data being shared or transferred. Where the Third Party is deemed to be a Data Processor, there must be a contract that requires the Data Processor to protect the Personal Data from further disclosure and to only process Personal Data in compliance with conditions set out in the contract.

Contracts and agreements will require third parties to implement appropriate technical and organisational measures to protect the Personal Data as well as procedures for providing notification of Personal Data Breaches.

Contracts must only be entered into with the involvement of the procurement and Data Security & Protection teams.

Sharing agreements must only be entered into with the Data Security & Protection team and signed off with approval from SIRO or Caldicott Guardian.

It should be noted, however, that a Memorandum of Understanding cannot be considered to be an Information Sharing Agreement and must, therefore, be viewed alongside the appropriate Sharing Agreement documentation.

Complaints Handling
Data Subjects with a complaint about the Processing of their Personal Data, should contact the PALS or Complaints Team in the first instance, If the processing of Personal Data was identified as part of and includes a health care complaint then the PALs or Complaints teams will carry out an investigation to the extent that is appropriate based on the merits of the specific case. PALS or Complaints will inform the Data Subject of the progress and the outcome of the complaint within a reasonable period.

If the issue cannot be resolved through consultation between the Data Subject and The Trust, then the Data Subject may, at their option, complain to the Information Commissioner's Office

Breach Reporting
Staff must report incidents via the Datix system and/or immediately escalate to the DSP team where the incident is deemed serious, in line with Trust policy. (Policy No (RM07) Trust Policy for Reporting and Management of Incidents including SIRI and STEIS Reportable Incidents.

Incidents will be reviewed and investigated as necessary in line with Trust policy (Policy No (RM07) Trust Policy for Reporting and Management of Incidents including SIRI and STEIS Reportable Incidents.

Service Evaluations/Audit
Staff may have a need to conduct service evaluations or audits to demonstrate the effectiveness of UHNM services upon patient care. Before any service evaluation or audits take place, they must be approved by the Data Security and Protection Team by emailing the request to DSPUHNM@uhnm.nhs.uk, where the requester will be asked to complete a screener detailing the purpose and process of the proposed activity. Once approval is given, the DSP team will register the service evaluation/audit with UHNM's audit team.

APPENDIX 2: MINIMUM HANDLING REQUIREMENTS

Classification		Appendix 2 - Minimum Handling Requirements			
Name	**Definition**	**Access Restriction**	**Transmission**	**Storage**	**Disposal**
Public	Information that is in or designed to be in the public domain – e.g. public website content, marketing materials, catalogues, brochures, leaflets. Also case law, commentary and other readily available public information.	None	• No restrictions	• No restrictions	• No restrictions – items can be recycled
Internal Use Only	Information that is not expected to be available to anyone outside the business e.g. internal communications, Employee Handbook, policies and procedures, some project reports (containing no patient information), operational KPIs, unused branded material including pre-printed letter head paper.	All Employees and any authorised 3rd parties.	• Email – check recipient • Post – external with consideration to readership • Internal mail is appropriate • Be mindful of surroundings if reading in public • Verbal disclosure - be aware of your surroundings • E-fax – check e-fax number carefully • Copy – free to copy, take care regarding appropriate distribution	• Appropriate electronic file location • Put away after working hours • Portable encrypted device only • Remote working “off-line” on UHNM owned equipment only	• Secure bin disposal for shredding • Delete from network drive when no longer relevant • Disposal of electronic devices must be carried out by IT

Classification		Appendix 2 - Minimum Handling Requirements			
Name	**Definition**	**Access Restriction**	**Transmission**	**Storage**	**Disposal**
Personal Data & Special Categories of Personal Data	**Person identifiable data (PID)** - items of data that, if used singly or in conjunction with other data items, could lead to identification of the data subject. Including (but not limited to) name, address, photographs and clinical images, telephone and email contact details. Also includes rare/unique information about a person that could identify them, even if their name is not present. **Special Categories of Personal Data -** Those items of Personal Identifiable Data consisting of information about; racial or ethnic origin, political opinions, religion, trade union membership, genetic or biometric data , physical or mental health or condition, sexuality, the commission or alleged commission of any offence or any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings	Access must be granted in accordance to job roles. Authorised groups of employees and any authorised 3rd parties.	• Email – check recipient carefully. Can be sent internally where appropriate. Cannot be sent externally without suitable encryption • Electronic file transfer only when secure • Post externally - consider recorded delivery • Internal mail – only in sealed envelope marked with the individual's name or deliver personally • Be mindful of surroundings if reading in public • E-fax – confirm e-fax number, pre notify and confirm receipt • Verbal disclosure - Do not discuss in public • Copy/Print – only using "secure printing" where possible.	• Put away when work area is unoccupied • Locked away after working hours • Electronic storage in network file storage • Portable encrypted device only • Remote working "off-line" on UHNM owned equipment only	• Secure bin disposal for shredding • Delete from network drive when no longer relevant in line with retention requirements • Disposal of electronic devices must be carried out by IT

Classification		Appendix 2 - Minimum Handling Requirements			
Name	**Definition**	**Access Restriction**	**Transmission**	**Storage**	**Disposal**
Restricted	Business or technically critical information likely to result in financial loss or serious harm e.g. HR/payroll information, technical configuration data acquisition plans, due diligence materials, company structure change proposals. Information a 3rd Party has classed as restricted.	Access must be granted according to job role. Authorised individual employees on a need to know basis only and any authorised 3rd parties.	• Email – check recipient carefully. Can be sent externally where required, consider encryption • Electronic file transfer only when secure • Post externally, consider courier, recorded delivery, • Internal mail – sealed addressed envelopes or deliver any hard copy personally • Be mindful of surroundings if reading in public • Verbal disclosure – Do not discuss in public • E-fax – confirm e-fax number, pre notify and confirm receipt • Copy/Print – only using “secure printing”	• Locked away when work area is unoccupied or after working hours • Electronic storage in secure network file storage • Portable encrypted device only • Remote working “off-line” on UHNM owned equipment only	• Secure bin disposal for shredding • Delete from network drive when no longer relevant • Disposal of electronic devices must be carried out by IT