University Hospitals of Leicester NHS
NHS Trust

DATA PROTECTION AND CONFIDENTIALITY POLICY

Approved By:	Trust Board
Date of Original Approval:	27 March 2003
Trust Reference:	**A6/2003**
Version:	5
Supersedes:	4 – June 2020
Trust Lead:	Saiful Choudhury – Head of Privacy
Board Director Lead:	Andrew Carruthers – Chief Information Officer & Senior Information Risk Officer
Date of Latest Approval	11 January 2024 – Trust Board
Next Review Date:	**January 2027**

CONTENTS

REVIEW DATES AND DETAILS OF CHANGES MADE DURING THE REVIEW

December 2023-

- remove the statement from section 1 about it being a new policy
- update the references to DHSC, NHSE/I, DSP Toolkit EIMT and roles
- grammatical corrections to paragraph 3.4 and paragraph 4.8
- include a signpost to HELM training in the policy standard

KEY WORDS

Information Governance, Confidentiality, Security, Data Protection, SIRO, Caldicott Guardian, Privacy

1 INTRODUCTION AND OVERVIEW

1.1 The Data Protection Act 2018 (DPA) imposes obligations on the use of all personal data held by University Hospitals of Leicester (UHL), whether it relates to patients and their families, employees, complainants, contractors or any other individual who comes into contact with the organisation. This has implications for every part of the organisation. UHL also has a duty to comply with guidance issued by the Department of Health and Social Care (DHSE), the NHS England/ NHS Improvement, the specific requirements of the Data Security and Protection Toolkit (DSP) and guidance issued by professional bodies.

1.2 UHL and its employees are bound by a legal duty of confidentiality to all patients which can only be set aside to meet an overriding public interest, legal obligation,

or similar duty. The DPA applies to all staff, contractors and volunteers working for the Trust. UHL is a Data Controller, as defined in Section 1 of the DPA, and is obliged to ensure that all of the DPA requirements are implemented.

1.3 This policy sets out how UHL meets its legal obligations and requirements under confidentiality, Data Protection and information security standards. The chief requirements outlined in this Policy are based upon the DPA, which is the central piece of legislation covering security and confidentiality of personal information.

2 POLICY SCOPE –WHO THE POLICY APPLIES TO AND ANY SPECIFIC EXCLUSIONS

2.1 This policy covers all forms of information held by the Trust, including (but not limited to):

- Information about members of the public
- Non Trust employees on Trust premises
- Staff and Personnel information
- Organisational, business and operational information

This policy applies to all Trust employees and third parties responsible for the delivery of contracted NHS services on behalf of the organisation

3 DEFINITIONS AND ABBREVIATIONS

3.1 **Information Governance (IG);** IG is the organisational practice of managing information from its creation to final disposal in compliance with all relevant information rights legislation. IG is focused on ensuring that standards and services are introduced to ensure that Trust information is managed securely, compliant with legislation and available for access by both staff and external parties, including the public and regulators.

3.2 **Data Security & Protection Toolkit (DS&P Toolkit);** The Data Security & Protection Toolkit is an online self-assessment tool that allows organisations to measure their performance against the National Data Guardian's 10 data security standards. All organisations that have access to NHS patient data and systems must use this toolkit to provide assurance that they are practising good data security and that personal information is handled correctly.

3.3 **Senior Information Risk Owner (SIRO):** The SIRO is a nominated person (Executive or Senior Manager on the Executive IM&T Board) who is familiar with information risk and the organisations response to risk. The SIRO takes ownership of the organisation's information risk policy and acts as an advocate for information risk on the Executive IM&T Board who is also the Senior Information Risk Officer. The SIRO for the Trust is the Chief Information Officer for IM&T.

3.4 **Caldicott Guardian;** The Trust's Caldicott Guardian has a particular responsibility for reflecting patients' interests regarding the use of patient

identifiable information. They are responsible for ensuring patient identifiable information is shared in an appropriate and secure manner. The UHL Caldicott Guardian is the Medical Director.

3.5 **Data Controller;** is a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

3.6 **DPA:** Data Protection Act 1998

3.7 **GDPR**: General Data Protection Regulation

4 ROLES – WHO DOES WHAT

4.1 **Senior Information Risk Officer:** The Senior Information Risk Officer (SIRO) has executive board level responsibilities and reviews the Trust's IG processes and provides written advice to the Chief Executive on the content of the Trust's Annual Governance Statement in regard to information risk. The SIRO is the executive lead for this policy. The key responsibilities of the SIRO are:

To review the IG strategy and policy for implementing the policy within the existing Framework;

To assess the risk assessment process for information governance, including review of the annual information risk assessment to support and inform the Annual Governance Statement and compliance submissions including DS&P Toolkit;

To review and agree action/s in respect of identified IG work programme and associated information risks.

4.2 **Caldicott Guardian:** The Trust Caldicott Guardian has board level responsibilities for the Trust's Caldicott Function and enables a direct reporting line to the Trust Board and the appropriate governance committee. The Caldicott Guardian's main responsibility is to be responsible for protecting the confidentiality of service user information and enabling lawful and ethical information sharing. This links directly to IG executive lead and will require the IG Lead to liaise directly to discuss information sharing issues. The additional responsibilities of the Caldicott Guardian are;

- Ensuring that the Trust processes satisfy the highest practical standards for handling patient information in line with Caldicott Principles for information sharing;
- Advising on policy issues to update standards with regard to patient data;

- Advocating policy requirements at board level to protect patient interests.

4.3 **Executive Information Management and Technology Board:** The Trust Leadership Board is responsible on behalf of the Chief Executive for all matters relating to this policy including;

Developing, implementing and maintaining a IG strategy and associated standards, an implementation strategy including an annual work programme to provide assurance to the Trust that effective arrangements are in place;

Reporting to the SIRO on annual basis to clarify performance and risks issues identified during audit and training cycles for executive level consideration.

Directing the Privacy Programme Board annual work programme to deliver IG standards and services across the Trust.

4.4 **Trust IG Lead:** The nominated IG Lead is the Head of Privacy within the IM&T department. The Trust's Head of Privacy has responsibility for managing the overall co-ordination, publicising and monitoring of the Trust IG Framework. The Trust's IG Lead has specific responsibility for;

The development of the IG strategy and policy, procedure and guidance;

Leading training and audit strategies to raise IG standards and services;

Producing IG performance monitoring reports and submitting annual compliance assessments as required;

4.5 **Employees & staff working on behalf of the Trust:** All Trust employees, whether permanent, temporary or contracted, and students and contractors are responsible for ensuring that they are aware of the requirements incumbent upon them and for ensuring that they comply with these on a day to day basis. This policy requires all staff to understand the need;

To comply with all information standards;

To hold information securely and confidentially;

To obtain information fairly and efficiently;

To record information accurately and reliably;

To share information appropriately and lawfully.

All employees are required to undertake regular Trust mandatory training in IG to ensure that they are fully aware of their individual responsibilities and have the relevant knowledge to ensure compliance. Misuse of or a failure to properly safeguard information will be regarded as a disciplinary offence. This is an annual requirement and is available at https://uhlhelm.com/

4.7 **Policy and Guidelines Committee (PGC):** Policy and guidelines committee is responsible for reviewing and approving policies.

4.8 **Information Governance Steering Group:**
The Information Governance Steering Group is a committee accountable to the Board. Its purpose is to support and drive the broader information governance agenda and provide the Board with the assurance that effective information governance best practice mechanisms such as this policy are in place within the organisation

5. POLICY IMPLEMENTATION AND ASSOCIATED DOCUMENTS

5.1 To meet the managing DPC (Data Protection and Confidentiality) standards there are three key interlinked aims to the policy which will ensure the delivery of an effective policy framework:

- **Legal compliance;** The Trust aims to meet and exceed all compliance requirements relating to DPC. The Trust will undertake or commission annual assessments and audits of its compliance with legal requirements through the Data Security & Protection Toolkit and demonstrating compliance to all relevant healthcare standards.
- **Information security;** The Trust will promote effective confidentiality and security practice to its staff through policies, procedures and training. The Trust has established and maintains incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and security.
- **Openness;** Non-confidential information on the Trust and its services should be available to the public through a variety of media. The Trust will undertake or commission annual assessments and audits of its policies and arrangements for openness through the Information Governance Toolkit.

6 EDUCATION AND TRAINING REQUIREMENTS

6.1 The Trust is committed to the provision of IG training and education to ensure the workforce is informed, competent, prepared and possesses the necessary skills and knowledge to perform and respond appropriately to the demands of clinical care and service delivery.

6.2 The Trust has a mandatory training programme which includes maintaining awareness of IG, data protection, confidentiality and security issues for all staff. This is carried out by regular training sessions covering the following subjects:

- personal responsibilities;
- confidentiality of personal information;
- relevant IG Policies and Procedures;
- general good practice guidelines covering security and confidentiality;
- Records management.

6.3 All staff will be required to complete annual IG training (including data protection and confidentiality training) commensurate with their duties and responsibilities. All new starters will be given IG training as part of the Trust mandatory induction process. Additional training in these areas will be given to those who require it due to the nature of their job, for example for system administrators who required further data protection and information risk training. Go to https://uhlhelm.com/ for further information.

7 PROCESS FOR MONITORING COMPLIANCE

7.1 The Information Governance Lead will establish a performance management framework, reported through the Information Governance Steering Group on a monthly basis.

POLICY MONITORING TABLE

The top row of the table provides information and descriptors and is to be removed in the final version of the document

Element to be monitored	Lead	Tool	Frequency	Reporting arrangements Who or what committee will the completed report go to.
IG Training	Head of Privacy	HELM, DATIX	Monthly	IG Steering Group
DS&P	Head of Privacy	Data Protection and Security Toolkit	Monthly	IG Steering Group, Trust Leadership Team

8 EQUALITY IMPACT ASSESSMENT

8.1 The Trust recognises the diversity of the local community it serves. Our aim therefore is to provide a safe environment free from discrimination and treat all individuals fairly with dignity and appropriately according to their needs.

8.2 As part of its development, this policy and its impact on equality have been reviewed and no detriment was identified.

9 SUPPORTING REFERENCES, EVIDENCE BASE AND RELATED POLICIES

9.1 The Senior Information Risk Owner (SIRO) will direct the Head of Privacy to take actions as necessary to comply with the legal and professional obligations set out in the key national guidance issued by appropriate commissioning bodies in particular;

- The NHS Confidentiality Code of Practice
- NHS Records Management Code of Practice Part 2
- Care Record Guarantee

9.2 There are a number of policies and procedures within the Trust that should be read in conjunction with this document for a complete understanding of how the Trust is organised and the strategies in place to fulfil its obligations. The key documents are listed below:

- E-mail and Internet Access and Monitoring Policy A9/2003
- Policy for the Retention of Records B10/2004

10 PROCESS FOR VERSION CONTROL, DOCUMENT ARCHIVING AND REVIEW

10.1 This policy will be communicated through clinical management groups (CMG's) and directorate management structures for cascade dissemination and implementation. It will also be communicated through promotional campaigns.

10.2 This policy will be reviewed every three years (or sooner if new legislation, codes of practice or national standards are to be introduced). The Policy and Guidelines Committee is responsible for reviewing and approving policies.