University Hospitals of Leicester NHS
NHS Trust

# INFORMATION GOVERNANCE POLICY

| | |
|---|---|
| **Approved By:** | Trust Executive |
| **Date of Original Approval:** | **25th February 2004** |
| **Trust Reference:** | **B4/2004** |
| **Version:** | 6 |
| **Supersedes:** | 5 – June 2020 Policy and Guideline Committee |
| **Trust Lead:** | Saiful Choudhury – Head of Privacy |
| **Board Director Lead:** | Andrew Carruthers – Chief Information Officer & Senior Information Risks Owner |
| **Date of Latest Approval** | 27 October 2023 – Policy and Guideline Committee |
| **Next Review Date:** | **December 2026** |

## CONTENTS



## REVIEW DATES AND DETAILS OF CHANGES MADE DURING THE REVIEW

This policy is put into place to develop the support for the Data Security & Protection Toolkit.

2023 review - EIMT replaced with The Trust Leadership Team.

Policy links updated

Roles section updated

Audit table updated to include Information Audits

## KEY WORDS

Information Governance, Confidentiality, Security

## 1 INTRODUCTION AND OVERVIEW

1.1 Information is a vital asset, both in terms of the clinical management of individual patients and in the management of services and resources. However, it is of paramount importance that any information relating to services, patients and employees is dealt with legally, securely, efficiently and effectively in order to deliver the best possible care.

1.2 Information Governance is an organisational discipline that combines policy standards and supporting procedures to ensure all aspects of information processing and handling are of the highest standards. Information Governance (IG) is therefore the key approach used by the Trust to ensure its information is managed to the highest standards.

1.3 IG aims to provide the policy framework which will enable the Trust to meet all legal requirements, improve information security and build information skills to ensure that the handling of information is undertaken to the highest standards.

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

2.1 This policy covers all forms of information across all media 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

2.2 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 **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. At UHL the Caldicott Guardian is the Medical Director.

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 orgnanisations 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 **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.

3.4 **Information Governance Steering Group;** The Information Governance Steering Group is a standing 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 are in place within the organisation

3.5 **Senior Information Risk Owner (SIRO);** The SIRO is a nominated person (Executive or Senior Manager on the Board) who is familiar with information risk and the organisations response to risk. The SIRO takes ownership of the organisation's information governance policy including all information risk and acts as an advocate on the Board. At UHL the Chief Information Officer is the SIRO.

3.6 **GDPR**: General Data Protection Regulation

## 4 ROLES – WHO DOES WHAT

4.1 **Senior Information Risk Officer and Executive Lead**: 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 key responsibilities of the SIRO are:

- To review the IG strategy, implementing the policy within the existing Framework including the Information Security Management System (ISMS);
- 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 IG & DS&P Toolkits;
- 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 **The Trust Leadership Team**

The Trust Leadership Team 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.

4.6 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/

## 5. POLICY IMPLEMENTATION AND ASSOCIATED DOCUMENTS –WHAT TO DO AND HOW TO DO IT

### Complying with Information Standards

5.1 The Trust will annually assess its performance against the requirements set out for Acute Trusts in the Data Security & Protection Toolkit (DS&P Toolkit) issued by NHS Digital. The Trust will report the results of its self-assessment to the Department of Health and Social Care in accordance with current guidance in the DS&P Toolkit.

5.2 The Trust will follow a program of continual improvement to increase IG compliance in the Trust year on year, providing regular performance reports to the IG Steering Group.

5.3 The IG Lead will also establish and maintain mechanisms through which departments and other units can manage business information to the highest standards to ensure that all security and compliance standards are maintained.

### Managing Security and Confidentiality

5.4 This policy requires all staff to manage information to the highest standards to ensure compliance with appropriate standards, to secure all Trust information and to promote appropriate information access. This will require all staff to manage information including patient identifiable data with due regard to security and confidentiality regulations.

5.5 The Trust regards all personal confidential data relating to service users and limited sensitive staff information as confidential. Individuals must be made aware of their responsibilities at local induction and through policy and training.

5.6 Failure to manage information securely including failure to protect confidentiality may result in disciplinary action.

5.7 The Trust will establish, develop and maintain policies and procedures for the effective and secure management of its key information assets and resources including the introduction of information classification and security schemes. Risk assessment, in conjunction with overall priority planning of organisational activity will be undertaken to determine appropriate effective and affordable information governance controls.

5.8 The Trust will promote effective confidentiality and security practice to its staff through policies, procedures and training and establish and maintain incident reporting procedures. It will monitor and investigate all reported instances of actual or potential breaches of confidentiality and security.

5.9 The Trust requires all its staff to ensure that all measures are taken to protect personal confidential data both manual and electronic e.g. locking away information, using passwords to log on to systems, only storing information on secure networks.

5.10 Staff non-compliance with legal requirements as defined in this policy will be monitored and managed through the Trust disciplinary procedure.

5.11 All breaches, actual or suspected, will be reported to, and investigated by IM&T via Datix. IM&T will document the incident and where necessary will report the findings of these investigations to the IG Steering Group.

### Sharing Information Appropriately and Lawfully

5.11 The Trust will undertake lawful sharing of information between the Trust, other NHS and partner organisations to support patient care as determined by law, statute and best practice. This will be based on securing clear legal basis and monitoring of ethical requirements of sharing of data including limiting processing and regularly reviewing sharing arrangements. Sharing with third parties is authorised by a number of information rights statutes and this should be done in line with the requirements of information sharing procedures.

## 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 Cyber Security / Data Protection training (including IG 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 uhlhelm.com for further information.

6.4 **Level 2 and Level 3 Training**

Level 2 - To provide staff with an in-depth knowledge on how to protect personal data in line with GDPR. All Staff within the Trust must complete this training: Unless you are Estates and Ancillary Staff upto a Band 6, in which case you need to complete Level 1 only. Unless you are Admin and Clerical Staff who are Band 8 and above, in which case you need to do Level 3 only.

Level 3- This course is for colleagues who: 1) Are in a Non-Clinical position of 8a and above who have not done the Level 3 course previously OR 2) have just entered into a role (not necessarily at the above banding) where they are responsible/ authorise data leaving the Trust.

Both L2 and L3 training are part of the Statutory Mandatory Training and are undertaken annually.

## 7 PROCESS FOR MONITORING COMPLIANCE

### Policy Monitoring Table

| 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, DS&P Toolkit, DATIX | Annual | IG Steering Group |
| DS&P Toolkit | Head of Privacy | DS&P Online Toolkit | Annual | IG Steering Group |
| Regular information audits | Head of Privacy | DATIX | Quarterly | IG Steering Group |

7.1 The IG Lead will monitor performance via the Data Security & Protection Toolkit reported through the IG Steering Group.

7.2 The IG Lead will develop specific key performance indicators to monitor and assess IG performance in line with this policy statement. The officer will report on performance and risk issues to both the SIRO and Trust Leadership Team to ensure all significant risks and information incidents are reviewed and subject to follow-up action.

7.3 An annual report on IG in the Trust, based on all available relevant performance and risk information, shall be produced. To ensure compliance with this policy the report, together with performance against the key performance indicators, shall be reviewed annually by IG Steering Group and used to inform the development of action plans to remedy deficiencies and to inform future strategies.

7.4 Regular information audits will be recommended by Privacy Unit for departments in severe/multiple breaches in line with the NHS England best practice standards for IG. This will determine on-going risks and threats for review by the IG Steering Group and will determine policy guidance updates and additions to training programmes for IG champions.

## 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 IG Lead 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 Data Protection Act 2018;
- The Freedom of Information Act 2000; the responsibility lies with the Director of Corporate and Legal Affairs to ensure compliance is met
- The Common Law Duty of Confidentiality; and
- The NHS Confidentiality Code of Practice.

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:

Freedom of Information Policy A9/2004

Policy for the Retention of Records B10/2004

E-mail and Internet Access Monitoring Policy A9/2003

Policy for Documenting in Patients' Health Records B30/2006

Information Access Policy B19/2006

Information Security UHL Policy A10/2003

## 10 PROCESS FOR VERSION CONTROL, DOCUMENT ARCHIVING AND REVIEW

10.1 This policy will be communicated through clinical management groups (CMGs) and directorate management structures for cascade dissemination and implementation.

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 Guideline Committee is responsible for reviewing and approving policies.