Hertfordshire Partnership NHS
University NHS Foundation Trust

HPFT

Information Governance Policy

This policy aims to ensure that standards of information handling are met by the creation and maintenance of appropriate policies and guidelines.

HPFT Policy

Version	7
Executive Lead	Executive Director – Innovation and Transformation
Lead Author	Head of Information Governance and Compliance
Approved Date	23/05/2018
Approved By	Information Management & Technology/Information Governance Group
Ratified Date	23/05/2018
Ratified By	Information Management & Technology/Information Governance Group
Issue Date	31/05/2018
Expiry Date	31/05/2021
Target Audience	All staff who working within HPFT

Document on a Page

Title of document	Information Governance Policy		
Document Type	Policy		
Ratifying Committee	IM&T Senior Managers Meeting		
Version	**Approval Date**	**Review Date**	**Lead Author**
7	23/05/2018	31/05/2021	Head of Information Rights & Compliance
Staff need to know about this policy because (complete in 50 words)	All staff need to be aware of Information Governance and what it encompasses.		
Staff are encouraged to read the whole policy but I (the Author) have chosen three key messages from the document to share:	• Information Governance is everyone's responsibility; • YOU are responsible for your actions including ensuring that you are only accessing personal data appropriately in line with what is required in your job role • Staff should be aware of changes in Data Protection Legislation brought in under the General Data Protection Regulations (GDPR) in May 2018.		
Summary of significant changes from previous version are:	Annual Review Inclusion of Data Protection Legislation changes and GDPR		

Contents Page

PART 1 – Preliminary Issues:

1. Introduction

Hertfordshire Partnership University NHS Foundation Trust (HPFT) recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. The Trust fully supports the principles of corporate governance and recognises its public accountability, but equally places importance on the confidentiality of, and the security arrangements to safeguard, both personal information about service users, staff and commercially sensitive information. The Trust also recognises the need to share service user information with other health organisations and other agencies in a controlled manner consistent with the interests of the service user and, in some circumstances, the public interest.

The Trust believes that accurate, timely and relevant information is essential to deliver the highest quality health care. As such it is the responsibility of all staff to ensure and promote the quality of information and to actively use information in decision making processes. This policy outlines the interlinked strands within information governance and refers to the standards to be employed relating to this.

The 4 key interlinked strands to the information governance policy are:

- Information security
- Legal compliance
- Openness
- Quality assurance

From 25 May 2018 the EU General Data Protection Regulations (GDPR) comes into effect. This is being complemented with domestic legislation, which will become the new Data Protection Act (DPA). Until the new Act receives Royal Assent, this policy continues to refer to either the GDPR or the more generic term of 'new Data Protection legislation'.

Under GDPR, the data protection principles set out the main responsibilities for organisations. These six principles are:

1. Fairly, lawfully and transparently
2. For specified purposes
3. Using the minimum amount necessary
4. Accurately
5. For only as long as it is needed
6. Securely.

The GDPR provides the following rights for individuals:

1. Information about how their information is being processed
2. The rights to have access to their information
3. The right to rectification when information is wrong
4. The right to erasure when it is appropriate to do so
5. The right to restrict processing

6. The right to data portability
7. The right to object to processing
8. The right to appropriate decision-making.

In health and social care, there are six Caldicott Principles that organisations should follow to ensure that information that can identify an individual is protected and only used when it is appropriate to do so:

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

2. Objectives

The aim of the policy is as follows:

1. To ensure that standards of information handling are met through the development of policies that specifically show how information is:
   - Held securely and confidentially
   - Obtained fairly and efficiently
   - Recorded accurately and reliably
   - Used effectively and ethically
   - Disclosed or shared appropriately and lawfully
2. To promote and assist management audits
3. To ensure all employees are aware of their individual responsibilities
4. To ensure procedures are monitored for their effectiveness

Information is a vital asset clinically and for the efficient management of services, resources and performance. It is therefore important that an appropriately robust policy framework is in place. Information Governance and Data Security Awareness stipulates the way in which information, in particular Personal Identifiable Data (PID), should be handled. PID is:

- Personal information about identifiable individuals, which should be kept private
- The legal definition of personal and special categories of data
- Information 'given in confidence' and 'that which is owed a duty of confidence'.

Under the new Data Protection legislation, Personal Data is defined as:

[A]ny information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

And Special Categories of Personal Data is defined as:

[R]acial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation […].

Information Governance (IG) also enables the Trust to ensure that all confidential information is dealt with legally, securely and efficiently, in order to deliver the best possible care to its patients.

3. Scope

This Policy will apply to all Trust employees and to Non-Executive Directors.

4. Definitions

Information Asset - An Information Asset is a body of information, defined and managed as a single unit so it can be understood, shared and protected by the Trust

CQC - Care Quality Commission, regulate, inspect and review all health and adult social care services in England

NHSLA - The NHS Litigation Authority handles negligence claims and works to improve risk management practices in the NHS.

Data Protection & Security Toolkit - An online system which allows NHS organisations and partners to assess themselves against Department of Health Information Governance policies and standards. It also allows members of the public to view participating organisations' Toolkit assessments.

5. Duties and Responsibilities

Chief Executive

The Chief Executive as Accountable Officer of the organisation has overall accountability and responsibility for information governance and is required to provide assurance through the Statement of Internal Control that all risks, including those relating to information, are effectively managed and mitigated.

Board of Directors

The Board has responsibility for the management of all records created and held by the Trust. This is devolved through the management line to all staff employed by the Trust. The IM & T/IG Programme Group reports to the Executive Team on all aspects of information governance. The Trust also has responsibility for social care records as well as health care records.

The Executive Director for Innovation and Transformation has the lead responsibility for the Trust's Information Governance. Responsibilities include ensuring the management of care records, and the transfer of service user identifiable information, are correct and lawful.

Senior Information Risk Officer (SIRO)

Senior level ownership of information risk is a key factor in successfully raising the profile of information risks and to embedding information risk management into the overall risk management culture of the Trust. Senior leadership through the appointment of a Senior information Risk Owner (SIRO) demonstrates the importance of ensuring information security remains high on the Board agenda.

The SIRO is the Director for Innovation and Transformation and is expected to understand how the strategic business goals of the organisation may be impacted by information risks. The SIRO will act as an advocate for information risk on the Board and in internal discussions and will provide written advice to the Accounting Officer on the content of their annual Statement of Compliance (SIC) in regard to information risk. This role is supported by the Head of Information Governance & Compliance, the Risk Manager, Head of IM&T and the Caldicott Guardian, although ownership of the Information Risk Policy and risk assessment process will remain with the SIRO.

Information Asset Owners (IAO)

The Information Asset Owner (IAO) is a senior member of staff who is the nominated owner for one or more identified information assets of the organisation. It is a core IG objective that all Information Assets of the organisation are identified and that the business importance of those assets is established.

The IAO is expected to understand the overall business goals of the organisation and how the information assets they own contribute to and affect these goals. The IAO will therefore document, understand and monitor:

- What information assets are held, and for what purposes;
- How information is created, amended or added to over time;
- Who has access to the information and why.

Caldicott Guardian

The Director for Quality & Safety is the Trust's Caldicott Guardian responsible for ensuring that person identifiable clinical information is received, stored and used in line with the organisation's obligations to Data Protection Legislation, the Caldicott Principles (below) and the NHS Digital Data Protection & Security Toolkit.

The Caldicott Guardian must be made aware of all procedures that relate to the use of patient information.

Following the Caldicott2 Review, the Trust has ensured the relevant recommendations made as a result of the review have been embedded into the Trusts Information Governance policies; relevant audit results are reported to the Caldicott Guardian, IM&T/IG Programme Group. See section 1 for the Caldicott principles

Associate Director of Information Management & Technology (IM&T)
The Head of IM&T is responsible for identifying and arranging the implementation of any device configuration requirements that the organisation may need. This will enable compliance with NHS Information Governance standards and IT security policy and procedures.

Head of Information Rights & Compliance
The Head of Information Governance and Compliance has operational responsibility for Information Governance within the Trust. This role has responsibility for ensuring that the Trust complies with Information Rights Law, including Data Protection Legislation and Freedom of Information Act 2000. The Head of Information Rights and Compliance is the Trust's registered Data Protection Officer and is responsible for ensuring the management of all records and requests for access to health records are correct and lawful.

Information Rights & Compliance Team
The Information Rights & Compliance Team implements the Trusts Information Governance Strategy and raises awareness of the importance of Information Governance across the Trust. They report to the Head of Information Rights and Compliance.

Information Management & Technology/Information Governance (IM&T/IG) Programme Group
IM&T/IG Programme Group is responsible for overseeing the IM&T and IG work programme, policies, standards, procedures and guidance, coordinating and raising awareness of Information Governance within the organisation.

Information Management & Technology Management Meeting
This Group acts as a sub group of the Information Management & Technology/Information Governance Programme Group. It will ensure alignments are made between IM&T and IG issues and the Trust's IM&T strategy.

Change Advisory Board (CAB)
The Change Advisory Board (CAB) is an authoritative and representative group of people who are responsible for assessing, from both a business and a technical viewpoint, all high impact Requests for Change (RFCs). All IM&T related change requests are reviewed by the CAB who will ensure that standardised methods and procedures are used for efficient and prompt handling of all Changes, in order to minimise the impact of Change related incidents upon service quality. The CAB will escalate any issues that are unable to be resolved within the Change Management process to the Senior IM&T management group where appropriate.

Managers and Staff
Individual members of staff and staff teams are accountable for:

- The content of records they make
- ensuring records meet the standards set by the Trust

- maintaining confidentiality of records/information
- safe storage of records
- ensuring they access training with regard to record keeping and maintenance

Part 2 – What needs to be done and who by

6. Information Security

- The Trust has established and maintains policies for the effective and secure management of its information assets and resources.
- The Trust will undertake or commission annual assessments and audits of its information and IT security arrangements, by means of penetration tests carried out by Hertfordshire Bedfordshire and Luton ICT Services (HBL ICT) who work to the requirements of the Data Protection & Security Toolkit. All results are fed to the HBL ICT Security Forum and notified to AD IM&T as appropriate.
- The Trust promotes effective confidentiality and security practice to its staff through policies, procedures and training.
- The Trust has established and maintains incident reporting procedures, monitors and investigates all reported instances of actual or potential breaches of confidentiality and security.

7. Openness and Transparency

The Trust recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. Information will be defined and where appropriate kept confidential, underpinning the Caldicott Principles and the regulations outlined in Data Protection Legislation.

- Service users have appropriate ready access to information relating to their own care, their options for treatment and their rights as service users.
- Non-confidential information on the Trust and its services is available to the public through a variety of media, in line with the Freedom of Information Act 2000.
- The Trust has established and maintains policies to ensure compliance with the Freedom of Information Act 2000.
- The Trust has clear procedures and arrangements for liaison with the press and broadcasting media.
- The Trust has clear procedures and arrangements for handling queries from service users and the public.

8. Legal Compliance

- The Trust regards all identifiable personal information relating to service users and staff as confidential except where national policy on accountability and openness require otherwise. Compliance with legal and regulatory frameworks will be achieved, monitored and maintained and the organisation will establish and maintain policies and procedures to ensure compliance with Data Protection Legislation, Human Rights Act 1998, the Common Law Duty of Confidentiality and the Freedom of Information Act 2000. The organisation will establish and maintain policies for the controlled and appropriate sharing of service user's information with other agencies, taking account of any relevant legislation.
- The Trust will undertake or commission annual assessments and audits of its compliance with legal requirements for example the Information Governance Annual Audit, Care Records Management and Corporate Records Audits.

9. Information Quality Assurance

The Trust will establish and maintain policies and procedures for information quality assurance and the effective management of all records held

- The Trust will undertake or commission annual assessments and audits of its information quality and records management arrangements
- Managers are expected to take ownership of, and ensure that the quality of information within their services meets Trust standards
- Wherever possible, information quality should be assured at the point of collection
- Data standards will be set through clear and consistent definition of data items, in accordance with national standards.
- The Trust will promote information quality and effective records management through policies, procedures/user manuals and training

10. Training

Training and staff awareness is a vital component of Information Governance; with appropriate training HPFT can be assured that employees are adequately informed how to:

- Respect service user's information rights.
- Use personal information appropriately and legally.
- Create, file and store corporate records in line with the best practice records management standards.
- Share good practice ideas across departmental boundaries and avoid duplication through shared efforts
- Seek assistance if required.

Training on the content and management of records is part of the annual mandatory training plan and is included in the induction programme for new staff.

The training is offered to all staff through Oracle Learning Management (OLM), this allows staff to complete their training through e-learning.

Course	For	Renewal Period	Delivery Mode
Data Security Awareness Training	All Staff	Annually	E-Learning and Face to Face
Care records and Confidentiality Training	Managers and Clinicians	Every 3 years	E-learning

11. Embedding a culture of Equality & RESPECT

The Trust promotes fairness and RESPECT in relation to the treatment, care & support of service users, carers and staff.

RESPECT means ensuring that the particular needs of ‘protected groups’ are upheld at all times and individually assessed on entry to the service. This includes the needs of people based on their age, disability, ethnicity, gender, gender reassignment status, relationship status, religion or belief, sexual orientation and in some instances, pregnancy and maternity.

Working in this way builds a culture where service users can flourish and be fully involved in their care and where staff and carers receive appropriate support. Where discrimination, inappropriate behaviour or some other barrier occurs, the Trust expects the full cooperation of staff in addressing and recording these issues through appropriate Trust processes.

RULE: Access to and provision of services must therefore take full account of needs relating to all protected groups listed above and care and support for service users, carers and staff should be planned that takes into account individual needs. Where staff need further information regarding these groups, they should speak to their manager or a member of the Trust Inclusion & Engagement team.

12. Process for monitoring compliance with this document

The Trust is responsible to review/monitor of all the requirements for Information Governance within the NHSLA Standards/Care Quality Commission (CQC) Standards and Information Governance Toolkit:

Key process for which compliance or effectiveness is being monitored	Monitoring method (i.e. audit, report, on-going committee review, survey etc.)	Job title and department of person responsible for leading the monitoring	Frequency of the monitoring activity	Monitoring Committee responsible for receiving the monitoring report/audit results etc.	Committee responsible for ensuring that action plans are completed
Check policy for compliance with the Data Protection & Security Toolkit	Annual Review	Information Governance Manager	Yearly	IM&T/IG Programme Group and Policy Panel	IM&T/IG Programme Group and Policy Panel
The Trust will undertake independent Internal Audit of IG Requirements	Annual Internal Audit	Head of Information Governance and Compliance	Yearly	Integrated Governance Committee	Integrated Governance Committee

Information Governance and Compliance Team have responsibilities for conducting the care records and corporate records monitoring/audit on a rolling basis	Audit	Head of Information Governance and Compliance	Yearly	IM&T/IG Programme Group	IM&T/IG Programme Group
Information Governance and Compliance Team have responsibility for conducting spot checks to ensure service user records are being appropriately accessed.	Audit	Head of Information Governance and Compliance	Monthly	IM&T/IG Programme Group	IM&T/IG Programme Group
The Information Governance and Compliance Team will undertake periodic spot checks with regard to information security	Spot Checks	Head of Information Governance and Compliance	Spot Checks	IM&T Management Meeting and IM&T/IG Programme Group	IM&T Management Meeting and IM&T/IG Programme Group
The Trust through the Information Governance Lead has a robust action plan to demonstrate year on year improvements	Action Plans	Head of Information Governance and Compliance	Yearly	IM&T/IG Programme Group and Executive Team	IM&T/IG Programme Group and Executive Team

The IM&T/IG Programme Group is responsible for ensuring that Information Governance is embedded within the organisation	Audits and Action Plans	Head of Information Governance and Compliance	On Going	IM&T/IG Programme Group and Executive Team	IM&T/IG Programme Group and Executive Team

Part 3 – Document Control & Standards Information

13. Version Control

Every procedural document must have a version control table showing the current version and previous versions to aid tracking and ensure that staff are working to the current document.

A Full Review results in the reviewed version becoming the next whole number e.g. Version 2.

An Interim Update where minor changes are made takes the next part number e.g. Version 2.1.

The date and the author, together with the current version number, following the rules above, are also stated on the front cover once ratified and this published version remains live until the next new version is published.

The full date the new version is published is noted in the document's version control table and the superseded document is taken off the Policy Website, as of that date to be archived and listed on the Archive Database.

Version control for the Procedural Document Management System

Version	Date of Issue	Author	Status	Comment
Version	**Date of Issue**	**Author**	**Status**	**Comment**
V2, Draft 1	11 June 2007	Head of Information and Access to Records	Superseded	Updated strategy and policy to reflect changes in reporting system Sent to J Hepburn for comments and to add implementation plan 2007/08
V2, Draft 1	2 Oct 2007	Head of Information and Access to Records	Superseded	Agreed at Workforce & Organisational Development Group
V2	30 Oct 2007	Head of Information and Access to Records	Superseded	Signed off by Exec Team
V2.1 draft	25th Jan 2009	Information Governance Officer	Superseded	Currently draft
V2.1	26th May 2009	Information Governance Officer	Superseded	Signed off by Exec Team
V3	June 2010	Information Governance Officer	Superseded	Annual Review
V3	24 June 2010	Information Governance	Superseded	Ratified by IG&R Group

		Officer		
	8th July 2010	Information Governance Officer	Superseded	Ratified by WODG
V3.1	13th July 2010	Information Governance Officer	Superseded	Minor Changes to Duties
V3.2	20th July 2010	Information Governance Officer	Superseded	Ratified by Exec, uploaded to Trustspace
V3.3	March 2011	Information Governance Officer	Superseded	Amendment following Internal Audit
V3.3	March 2011	Information Governance Officer	Superseded	Ratified by IG&R,
	May 2011	Head of Information and Access to Records	Superseded	EIA Approved 9/5/2011
V4	May 2012	Head of Information and Access to Records	Superseded	Annual Review Approved by IG&R Group 12th July 2012
V5	10th March 2014	Head of Information Management and Compliance	Superseded	Annual Review Approved by IM&T/IG Programme Group
V6	3rd February 2015	Senior Information Governance Analyst	Superseded	Annual Review
V6.1		Senior Information Governance Analyst	Superseded	Six month review
V6.2		Information Governance Manager	Superseded	Annual Review
V6.3	Dec 2016	Senior Information Governance Officer	Superseded	Annual Review
V7	May 2018	Interim Head of Information	Current	GDPR Review

		Rights & Compliance		

14. Relevant Standards

a) Data Protection & Security Toolkit Requirements
b) Care Quality Commission (CQC)
c) NHSLA
d) **Equality and RESPECT:** The Trust operates a policy of fairness and RESPECT in relation to the treatment and care of service users and carers; and support for staff.

15. Associated Documents

- Access to Personal Records Policy
- Care Records Management Policy
- Corporate Records Management Policy
- Confidentiality Statement
- CPA Integrated Care Programme Approach and Care Management
- Data Quality Policy
- Data Protection Impact Assessment Policy
- Information Risk Policy
- Information Security Policy
- Learning from Incidents Policy
- Freedom of Information Act 2000 Policy & Procedure
- Protection and Use of Service User Information Policy
- Written & Electronic Communications Policy
- Social Media Policy

16. Supporting References

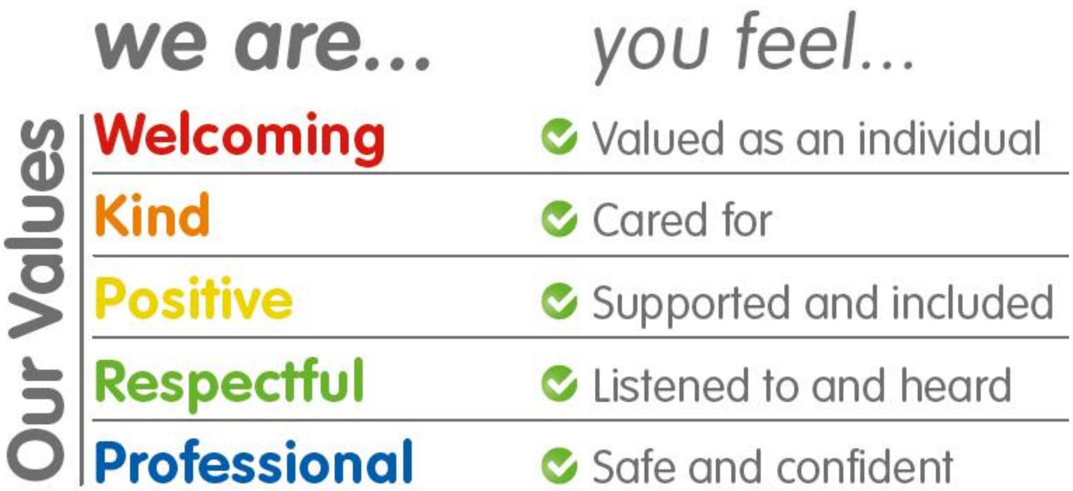
Information Governance is the framework which brings together all of the requirements, standards and best practice that apply to the handling of electronic information. The areas that are included within Information Governance are:

- NHSDigital: What You Should Know About Information Governance Booklet
- DH:Guidance for NHS Boards – Information Governance
- Report of the Caldicot2 Review – Information: To share or not to share? The Information Governance Review
- Data accreditation and data quality
- Consent to sharing of personal information
- ISO27001 – Information security management
- Common law duty of confidentiality
- Data Protection Legislation
- Records Management
- The Freedom of Information Act 2000
- Human Rights Act 1998 (Article 8)
- Professional Standards
- The Access to Health Records Act 1990

17. Consultation

Approval and ratification process for this document by IM&T/IG Programme Group and HPFT Policy Panel.

Job Title of person consulted for initial Policy	
IM&T/IG Programme Group	Caldicott
Head of Infrastructure HBLICT	SIRO
IM&T Managers	Head of Information Rights and Compliance
Service Line Leads	Trust Risk Manager
HR Manager	Information Governance Manager
	Senior Information Governance Officers



Our Values

we are...	you feel...
Welcoming	✓ Valued as an individual
Kind	✓ Cared for
Positive	✓ Supported and included
Respectful	✓ Listened to and heard
Professional	✓ Safe and confident

Our ✓alues

Welcoming Kind Positive Respectful Professional