Frimley Health NHS
NHS Foundation Trust

Policy

Information Governance policy

Key Points

- Information is a vital asset, both in terms of the clinical management of individual patients and the efficient management of services and resources throughout the Trust. It is therefore of paramount importance that information is efficiently managed, and that appropriate policies, procedures and management accountability provide a robust governance framework for information management.

- The Trust will ensure that Information Governance (IG) is embedded in all Trust activities or processes.

- The Trust will deploy a series of IG policies, supported by procedures, standards or guidelines to ensure its information is secure and managed in accordance with all relevant legislation and standards.

Version:	1.0
Role of Policy Lead(s):	
Role of Executive Lead:	Director of Finance
Name of Responsible Committee:	Information Governance Committee
Date Approved by Responsible Committee:	April 2015
Date Approved by Policy Review Group:	(scheduled but not yet approved)
Date Issued:	October 2015
Review Date:	October 2018
Target Audience:	All staff
Key Words & Phrases:	Information Governance

Version Control Sheet

Version	Date	Policy Lead(s)	Status	Comment
1.0	01/07/2015	Nicola Gould	Draft	New Policy following acquisition

Document Location

Document Type	Location
Electronic	Policy Hub (Trust-wide)
Paper	Information Governance Department, Tower Block, Wexham Park Hospital
Paper	Information Governance Department, Frimley Park Hospital

Related Documents

Document Type	Document Name
Code of Conduct	Department of Health Confidentiality Code of practice
Policy	Information Security Policy
Policy	Email Policy
Policy	Freedom of Information Policy
Policy	Clinical Records Management Policy
Policy	Data Quality Policy
Policy	Data Protection and Confidentiality Policy
Policy	Non - Clinical Records Management Policy
Strategy	Information Governance Strategy
Strategy	Records Management Strategy

Contents

Page No

1. Introduction **4**

2. Scope of the Policy **4**

3. Definitions **5**

4. Purpose of the Policy **5**

5. The Policy **5**

6. Duties / Organisational Structure **7**

7. Raising Awareness / Implementation / Training **8**

8. Monitoring Compliance of Policy **8**

9. References **9**

10. Appendices **9**

Appendix A **9**

1. Introduction

1.1 Information is a vital asset, both in terms of the clinical management of individual patients and the efficient management of services and resources throughout the Trust. It plays a key part in clinical governance, service planning and performance management. It is therefore of paramount importance that information is efficiently managed, and that appropriate policies, procedures and management accountability provide a robust governance framework for information management. The Information Governance Committee oversees IG.

2.0 Scope of the Policy

2.1 This is an overarching policy setting out the principles of information Governance. It is supported by a framework of policies covering Confidentiality, Data Protection, Freedom of Information, Information Security, Data Quality and Records Management.

2.2 This policy covers the use and management of information in all formats., both paper-based and computerised information, including the collection, processing, storage, communication and disposal of information.

2.3 The policy applies to all employees and contractors working for, or supplying services, for the Trust.

2.4 There are four key interlinked strands to Information Governance which are:

- Openness
- Information Quality Assurance
- Information Security
- Legal and NHS compliance

3. Definitions

3.1 The Glossary of terms refers to terms which the user may find in any of the information governance documentation and can be found at Appendix A.

14.1.2 This list is dynamic and may be updated at any time to reflect changes in guidance or legislation.

4. Purpose of the Policy

4.1 This IG policy ensures the following primary objectives are achieved by the Trust:

- Information will be organised and managed in accordance with mandated and statutory standards and kept confidential where appropriate
- Ensure staff understand their own responsibility regarding Information Governance
- Compliance with legal and regulatory frameworks will be achieved, monitored and maintained.
- All information risks will be identified and mitigated and where necessary serious risks will be added to the Corporate Risk Assurance Framework.

5. The Policy

5.1 Principles

5.2 There is a fine balance between openness and confidentiality in the management and use of information and the Trust recognises the principles of corporate governance and public accountability.

5.3 The importance of confidentiality, security and data quality play in the role of safeguarding information within the Trust cannot be overstressed. These include patient and staff information as well as commercially sensitive information. The Trust has agreements to share patient information with other healthcare organisations and other agencies in a controlled manner, which ensure the patients and public interests.

5.4 It is essential that accurate, timely and relevant information is recorded and is essential to deliver the highest quality healthcare. As such it is the responsibility of ALL staff to promote data quality and confidentiality.

5.5 Openess

5.6 Non confidential information on the Trust and its services should be available to the public through a variety of media in line with the Freedom of Information Act 2000.

5.7 Patients have ready access to information relating to them under the Data Protection Act 1998. This includes both facts and opinions.

5.8 Procedures and arrangements are in place for handling requests and queries from patients and the public under the Data Protection Act 1998, the Freedom of Information Act 2000 and the Environmental Information Regulations 2004.

5.9 Information Quality Assurance

5.10 Information Quality is an important part of the Information Governance agenda in terms of data quality and integrity. Quality is generally defined as ‘fit for purpose’ and all staff need to ensure that data is relevant and accurate.

5.11 Good quality data means that data is recorded in full, as accurately as possible and in a timely manner. Timely data entry will help avoid discrepancies and inaccuracies. Where it is not possible to enter data in real time this data should be recorded as soon after the event as possible.

5.12 Data should not be duplicated unless absolutely necessary and this fact should be recorded with the original data. If duplicated the data owner must ensure that all copies of the data are kept up to date and synchronised.

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

5.14 The Trust will undertake or commission regular assessments and audits of its information quality and records management arrangements.

5.15 Managers will take ownership of, and seek to improve, the quality of information within their services.

5.16 Wherever possible, the member of staff responsible for recording information should ensure the quality and accuracy of that information.

5.17 Data Standards will be set, or adopted, through clear and consistent definition of data items, in accordance with NHS standards.

5.18 The Trust will promote information quality and effective records management through policies, procedures and guidelines.

5.19 Information Security

5.20 Information Security is the responsibility of mangers and staff to ensure they follow guidelines and best practice. The Trust maintains an Information Security Policy that sets out, in detail, everyone's responsibilities and best practice for the management of the Trust's IT Systems and information assets.

5.21 As part of its overall information security practices the Trust will develop an Information Security Management System for the effective and secure management of its information assets and resources.

5.22 The Trust will undertake or commission regular assessments and audits of its information security procedures and practices.

5.23 The Trust will promote effective confidentiality and IT security practices to its staff through policies, procedures and training.

5.24 The Trust will establish and maintain incident reporting procedures and will monitor and investigate all reported instances of actual or potential threats and breaches of confidentiality and security.

5.25 Legal and NHS Compliance

5.26 The Trust regards all identifiable personal information relating to patients as confidential and the Trust will establish and maintain policies to ensure compliance with common law of confidentiality.

5.27 Personal information relating to staff is confidential, except where national policy on accountability and openness requires otherwise.

5.28 The Trust has established policies to maintain controlled and appropriate sharing of patient information with other agencies and will continue to monitor and establish new agreements when necessary. These agreements take into account relevant legislation as outlined in section XX.

5. Duties / Organisational Structure

5.14 Information Governance Committee

5.29 The Information Governance Committee is responsible for overseeing Information Governance issues, information risks and channels of accountability exist between this group and the Trust Board.

5.30 The progress on Information Governance issues will be reported to Trust Board by the Trust's Senior Information Risk Owner (SIRO) through the Information Governance Committee, on a quarterly basis. There is Directorate representation on the Information Governance Committee to ensure that Information Governance is embedded within the organisational structure.

5.31 The SIRO is the Chair of the Information Governance Committee with the Caldicott Guardian as the deputy Chair, both of these persons are Executive Directors on the Trust Board with responsibility for Information Governance.

5.32 In the absence of any Executive Directors, the Head of Performance and Planning may deputise for the Director of Finance.

6. Raising Awareness / Implementation / Training

6.11 Fundamental to the success of delivering the Information Governance is developing an Information Governance culture within the Trust. Awareness and training to all Trust staff, particularly those who utilise information in their day to day work, will promote this culture. The methods used to facilitate this are detailed in the Trust's Information Governance Strategy.

6.12 The Trust makes every effort to provide appropriate training and guidance on Information Governance issues. It is the responsibility of managers and staff to ensure they have adequate knowledge and access to appropriate resources.

6.13 The Trust has a slot at Trust induction for Information Governance and runs a mandated IG training sessions for all staff. Staff are mandated to attend IG training every year for an update refresher.

6.14 Important or new Information Governance issues and information are communicated via various Trust communication channels.

6.15 Information and documents relating to Information Governance will be made available on the Trust's Intranet site.

7. Monitoring Compliance of Policy

7.11 The Trust will monitor staff compliance against this policy through the monitoring of reported Trust incidents relating to breaches of confidentiality, loss of personal information.

7.12 This policy will be formally reviewed every three years. However, compliance with the IG Toolkit will be monitored on an ongoing basis and, if considered appropriate, a formal review may be prompted sooner.

8. References

8.11 The Trust is required to comply with the following legislation:

- Data Protection Act 1998
- Human Rights Act 1998
- Access to Health Records Act 1990
- Freedom of Information Act 2000
- Health and Social Care Act 2001
- Computer Misuse Act 1990
- Copyright Designs and Patents Act 1988
- Crime and Disorder Act 1998
- Electronic Communications Act 2000
- Regulation of Investigatory Powers Act 2000
- Public Interest Disclosure Act 1998
- Audit and Internal Control Act 1987
- National Health Service Act 1977
- Human Fertilisation and Embryology Act 1990
- Abortion Regulations 1981
- Prevention of Terrorism Act 2000
- Road Traffic Act 1988
- Mental Health Act 1983
- Children’s Act 1989
- Mental Capacity Act 2005

9. Appendices

9.11 Appendix A – Glossary of Terms

Appendix A – Glossary of Terms

Term	Definition
Access	Right, opportunity, means of finding using or retrieving information
Accessible Public Record	Records kept by a public body such as the Trust and covered by the Data Protection Act 1998.
Accountability	Principle that individuals, organisations, and the community are responsible for their actions and may be required to explain them to others
Action tracking	Process in which time limits for actions are monitored and imposed upon those conducting the business
Anonymised Data	Data from which the identity of an individual cannot be determined. Anonymisation requires the removal of name, address, full post code and any other detail or combination or details that might support identification.
Applicant	An individual requesting information from a public body
Audit	An examination of records or financial accounts to check their accuracy
Availability	The property of being accessible and usable upon demand by an authorised entity.
BC / DR	Business Continuity / Disaster Recovery
BCS	British Computer Society
BMA	British Medical Association
Browser	A software program that allows a user to interact with resources on the internet. Common browser programs include Internet Explorer, Mozilla Firefox and Netscape Navigator.
Business critical	An element of a process without which the remainder of the process cannot function.
Caldicott Committee	The name of the Committee formed to review the use of patient-identifiable information in the NHS. Named after its chairperson, Dame Fiona Caldicott.
Caldicott Guardian	A person, usually of Director level, to oversee the arrangements for the use and sharing of person-based clinical information.
Caldicott Principles	A set of principles to control the use or flow of patient-identifiable information
CCTV	Closed Circuit Television
Classification	Systematic identification and arrangement of business activities and/or records into categories according to logically structured conventions, methods and procedural rules represented in a classification system
Clinical Audit	The evaluation of clinical performance against set standards or though comparative analysis, with the aim of informing the management of services.

Term	Definition
Code of Practice	A set of documented procedures used by public bodies to ensure they comply with legislation. For example, the NHS code of confidentiality.
Common Law	A law which is determined by decisions made by the courts and can therefore change over time. A law set by precedents.
Confidentiality	The property that information is not made available or disclosed to unauthorised individuals, entities, or processes.
Confidential Information	Confidential information could include, without limitation details of: • Business Contacts, associates, list of suppliers and details of contract with them. • Identities of patients • Expenditure levels and Trust specific pricing policies • Proposal plans or specification for the development of existing services and of new services • Details of employees and officers of the Trust and of the remuneration and other benefits paid to them • Presentations, tenders, projects, joint ventures, mergers and developments contemplates, offered or undertaken by the Trust
Consent	Consent is the fact that permission has been given. A person who consents to something is, in effect, giving permission for that thing to happen.
Control	Means of managing risk, including policies, procedures, guidelines, practices or organisational structures, which can be of administrative, technical, management, or legal nature
Conversion / migration	Process of changing records from one medium to another or from one format to another
Data	collection of facts from which conclusions may be drawn; "statistical data"
Data Controller	This is the authority which defines the purposes for which personal data is processed. For our purposes the Trust is the data controller.
Data Processor	Any person (other than an employee of the data controller) who processes the data on behalf of the data controller
Data Protection Act 1998	UK wide legislation that governs the use of personal information. Its purpose is to protect the right of the individual. The Act laid down eight data protection principles
Data Protection Officer	The person within an organisation, in this case the Trust, who is responsible for compliance with the Data Protection Act 1998.
Data Protection Principles	The set of standards for good practice in information processing as defined in the Data Protection Act 1998. The Act laid down eight data protection principles.
Data Subject	An individual whose personal data is held by an organisation. For example, a data subject can be a patient but also a member of staff who's personal information is held by the Trust

Term	Definition
Destruction	Process of eliminating or deleting records, beyond any possible reconstruction
Disclosure	The release of personally identifiable data to a third party.
Disposition	Range of processes associated with implementing records retention, destruction or transfer decisions which are documented in disposition authorities or other instruments.
Document	Recorded information or object which can be treated as a unit
DPA	Data Protection Act 1998
DR / BC	Disaster Recovery / Business Continuity
DSCN	Data Set Change Notices
EIR	Environmental Information Regulations 2004
E-mail	Electronic mail communication, used for sending and receiving text messages and attached files
Explicit or Express Consent	This means the individual has articulated agreement either orally or in writing. Both terms are used to describe circumstances where a clear and voluntary preference or choice, is given. It must be given freely in circumstances where the available options and the consequences have been made clear.
Fair Processing	The first principle of the 1998 Data Protection Act is that personal data must be processed fairly and lawfully. In order to achieve this, patients must be made aware of, and consent to, the ways in which information about them may be collected and used.
FoI Act	The Freedom of Information (FoI) Act puts a legal requirement on organisations to publish and share information. From January 2005, FoI allowed members of the public, including the press, to access information stored by organisations.
FoI Officer	The person within a public body who is responsible for compliance with the Freedom of Information Act.
GMC	General Medical Council
Guideline	A description that clarifies what should be done and how, to achieve the objectives set out in policies
Guidelines	Procedural suggestions to achieve best practice
HORUS	An acronym representing rules for processing personal information. It means data must be: held securely & confidentially; obtained fairly and efficiently; recorded accurately and reliably; used effectively and ethically; shared appropriately and lawfully. There is a common school of thought that a second ‘S’ should be added to include ‘Shredding’ or ‘Deleting’ and that this should be done appropriately.
ICD-nn	International Statistical Classification of Disease and Related Health Problems, nnth Revision
ICT	Information and Communication Technology
Identifiable Data	Data items that can be used to identify an individual, also referred to as personal data or personal information.

Term	Definition
IM & T	Information Management and Technology
Indexing	Process of establishing access points to facilitate retrieval of records an/or information
Information	A collection of data with which the user can gain knowledge
Information Asset	Anything that has value to the Trust
Information Governance	A framework for handling information in a confidential and secure manner to appropriate ethical and quality standards
Information processing facilities	Any information processing system, service or infrastructure, or the physical locations housing them.
Information Security	Preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved
Information Security Event	An identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant.
Information Security Incident	A single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security
Information Security Management System. (ISMS)	That part of the overall risk management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security
Information Sharing Protocol	Documented rules and procedures for the disclosure and use of patient information between two or more organisations or agencies
Integrity	The property of safeguarding the accuracy and completeness of assets
Internet	A network of computers linked world wide to allow people to view, download and upload data. Referred to as ‘The Web’
Intranet	A network of computers linked in a private network that allows restricted access to a specified group of people. For example, NHSNET and the Trust’s own Intranet.
IPR	Intellectual Property Rights
ISEB	Information Systems Examination Board – an element of the BCS
ISO 17799	International Standard – Code of Practice for information security management
ISP	Information Sharing Protocol
IT	Information Technology
Knowledge	Information gained through the provision of information.
Manual Data/ Records	Information that is not processed by means of equipment. It is referred to in the Data Protection Act 1998 when defining a relevant filing system.

Term	Definition
Medical Purposes	As defined in the Data Protection Act 1998, medical purposes include but are wider than healthcare purposes. They include preventative medicine, medical research, financial audit and management of healthcare services. The Health and Social Care Act 2001 explicitly broadened the definition to include social care.
Migration / conversion	Act of moving records from one system to another, while maintaining the records' authenticity, integrity, reliability and useability.
NHS Code of Confidentiality	A guide to required practice for those who work within or under contract to NHS organisations concerning confidentiality and patients' consent to the use of their health records.
NHSLA	National Health Service Litigation Authority
NMC	Nursing Midwifery Council
OPCS n.n	Office for Population Censuses and Surveys (version number)
PbR	Payment by Results
Personal Data	Data concerning an individual. Personally-identifiable data is personal data from which the identity of the individual may be deduced.
Policy	Overall intention and direction as formally expressed by management
Preservation	Processes and operations involved in ensuring the technical and intellectual survival of authentic records through time
PRIMIS	PRIMary care Information Service
PRINCE2	PRojects IN a Controlled Environment – A widely accepted project management methodology.
Processing	This covers almost any use of data, including holding, obtaining, recording, using and sharing.
Pseudonymised Information	This is similar to anonymised information but the holder retains a means of identifying individuals; this will often be by attaching codes to information to allow linking of information about individuals for research purposes
Public Interest	Exceptional circumstances that justify overruling the right of an individual to confidentiality in order to serve a broader societal interest.
Records	Information created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business
Records management	Field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records
Records system	Information system which captures, manages and provides access to records through time

Term	Definition
Registration	Act of giving a record a unique identifier on its entry into a system
Relevant Filing System	A term which defines sets of manual data/records in the Data Protection Act 1998. It means any structured set of information which is organised either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual can be easily found.
Residual risk	The risk remaining after risk treatment
Risk	Combination of the probability of an event and its consequence
Risk acceptance	The decision to accept a risk
Risk analysis	Systematic use of information to identify sources and to estimate the risk
Risk assessment	Overall process of risk analysis and risk evaluation
Risk evaluation	Process of comparing the estimated risk against given risk criteria to determine the significance of the risk
Risk management	Coordinated activities to direct and control an organisation with regard to risk
Risk treatment	Process of selection and implementation of measures to modify risk
S4BH / SBH	Standards For Better Health
Sensitive Personal Data	A term used in the Data Protection Act 1998. It is defined in the Act as personal data consisting of a person’s racial or ethnic origin, political opinions, religious beliefs or beliefs of a similar nature, membership of a trade union, physical or mental health or condition, sexual life or the commission or alleged commission of any offence (or proceedings for those offences) by that person.
Special Purposes	A term used in the Data Protection Act 1998. It refers to data used for the purposes of journalism, artistic or literary purposes
Statement of applicability	Documented statement describing the control objectives and controls that are relevant and applicable to the organisation’s ISMS
Strategy	a long term plan of action designed to achieve a particular goal
Subject Access	This means the right of any individual (under the provisions of the 1998 Act) to have access to personal information about themselves.
Third party	That person or body that is recognised as being independent of the parties involved, as concerns the issue in question
Threat	A potential cause of an unwanted incident which may result in harm to a system or organisation
Tracking	Creating, capturing and maintaining information about the movement and use of records
Transfer (custody)	Change of custody, ownership and/or responsibility for records
Transfer (movement)	Moving records from one location to another
UPS	Uninterruptible power supply
Vulnerability	A weakness of an asset or group of assets that can be exploited by one or more threats.