

Policy

Information governance

Key messages

- All new staff will receive a copy of the information governance code of conduct in their staff handbooks. This is a summary of all of the information governance policies and procedures.
- An information governance checklist must be completed before the implementation of any new systems or processes eg new information technology (IT) system.
- Identified information risks must have an information risk assessment completed.
- Contracts with third parties must include information governance clauses, an information governance checklist must be completed for all new contract negotiations.
- All staff will receive information governance training on a yearly basis

1 Scope

This policy applies to all Trust employees, including:

- staff who hold honorary contracts;
- contractors working on behalf of the Trust;
- the Board of governors;
- Non executive directors.

2 Purpose

- inform staff of their responsibilities in relation to information governance;
- ensure compliance with the standards required in relation to information governance;
- embed the culture of information governance in the organisation.

3 Definitions

3.1 Business continuity plan (BCP)

This is a formal structured plan which describes how the business unit is to operate during a declared major incident which could incorporate the absence of information assets or critical systems.

3.2 Information governance

This is a framework that ensures that personal and corporate information is dealt with legally, securely, efficiently and effectively to appropriate ethical and quality standards.

Information governance

Directorate of information systems and analysis

3.3 Information governance toolkit

This enables organisations to measure their compliance with the information-handling requirements by assessing themselves against the following initiatives:

- Information governance management
- Confidentiality and data protection assurance
- Information security assurance
- Clinical information assurance
- Secondary uses assurance
- Corporate information assurance

3.4 Information risk assessment

The chance of something happening that involves information, which will have an impact upon the trust's compliance with information governance requirements, the achievement of the trust's objects and the provision of patient care.

3.5 Information asset (IA)

An information asset is an identifiable and definable information-based organisational component which is 'valuable' to the business of that organisation and without which critical business processes would potentially fail. Please refer to the information asset user guide for more information.

3.6 New system

This is the implementation of a new or substantial upgrade to an IT system, eg Vitalpac, Real-time, patient monitor, e-learning, outpatient coding. Projects will be managed through the IT department's project process or via designated IT managers within departments such as pathology.

3.7 New processes

This is the implementation of a new process that will have an impact on the way the Trust handles and uses personal identifiable information, eg medical records filing pool, computers on wheels.

3.8 Personal identifiable data (PID)

This is data that may be used to identify an individual patient, staff member or other member of the public. For a more complete description, refer to the data protection policy and procedure.

3.9 Third party service provider/ data processor

Setting up of a contract with an external supplier to either process personal data on the Trust's behalf or to provide a service to the Trust where they will require or have access to Trust information eg outsourcing services, software support and maintenance, cleaning services.

4 Introduction

The Trust 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 patients and staff and commercially sensitive information. The Trust also recognises the need to share patient information with other health organisations and other agencies in a controlled manner consistent with the interests of the patient and, in some circumstances the public interest.

This policy sets out how the Trust will meet its obligations in relation to information governance.

The legal framework and standards relevant to information governance includes:

- The Data Protection Act 1998
- The Freedom of Information Act 2000
- Common law on confidentiality
- ISO/IEC 17799:2005 Information Security Management
- The NHS Information Security Code of Practice
- The NHS Confidentiality Code of Practice
- The NHS Records Management Code of Practice
- Caldicott
- Information Quality Assurance (data quality)
- Payment by Results Code of Conduct

5 Responsibilities

5.1 Board responsibility

The director of information systems and analysis is the named executive director with responsibility for information governance.

5.2 Information Governance Steering Group (IGSG)

Overall responsibility for overseeing the implementation of the information governance strategy, the information governance policy and information governance action plan.

5.3 Information governance lead

The information governance lead is responsible for the co-ordination and management of information governance, undertaking information risk assessments, investigate incidents & breaches, ensuring new systems and processes comply with information governance, ensuring all third party contracts contain appropriate information governance clauses, drafting information governance policies and procedures, ensuring all staff receive the appropriate information governance training and awareness, maintaining

Information governance

Directorate of information systems and analysis

the mobile device register, providing advice and assistance and ensuring information governance compliance through the audit program.

5.4 IT governance lead

is responsible for ensuring information governance compliance in IT processes and systems, providing technical information governance advice and direction, ensuring new systems and IT processes comply with information governance, undertaking information risk assessments, drafting information governance policies and procedures and ensuring all staff receive the appropriate information governance awareness.

5.5 Information governance team

The information governance team is responsible for undertaking tasks as directed by the information governance lead and providing information governance training to all Trust staff.

5.6 Information governance owners (IGO)

Information governance owners are nominated senior managers with an area of expertise who are responsible for ensuring compliance with elements of the information governance toolkit, meeting level 2 standards and achieving or working towards meeting level 3 standards.

5.7 Senior information risk owner (SIRO)

This is a board level role to;

- lead and foster a culture that values and protects and uses information for the success of the organisation and benefits of its patients;
- own the organisations overall information risk policy and information risk assessment process, test its outcome and ensure it is used;
- advise the accounting officer on the information risks aspects of the statement of internal control. Ensure the board are aware of risks;
- own the organisations information incident management framework;
- ensure that serious untoward incidents and data losses are reported in the organisations annual report.

5.8 Data protection officer

The data protection officer is responsible for all aspects of compliance with the Data Protection Act, please refer to the Data Protection Policy for more information.

5.9 Caldicott guardian

This is a senior clinician appointed by the Trust to advise on issues of patient confidentiality, in accordance with the caldicott principles. Oversees data-sharing agreements between the Trust and non-NHS agencies and may arbitrate on confidentiality issues not clearly defined in law.

Information governance

Directorate of information systems and analysis

5.10 Information asset owner (IAO):

This is a senior person within a division or department who is accountable for a particular asset or group of assets. Specifically, this individual will:

- be required to complete the relevant CFH modules in the information governance e-learning training tool;
- be supported by the information governance lead and IT governance lead;
- undertake a strategic role and provide assurance to the SIRO that:
 - i. assets are managed efficiently: access rights are being appropriately managed, business continuity and recovery plans are in place for business critical assets, assets are available and that the confidentiality and integrity of each asset is protected;
 - ii. dependencies on other assets are managed and the nature of these dependencies is understood and accounted for
 - iii. an information asset register entry is maintained;
 - iv. a risk assessment has been undertaken and any medium and high risks have an agreed action plan and that the requirements of the action plan are implemented in order to reduce the risk;
 - v. staff are aware of and adhere to the information governance policies and procedures, supporting a culture that values, protects and uses information for the success of the organisation and the benefit of its patients.

5.11 Information asset administrator (IAA)

This is a practical role covering the ongoing maintenance of the data held in the information asset register. Specifically, this individual will:

- provide support to the IAO;
- be required to complete the relevant CFH modules in the information governance e-learning training tool;
- for each asset under their control, the IAA will:
 - vi. ensure that information governance policies and procedures are followed;
 - vii. recognise potential or actual security incidents;
 - viii. ensure that information assets are entered into the register and that they are accurate and maintained up-to-date;
 - ix. prepare risk assessment action plans for the IAO to approve (in consultation with risk officer and IG team as appropriate);
 - x. oversee implementation of risk assessment action plans in order to reduce risk to the business.

Information governance

Directorate of information systems and analysis

5.12 Senior managers

Senior managers are to ensure that all staff comply with the policies and procedures and that they attend training on a yearly basis. To implement any necessary/ reasonable changes that is highlighted by audits. Ensure all staff sign compliance with the information governance code of conduct

5.13 Data awareness representatives

Each department has a nominated data awareness representative, along with the department's senior manager they are responsible for ensuring that staff comply with the relevant policies and procedures and to undertake key tasks as directed by the information governance team or head of patient services.

5.14 All Trust staff

All Trust staff must adhere to the confidentiality clause in their contract, attend information governance training on a yearly basis, report any breaches of confidentiality and comply with this policy.

6 Key elements

There are five key strands to information governance:

1. Proactive use of information in the organisation for patient care and service management as determined by law and statute
2. Proactive use of information between the Trust, NHS organisations and partner organisations to support patient care as determined by law and statute
3. Commitment to make non confidential information widely available in line with freedom of information (FOI)
4. Effective arrangements to ensure confidentiality, security and quality of personal and sensitive information
5. Information held is of highest quality in terms of accuracy, timeliness & relevance

7 Information asset register

As part of the information governance toolkit, the Trust is required to build and maintain a register of all its major information assets and assign responsibility for their ownership.

Each asset is assigned an accountable owner and has a number of parameters associated with it which together define key characteristics enabling the Trust to manage risk, security, availability and interdependence.

For further guidance please refer to the information asset user guide.

Information governance

Directorate of information systems and analysis

8 New systems and processes

The implementation of new systems and processes must comply with information governance requirements. All projects will require information governance approval prior to deployment.

Information governance compliance is required to:

- identify and manage risks;
- avoid unnecessary costs;
- avoid inadequate solutions;
- avoid loss of trust and reputation;
- meet legal and information governance requirements.

8.1 Information governance checklists

Part 1 information governance checklist form must be completed by the project manager/department manager at the conception/design stage of the project, once completed this form must be returned to the information governance team. Based on the information provided the information governance team will:

- where applicable issue the Part 2 information governance checklist form to the project manager/ department manager to complete at the appropriate stages of the project progression;
- advise that a privacy impact assessment is required, please refer below;
- advise that a third party contractor needs to completed the Third party contractor checklist form.
- final deployment of a new system/process cannot proceed until information governance approval has been provided

The information governance checklists forms are available on [Connect](#).

8.2 Conducting a privacy impact assessment:

What is privacy?

- Personal information
- Person – integrity of the individuals body e.g. body searches
- Personal behaviour – observation of what individuals do
- Personal communication – various means of recording and analysing communications

Information governance

Directorate of information systems and analysis

Do we need to undertake a privacy impact assessment?

1. The following information is required:
 - An outline of the project
 - Completion of IG checklist form part 1
2. Undertake an initial assessment of the privacy risks – impacts, risks and vulnerabilities
3. Privacy impact assessment not required – record decision on new systems log
4. Privacy impact assessment required – the following steps must be completed:
 - a) Obtain a project outline
 - b) Set up a consultation group, involving stakeholders
 - c) Undertake consultation and analysis of the privacy risks – document the privacy impacts, solutions and actions to deal with these. Send to the project manager to cascade to the project steering group
 - d) Document the outcome
Review and audit – set timeframe to ensure recommendations implemented

9 Third party supply contracts

- all contracts must contain appropriate information governance clauses;
- the information governance team will maintain a log of contracts reviewed for information governance compliance, this will periodically updated against the information held by procurement, finance and IT;
- contractors who are processing the Trust's data on our behalf must comply with information governance requirements;
- contractors who are providing a service to the Trust and either require access to the Trust's information assets (remote or on site) or will have access to Trust information because they are working on site must comply with information governance requirements;
- the IG team will audit that contractors comply with information governance requirements every two years

9.1 Joint ventures with third parties

- when the Trust is considering setting up a joint venture with a third party the Trust representative must contact the information governance team for advice to ensure compliance with information governance requirements;

Information governance

Directorate of information systems and analysis

- a 'not for disclosure agreement' may be appropriate, this agreement must contain appropriate information governance clauses, advice is available from the information governance team;
- once agreement has been reached to set up a joint venture, a contract between the organisations will be required, the contract must include appropriate information governance clauses, advice is available from the information governance team.

9.2 Outsourcing of a Trust service

- the provision of services may be outsourced to a third party, either to a data processor or service provider;

9.2.1 Data processor

- The data processor must complete the Third Party Information Governance Checklist form, completed forms must then be returned to the information governance team. If appropriate actions may be identified for the Trust or contractor to undertake. Approval with information governance requirements will be provided once all actions are completed or if no actions are appropriate;
- all contract terms and conditions must include the appropriate data processor information governance clauses; these are available on Connect;
- all new data processor's must complete and work towards achieving at least level 2 in all of the requirements of the information governance toolkit for third party contractors;
- the third party checklist will be issued to all data processors every two years to review information governance compliance.

9.2.2 Supplier of services

- The contractor must complete third party information governance checklist form, completed forms must then be returned to the information governance team. If appropriate actions may be identified for the Trust or contractor to undertake. Approval with information governance requirements will be provided once all actions are completed or if no actions are appropriate;
- all contract terms and conditions must include the appropriate service provider information governance clauses; these are available on Connect.

If the contract is being set up as part of a new system/ process please also refer to the new systems and processes section above.

Information governance

Directorate of information systems and analysis

9.2.3 Visitors with visibility off or access to the Trust's information assets

In certain situations visitors to the site may require access to the Trust's information assets or have visibility of the confidential patient information because of the areas they are visiting, not all of these visitors will have a contract agreement with the Trust. These visitors to the Trust must sign a confidentiality statement. A copy of the confidentiality agreement is available on Connect. Advice is available from the information governance team.

9.2.4 Request to share an extract of a database or copy of a database with a service provider contractor

Where there is a need to share personal identifiable data with a service provider contractor eg they require an extract of a database to fix a problem or they require data to perform an analysis on behalf of the trust and that data cannot be anonymised, the third party contractor must firstly sign the data protection contractor form, this form must be completed before any data is shared. This form is available as a word document on [Connect](#). The contractor must copy this form onto their headed paper. A copy of the signed form must be sent to the information governance lead.

Once approval has been received to share the data with the third party contractor from information governance the database must be sent in a secure manner either by encryption or uploading to a secure site, please contact the IT helpdesk for further advice.

10 Information governance code of conduct

All new starters to the Trust will receive the information governance code of conduct in their staff handbooks. The code is a summary of the various information governance policies. All staff will be required to sign compliance with the information governance code of conduct and a record of this will be recorded on OLM.

For further information please refer to Connect and the [induction checklist](#).

11 Training and awareness

All new starters will receive information governance training as part of their Trust Induction and orientation program.

All Trust staff will receive an information governance yearly update.

Staff will be kept up to date on information governance issues via the information governance pages on [Connect](#), the Connect e-bulletins, the information governance newsletter or via emails.

Information governance

Directorate of information systems and analysis

12 Management of the information governance toolkit

All IGO's will be required to produce an action plan for the elements that they are responsible for to demonstrate how the Trust will meet the requirements of the information governance toolkit. These action plans will be monitored through the IGSG.

The IGO will be responsible for collating a list of evidence that is being used to demonstrate compliance with the information governance toolkit requirements.

The Trust's assessment of its compliance with the information governance toolkit will be submitted to connecting for health as required.

The Trust will undertake internal and external audit as directed by the director of information systems and analysis.

Information governance will be reported quarterly to the information systems program board and the quality committee, which is a designated sub committee of the board. Reports to the board will be presented as requested by the director of information systems and analysis.

The information governance quarterly report will monitor performance against key standards; the report will be presented to the IGSG.

13 Information risk assessment

Information risk is inherent in all administrative and business activities and everyone working for and on behalf of the Trust continuously manages information risk. The aim of information risk management is not to eliminate risk, but rather to provide the structural means to identify prioritise and manage the risks involved. It is an essential element of information governance.

Information risk assessment will either be undertaken by the departmental risk officer/ lead or the information governance lead or IT governance lead. Information risk assessments will be assessed using the information risk assessment tool, please refer to [Connect](#). All information risk assessments will be approved by the SIRO and a monthly report will be provided to the IGSG.

Further guidance is available in the information risk assessment flow chart, and the information risk assessment leaflet on [Connect](#) and in the [risk management policy](#).

14 Information governance audit program

The information governance team will regularly undertake audits to ensure compliance with information governance requirements. Reports will be

Information governance

Directorate of information systems and analysis

available from these audits and action plans produced where necessary to ensure that any findings from the audits are implemented.

15 Audit of access to confidential information

- incidents are monitored by the Information Governance Lead and IT Governance Lead, for further information please refer to the [information governance incident and investigation procedure](#);
- IT service helpdesk and support team will inform the information governance team of any calls that involve miss use or sharing of passwords, the information governance team will investigate these incidents. If a member of staff is logged out of the system because a password has been shared, the IT service helpdesk will not reset the password until one of the information governance team has spoken to the member of staff;
- a review will be undertaken by the information governance team on a yearly basis of all main applications/systems that handle personal identifiable information to ensure they comply with the appropriate mechanisms that have been put in place to manage and safeguard confidentiality including a review of access rights, profiles, reporting, audit trails and to review a sample of forms requesting access to the system;
- medical records follow authorise access to the library, for further information please refer to the [confidentiality of personal health information policy](#);
- a summary of the findings will be included in the information governance yearly audit report provided for the information governance steering group.

16 Business continuity

Business continuity plans help organisations predict, assess and counteract threats and risks that may lead to events that seriously disrupt or curtail all or part of their business functions. The assessments analyse the probability of the events occurring, their likely impact and determine the procedures that the Trust should follow if such an event were to occur.

For further information please refer to the [service level continuity policy and procedure](#).

17 Policy exception

There may be exceptional circumstances where Trust staff require approval for a process/ device that will not fully comply with the Trust information governance policies, a [policy exception form](#) should be completed and submitted to information governance for a decision to be made as to whether the exception can be approved.

Information governance

Directorate of information systems and analysis

18 Breaches and incidents

It is each member of staff's responsibility to comply with the relevant policies and procedures that meet the requirements of information governance. Failure to comply with the trust policies, breach Confidentiality or breach the Data Protection Act could result in staff being taken through disciplinary procedures which could result in the loss of employment.

Further guidance is available in the [information governance incident and investigation procedure](#).

19 Monitoring compliance with and the effectiveness of the policy

Key standards:

- new systems and processes comply with information governance requirements;
- third party contracts comply with information governance requirements;
- information risk assessments are in place to manage information risks;
- the trust complies with the requirement to meet minimum level 2 standard in the information governance toolkit assessment;
- staff attend information governance training and sign compliance with the information governance code of conduct.

The standards will be monitored by the information governance team by:

- submission of evidence required on a yearly basis as part of the information governance toolkit;
- completion of information governance audits in all areas, producing a report and action plan. The IGSG will receive a yearly report in March highlighting the findings of the audits;
- information governance quarterly report monitors key standards for information governance such as incidents, freedom of information requests and data quality;
- a log will be maintained of all new system/ processes information governance actions;
- a log will be maintained of all third party contract information governance actions;

The IGSG is responsible for monitoring compliance with information governance and ensuring that the necessary actions are undertaken.

20 References

- Data Protection Act 1998
- NHS Confidentiality Code of Practice
- NHS Records Management Code of Practice
- NHS Information Security Code of Practice
- Information Governance Toolkit

Information governance

Directorate of information systems and analysis

21 Associated documents

- [Confidentiality of personal health information policy](#)
- [Data protection policy and procedure](#)
- [Information asset procedure](#)
- [induction checklist](#)
- [Information governance checklists](#)
- [Information governance incident and investigations policy and procedure](#)
- [Information security policy](#)
- [Risk assessments](#)
- [Risk management policy and strategy](#)
- [Service continuity procedure](#)

Equality and diversity statement

This document complies with the Cambridge University Hospitals NHS Foundation Trust service equality and diversity statement.

Disclaimer

It is **your** responsibility to check against the electronic library that this printed out copy is the most recent issue of this document.

Approval:	Information governance steering group- 9 February 2012		
Owning department:	Information governance		
Author(s):	Michelle Ellerbeck- Information Governance Lead		
File name:	Information governance policy Version 7 February 2012 .doc		
Supersedes:	Version 6, March 2010		
Version number:	7	Review date:	February 2015
Local reference:		Media ID:	7494