

Strategy

Information governance

1 Scope

There are two key components underpinning this strategy which are:

1. The Trust's [information governance policy](#), which outlines the objectives for information governance; and
2. An annual action plan arising from a baseline assessment against the standards set out in the NHS Connecting For Health Information Governance Toolkit within the following initiatives:
 - Information governance management
 - Confidentiality and data protection assurance
 - Information security assurance
 - Clinical information assurance
 - Secondary use assurance
 - Corporate information assurance

The legal framework and standards relevant to Information Governance include the following:

- Data Protection Act 1998
- Freedom of Information Act 2000
- Access to Health Records Act 1990
- The NHS Code of Practice on Confidentiality
- The NHS Code of Practice for Information Security
- The NHS Code of Practice for Records Management
- BS ISO/IEC 27001/27002 Information Security

2 Purpose

This strategy sets out the approach to be taken within the Trust to provide a robust information governance framework for the current and future management of information.

It applies to all information held by the Trust and all information systems used to hold that information. These systems may be purely paper based or partially or totally electronic.

Information governance

Directorate of information, systems, and analysis

3 Introduction

Information is a vital asset, in terms of the clinical management of individual patients and the efficient management of services and resources. It plays a key part in clinical governance, service planning, performance management, and the Trust's interactions with other organisations.

It is therefore of paramount importance to ensure that information is efficiently managed, and that appropriate policies, procedures and management accountability and structures provide a robust information governance framework to assure and demonstrate the proactive use of information as determined by legislative acts, statute and best practice.

Information governance is 'A framework for handling information in a confidential and secure manner to appropriate ethical and quality standards in a modern health service. It enables NHS organisations to ensure that information is dealt with legally, securely, effectively and efficiently in order to deliver the best possible care to patients, clients and service users.

4 Responsibilities

The ultimate responsibility for information governance in the Trust lies with the board of directors. The director of information systems and analysis is the named executive director with responsibility for information governance and has been nominated as the Trust's senior information risk owner.

The Information Governance Steering Group (IGSG) will have delegate authority from the Board to discharge its functions in this respect, having overall responsibility for overseeing the implementation of this strategy, the [information governance policy](#) and information governance action plan.

The IGSG is accountable through the quality committee to the board of directors.

The information governance work program is supported by key roles:

- the information governance lead is responsible for the co-ordination and management of information governance;
- elements of the information governance toolkit are assigned to information governance owners according to their area of responsibility and expertise;
- the IT information governance lead is responsible for ensuring governance compliance in IT and for providing IT security advice and direction
- the caldicott guardian, a senior clinician appointed by the Trust to advise on issues of patient confidentiality.
- the head of patient services is the Trust's caldicott officer and data protection officer.

Information governance

Directorate of information, systems, and analysis

Any associated resource implications arising from the implementation of the [information governance policy](#) and action plan will be identified by the IGSG. Business cases will then be developed and submitted for approval.

5 Aims

The aim of this strategy is to ensure the effective management of information governance by:

- the issue and review of appropriate policies, procedures and guidance, to deliver compliance with Department of Health information governance standards;
- the issue of an information governance framework, the standards that the Trust should adhere to when implementing new systems, technologies and processes;
- to comply with best practice and the highest standards of information governance;
- to work to instil an information governance culture within the Trust so that it is part of every day business;
- the provision of appropriate information governance training and awareness for all Trust staff;
- to oversee the implementation of the Connecting for Health IG Toolkit ensuring that improvements plans are in place; working towards year on year improvements;
- minimise the risk of breaches and inappropriate use of personal data;
- ensuring compliance with information governance through a robust audit program;
- ensuring information governance compliance with key processes including business continuity, implementation of new systems and processes and the setting up of third party supplier contracts;
- ensuring compliance with the NHS Care Records Guarantee;
- aiming to reduce the level of risk identified through the Information Risk Assessments program;
- ensuring compliance with the Freedom of Information Act, identifying and processing requests for information in accordance with the Act, being open and honest by placing as much information into the public domain as possible through the publication scheme;
- ensuring compliance with the NHS Records Management Code of Practice by implementing a records management system for corporate records and health records that ensures that information is:
 - available to staff on a need to know basis
 - is accessible and easily retrieved when required
 - departments have a record of what information is held and where it is kept
 - retained according to retention schedules
 - retained in appropriate secure storage facilities
 - created to support business and clinical functions of the Trust
- developing an information asset register by identifying all information assets held by the Trust, nominating an information asset owner for each asset, undertaking an information risk assessment and business

Information governance

Directorate of information, systems, and analysis

- impact assessment for all assets and ensuring that all areas have a business continuity plan in place;
- ensuring compliance with the Data Protection Act 1998 by
 - informing patients on the uses of their information
 - keeping personal identifiable data secure and so that access is on a strict need to know basis
 - retaining only the information that is required and not keeping it for longer than necessary
 - ensuring information is shared legally and securely
 - ensuring information is only used for lawful purposes
 - ensuring the rights of patients are protected
- to be innovative and proactive in developing future information governance standards in order to support new ways of working such as the E-hospital project and developments because of changes to the ways the NHS will work in the future

6 Monitoring compliance with and the effectiveness of the strategy

Each year, this strategy and the [information governance policy](#) will be reviewed and an action plan developed against the information governance toolkit to identify key areas for continuous improvement.

Performance against the information governance toolkit will be monitored by the IGSG and submitted to Connecting for Health via the IG Toolkit assessment process on an annual basis.

Progress reports will be submitted to the Quality Committee on a quarterly basis.

A random selection of the elements of the information governance toolkit will be audited internally by a senior manager prior to the annual submission to Connecting for Health. Information governance will be included in the internal auditor's work program as directed by the director of information systems and analysis.

Information governance audits will be undertaken by the information governance team across the Trust to monitor compliance with the information governance policies and procedures.

7 Associated documents

- [Confidentiality of personal health information policy](#)
- [Data protection policy and procedure](#)
- [Data quality policy](#)
- [Freedom of information policy and procedure](#)
- Information governance management framework
- [Information governance policy](#)
- [Information security policy](#)
- [Medical records procedures](#)
- [Records management policy](#)

Information governance

Directorate of information, systems, and analysis

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.

Document management

Approval:	Information Governance Steering Group- 9 February 2012		
Owning department:	Information governance		
Author(s):	Michelle Ellerbeck- Information Governance Lead		
File name:	Information governance strategy Version 7 February 2012 .doc		
Supersedes:	Version 6, October 2010		
Version number:	7	Review date:	February 2015
Local reference:		Media ID:	7498