Policy Document Control Page

Title

Title: Information Governance Strategy

Version: 3

Reference Number: CO87

Keywords:

Information governance

Supersedes
Supersedes: Version 2
Description of Amendment(s):

- Updated to reflect work programme for Information Governance

Important Notice
From May 2018 the UK will be adopting the European General Data Protection Regulations. These regulations will be replacing the Data Protection Act 1998. In the UK we are still awaiting some health sector specific guidance and instruction regarding GDPR, and as such have deemed that, unless there is a legal requirement or a fundamental change that is required in a policy, all policies, regardless of review date, shall remain current, valid and must be followed for the foreseeable future, to be reviewed prior to the implementation of GDPR from May 2018. Any queries in relation to this statement should be directed to the Trust Information Governance Manager.

Originator

Originated By: Jenny Spiers

Designation: Information Governance Manager

Equality Impact Assessment (EIA) Process
Equality Relevance Assessment Undertaken by: Jonathan Mayes
ERA undertaken on: 14th June 2013 (passed to Equality Team on same day)
ERA approved by EIA Work group on: 23rd August 2013
Reviewed as appropriate: Kevin Tarleton, Information Risk Manager; 11 March 2015

Where policy deemed relevant to equality- N/A
EIA undertaken by N/A
EIA undertaken on N/A
EIA approved by EIA work group on N/A

Approval and Ratification

Referred for approval by: Information Governance Manager

Date of Referral: 1st March 2017

Approved by: Information Governance Assurance Group

Approval Date: 1st March 2017

Date Ratified by Executive Directors: 20th March 2017

Executive Director Lead: Director of Service Development and Sustainability

Circulation

Issue Date: 23rd March 2017

Circulated by: Information Department

Issued to: An e-copy of this policy is sent to all wards and departments

Policy to be uploaded to the Trust's External Website? YES

Review

Review Date: January 2019

Responsibility of: Jenny Spiers

Designation: Information Governance Manager

This policy is to be disseminated to all relevant staff.

This policy must be posted on the Intranet.

Date Posted: 23rd March 2017

Contents

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.

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

1.3 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"[1]. It brings together within a singular cohesive framework, the interdependent requirements and standards of practice.

1.4 Information Governance (IG) combines requirements for Information Security, Corporate Governance and Business Continuity, and the increasing legislative and regulatory requirements, into a single unified management framework.

1.5 Information Governance is not simply a matter of good corporate housekeeping. Good Information Governance can lead to efficiency gains and make for more effective management by helping to assure the quality of information we hold and use.

1.6 The Trust is required to have effective arrangements in place to govern the use of information and information systems, as set out in the Information Governance Toolkit, Care Quality Commission – Essential Standards of Quality and Safety, and the NHS Litigation Authority Risk Management Standards.

[1] *Records Management: NHS Code of Practice Part 1*

2. PURPOSE

2.1 This strategy sets out the approach to be taken within the Trust to ensure legal and regulatory compliance for the management of information.

2.2 The Information Governance Strategy cannot be seen in isolation as information plays a key part in Corporate Governance, strategic risk, Clinical Governance, service planning, informatics, performance and business management. We are committed to ensuring this strategy is aligned with other strategies to ensure integration with all aspects of the Trust's business activities.

3. SCOPE

3.1 Information Governance covers all aspects of information handling within the Trust, including patient / service user information, staff related information and Trust information, including structured record systems (paper & electronic).

3.2 There are two key components underpinning this Strategy, which are:

- The Trust's Information Governance Policy, which outlines the objectives for Information Governance
- An annual action / improvement plan arising from a baseline assessment of the Health and Social Care Information Centre (HSCIC) Information Governance (IG) Toolkit standards, within the following initiative areas:
    - Information Governance Management
    - Confidentiality & Data Protection
    - Information Security Assurance
    - Clinical Information Assurance
    - Secondary Use Assurance
    - Corporate Information Assurance

3.3 The Information Governance agenda encompasses the following areas:

- Caldicott principles (management of patient-identifiable information)
- NHS Confidentiality Code of Practice
- Data Protection Act 1998 (DPA)
- Freedom of Information Act 2000
- Records Management (Health, Business and Corporate)
- Information Security
- Information Quality
- Information Risk Management
- Confidentiality
- Openness
- Legal Compliance

4. DUTIES AND RESPONSIBILITIES

4.1 **Senior Information Risk Owner** (**SIRO)**

The SIRO has responsibility for ensuring compliance with legislation and national policy in relation to the security of information, in particular person identifiable information. An annual report on Information Governance is presented to the Trust Board by the Senior Information Risk Owner. The SIRO is the Director of Service Development and Sustainability.

4.2 **Caldicott Guardian (CG)**

The CG plays a key role in ensuring that the Trust satisfies the highest practical standards for handling patient identifiable information. The CG also supports work to facilitate and enable information sharing and advises on options for lawful and ethical processing of information, as required. The CG is the Medical Director.

4.3 **Information Asset Owners (IAOs)**

Information Asset Owners - IAOs are directly accountable to the SIRO and will provide assurance that information risk is being managed effectively for their assigned information assets. The IAOs are assisted in their roles by **Information Asset Managers (IAMs) and Information Asset Administrators** (IAAs) who have day to day responsibility for management of information risks affecting one or more assets. The IAOs are responsible for providing or informing regular written reports to the SIRO, (annually as a minimum) on the assurance and usage of their asset(s).

4.4 **Information Governance Manager**

The Trust's Information Governance Manager shall ensure the Trust complies with all legislation and national policy in relation to Data Protection, Freedom of Information, Records Management, Information Risk Management, Caldicott principles, confidentiality and Information Security.

4.5 **Senior Information Governance and Risk Officer**

The Trust's Senior Information Governance and Risk officer shall have responsibility for implementing robust information risk management throughout the Trust, ensuring compliance with legislation and national policy in relation to the management of information risk and Freedom of Information.

4.6 **Records Manager**

The Trust's Records Manager is responsible for the overall development and maintenance of records management practices throughout the organisation. In particular, the Records Manager is responsible for drawing up guidance for good records management practice and promoting compliance with records management to ensure the easy, appropriate and timely retrieval of service user and business information.

4.7 **Line Managers / Senior Managers**

All Line Managers have responsibility to ensure that staff are compliant with and working to all relevant policies and procedures in relation to Information Governance. They also have responsibility for ensuring all

staff have completed annual mandatory IG Training and that any incidents or policy breaches in relation to IG principles are reported immediately.

4.8 **All employees and contractors, and anyone providing a service on behalf of the Trust**

All employees and contractors of the Trust, whether permanent, temporary or contracted, have responsibilities for IG on a day-to-day basis, whether they work in a clinical or non-clinical environment. All employees and contractors must complete the mandatory IG training annually. Contractors are responsible for ensuring that they are aware of the requirements incumbent upon them and for ensuring that they comply with these. Any incident involving a breach or suspected breach of the DPA shall be reported to their line manager immediately and, where they are not available, to the Trust's Information Governance Manager or Senior Information Governance & Risk Officer.

5. PROCESS

5.1 Information Governance is about demonstrating that we can be trusted by patients / services users and partner organisations to maintain the confidentiality and security of personal information, by helping individuals to practice good information governance and to be consistent in the way we handle personal and corporate information.

5.2 The aim of this Strategy is to ensure the effective management of Information Governance by:

- Complying with all legislation
- Establishing, implementing and maintaining policies for the effective management of information
- Ensuring a consistent approach to information management
- Recognising the need for an appropriate balance between openness and confidentiality in the management and use of information
- Ensuring all Trust staff follow and promote best practice
- Ensuring maintenance or year on year improvement with the IG Toolkit assessment
- Developing a culture of increased Information Governance awareness throughout the Trust
- Helping staff to manage personal information for the benefit of patient care
- Reducing duplication and looking at new ways of working effectively and efficiently
- Minimising the risk of incidents involving personal data
- Minimising inappropriate use of personal data

5.3 **Information Governance work streams 2017 – 2018**

Strategic objective	Requirement / Plan	Monitoring / Assessment	Lead / Target Date
We will be a committed and trusted local partner by assuring the safety and effectiveness of services through robust governance	Comply with the requirements of the Information Governance Toolkit V14 and V15	IG Assurance Plan 2017/18 monitored via the Information Governance department, IGAG and Internal Audit	Information Governance Manager – March 2017 (V14) and March 2018 (V15)
	Ensure completion of privacy impact assessments (PIAs) for the implementation of new systems and processes	PIA process and procedure. Completed PIAs reported to IGAG.	Information Governance Manager February 2017 and on-going
	Improve and manage the archiving solution of paper health care records across the Trust	Mitigate against risks by undertaking risk assessments and appropriate use of the taskforce. Continue to provide an efficient helpdesk function for the archiving and retrieval of records. Report any issues to IGAG.	Records Manager February 2017 and on-going
	Manage information risk within the Trust to an acceptable level	Identify and document information assets and data flows. Complete	Senior IG and Risk Officer – February 2017 and on-going

Strategic objective	Requirement / Plan	Monitoring / Assessment	Lead / Target Date
		information risk assessments. Regular review and monitoring of information risks. Report risks to IGAG	
	Monitor system activity for any inappropriate access via Paris break glass and SCR self-claim access	Completion of privacy audits. Spot checks of minimum 10% staff access and report to IGAG	Privacy Officer February 2017 and on-going
We will create a positive experience by delivering care that is integrated and seamless and is local, accessible and responsive	Fully Implement Paris clinical system to additional clinical areas incorporating agreed information security strategy	Via clinical system project implementation group/IAOs/IAMs/IAAs	ICT Director/Information Governance Manager – April 2018
	Contribute to the Integrated Care projects ensuring IG requirements are recognised and acted upon.	Completion of PIAs and ISAs Monitor and reviewed at IGAG	Information Governance Manager – March 2018
We will create a positive experience by delivering care that is high quality and evidence based	Undertake reviews of Information Governance incidents	1:1 contact with staff reporting incidents to ensure all actions are identified and implemented. Identify lessons learned to mitigate	Information Governance Manager/Records Manager – February 2017 and on-going

Strategic objective	Requirement / Plan	Monitoring / Assessment	Lead / Target Date
		against further incidents. Bulletins to staff on incidents and lessons learned. Fully implement action plan following receipt of ICO undertaking.	
We will be a committed and trusted local partner by working in partnership	Continue to develop and agree Information Sharing agreements with partner organisations	Documented Agreements on Trust Internet site Reporting of Agreements in place via IGAG	Information Governance Manager February 2017 and on-going
	Engage with projects that require joint working with partner organisations	Individual and integrated working/project groups	Information Governance Manager – in place and continually ongoing

5.4 **Other key Information Governance metrics**

- Subject Access reports – compliance with DPA and, in particular, 21 day best practice DoH timeframe and 40 calendar day legal timeframe
- Freedom of Information reports – compliance with relevant Codes of Practice and in particular response within 20 working day legal timeframe
- Care Quality Commission - Information Governance contributes to the implementation of the Care Quality Commission's Essential Standards of Quality and Safety. It is specifically included in Outcome 1 (Respecting and involving people who use services), Outcome 6 (Co-operating with other Providers) and Outcome 21 (Records).

6. TRAINING

6.1 **New Staff**

Information Governance basic training takes place at every induction. All staff (substantive, temporary and students) attend the corporate induction, additionally, the Trust provides four further inductions for psychiatrists (training grades) and the Practice Education Facilitators provide two induction sessions for student nurses entering fieldwork practice within the Trust.

Students from other groups, e.g. occupational therapists, are prepared for fieldwork by the Higher Education bodies and, as such, may not receive the Information Governance training at induction. These students are, however, supervised by staff who will have undertaken the Information Governance training.

At corporate induction, staff are instructed to complete the mandatory on-line IG training within three months of starting their post. Induction is a process that starts with an initial contact day via the corporate process but continues in post for up to three months, hence the instruction to complete the on-line training as part of their ongoing induction with the Trust.

6.2 **Current staff**

Staff are required to complete:

- *311 CSF Information Governance* – this must be completed every 12 months

All staff who handle records should undertake mandatory record keeping training with a 3 year refresher. Face to face record keeping training can be provided by the records management team for 6 or more staff. Individuals will be able to undertake record keeping training through the CEST log in.

7. IMPLEMENTATION

The strategy will be added to the Trust's Policy site on the intranet which will be communicated to all IAO/IAMs/IAAs and to all staff via the communications department announcements update.

8. MONITORING OF COMPLIANCE

8.1 There is an on-going programme of internal and external audit in order to monitor compliance. Compliance is also monitored via the scores achieved in the IG Toolkit which is submitted on an annual basis to HSCIC.

9. REVIEW ARRANGEMENTS

9.1 This strategy will be reviewed in January 2018.