Information Governance Bulletin: Healthcare Providers
Quarter 1, 2012/13

Back ground:

"Information can have great value as an organisational asset but can be a toxic liability if not handled properly", (UK Information Commissioner's Annual Report 2007/08).

Information governance - increasingly seen as a critical component of corporate governance - is not just about ensuring information is secure. Good information governance covers the management, sharing and retention of information, so that an organisation can meet its corporate objectives, customer needs and regulatory obligations.

Good information governance for all organisations - whether public, private or third (not-for-profit) sector – is achieved through the application of standards that will assist in the effective management of information assets and personal data. The following key areas have been identified as the four pillars of information governance:

- ***Effective management of records and electronic documents:***

Part 1 of the British Standard, BS ISO 15489-1, provides guidance on managing records of originating organisations, public or private, for internal and external clients. It:

- Applies to the management of records, in all formats or media, created or received by any public or private organisation in the conduct of its activities, or any individual with a duty to create and maintain records
- Provides guidance on determining the responsibilities of organisations for records and records policies, procedures, systems and processes
- Provides guidance on records management in support of a quality process framework to comply with ISO 9001 and ISO 14001
- Provides guidance on the design and implementation of a records system, but does not include the management of archival records within archival institutions.

- ***Maintenance of document authenticity****:*

If a document is to be admissible, for example in court, its authenticity must be beyond question. Organizations that process large volumes of data therefore need to maximise the reliability of the electronic information they manage, whilst minimising the risk of its long-term storage. British Standard BS 10008, (evidential

weight and legal admissibility of electronic information), specifies the requirements for the implementation and operation of electronic document management systems.

- ***Secure management of information*:**

Information security protects information held by organisations from a wide range of threats to ensure business continuity, minimise business damage and maximise return on investment and business opportunities.

- ***Compliance with data protection legislation:***

Any business required to store personal data, such as details of customers, patients / service users or employees must comply with the Data Protection Act 1998 .The purpose of data protection legislation is to ensure that personal data is not processed without the knowledge and, except in certain cases, the consent of the data subject. It is meant to ensure that personal data is accurately processed, and to enforce a set of standards for the processing of the information. The British Standard BS 10012:2009 (data protection specification for a personal Information management system), offers guidance on how to implement a framework with which to effectively manage personal information (a Personal Information Management system, or PIMS). It provides guidance on putting in place an infrastructure for maintaining and improving compliance with the Data Protection Act.

Information governance in simple terms

Information governance is to do with the way organisations 'process' or handle information. It covers personal information, i.e. that relating to patients/service users and employees, and corporate information, e.g. financial and accounting records. It provides a means whereby employees are able to deal consistently with the many different rules about how information is handled, including those set out in:

- The Data Protection Act 1998.
- The common law duty of confidentiality.
- The Confidentiality NHS Code of Practice.
- The NHS Care Record Guarantee for England.
- The Social Care Record Guarantee for England.
- The international information security standard: ISO/IEC 27002: 2005.
- The Information Security NHS Code of Practice.
- The Records Management NHS Code of Practice.
- The Freedom of Information Act 2000.

Therefore at its heart, Information governance is about setting information handling standards and giving organisations the tools to achieve these standards, with the

ultimate goal being to help organisations and individuals to act consistently in the way they handle personal and corporate information and avoid duplication of effort, leading to improvements in:

- Information handling activities
- Patient and service user confidence in care providers
- Employee training and development

The information governance assessment

All organisations have to assess themselves against requirements for:

- management structures and responsibilities (e.g. assigning responsibility for carrying out the IG assessment, providing staff training, etc)
- confidentiality and data protection; and
- information security

The purpose of the assessment is to enable organisations to measure their compliance against the law and central guidance and to see whether information is handled correctly and protected from unauthorised access, loss, damage and destruction.

Where partial or non-compliance is revealed, organisations must take appropriate measures with the aim of making cultural changes and raising information governance standards through year on year improvements.

Organisations that are required to carry out an assessment

Assessments must be completed by all organisations that fall under the responsibility of the Department of Health (DH). These include:

- NHS organisations (acute trusts, ambulance trusts, mental health trusts, primary care trusts and strategic health authorities) including foundation trusts
- adult social care
- community pharmacies
- dental practices
- eye care services
- general practices
- DH arms' length bodies (ie executive agencies such as the Medicines and Healthcare products Regulatory Agency; special health authorities such as the

NHS Business Services Authority; and non-departmental public bodies such as the Health Protection Agency)

- Organisations that (i) have access to NHS patients and/or to their information; (ii) provide support services directly to an NHS organisation; or (iii) have either direct or indirect access to NHS Connecting for Health services, including N3 - the NHS National Network

Carrying out the Information governance assessment

Assessment of an organisations Information governance compliance status is through the on line Information governance toolkit. The toolkit, acknowledged as the bench mark standard for assuring good information and data security management, is completed on an annual basis and is typically updated by the DH every year, currently being at version 10. In completing the Information governance toolkit organisations are basically self assessing themselves against the principles of information security. These are:

Confidentiality - Information must be secured against unauthorised access

Integrity - Information must be safeguarded against unauthorised modification

Availability - Information must be accessible to authorised users at times when they require it

The toolkit therefore enables the NHS and partner organisations to measure their information governance compliance in respect to aspects of information governance including:

- data protection and confidentiality
- information security
- information quality
- health / care records management
- corporate information

The role of 'Connecting for Health'

NHS Connecting for Health (NHS CFH) is part of the Department of Health Informatics Directorate and is charged with maintaining and developing the NHS national IT infrastructure. This includes organisations entering into an agreement with NHS CFH for access to the NHS National Network (N3). In order to access the N3 network – essential for organisations to share information and therefore a prerequisite of the IG toolkit requirements – they are required to comply with the Information Governance Statement of Compliance (IG SoC) process.

The process includes elements that set out terms and conditions for use of NHS CFH systems and services including the N3, in order to preserve the integrity of those systems and services. The steps in the IG SoC process set out a range of security related requirements which must be satisfied in order for an organisation to be able to provide assurances in respect of safeguarding the N3 network and information assets that may be accessed.

Developments in Information Governance

The field of Information governance is dynamic, driven by ever increasing challenges in data security requirements and the changing needs and demands of the NHS landscape. Consequently changes and updates to the systems and processes supporting Information governance are inevitable. Recent changes include:

- the release of version 10 of the tool kit

- the intended joint working between the NHS and the information Commissioning Office

- Launch of the Health Informatics Apprenticeship Framework

- Publication of the information strategy for health and social care.(The three main themes of the strategy being (i) Modern, convenient information access; (ii)Modern information and technology for professionals; (iii) Patient and citizen rights

- Guidance on information sharing published jointly by the DH and the UK Council of Caldicott Guardians to assist those who need to share information about individuals involved in domestic violence

- NHS Information governance: Information Risk Management - Dealing with Cookies and Legal Compliance