echogenicity

September 2019

www.echogenicity.co.uk

Information Governance Management Framework

Scanning Cornwall's Hearts

Table of Contents

Date ratified March 2018, March 2019
Review date March 2020

1. Introduction

Information Governance (IG) requires clear and effective management and accountability structures, standards, policies and procedures to ensure that all types of information used in Echogenicity are sourced, held and used appropriately, securely and legally.

Information Governance is the framework for handling information in a confidential and secure manner to the appropriate professional and quality standards required in a echocardiography service. It brings together into a single framework independent requirements and standards of practice.

Information is a vital asset for Echogenicity, supporting both day-to-day clinical operations and the effective management of services and resources. It plays a key part in clinical governance, service planning and performance management.

Echogenicity recognises the importance of maintaining an appropriate and robust system of information governance management so as to underpin and support the organisation in the exercise of its functions, to protect privacy and confidentiality together with maintaining public trust.

2. Purpose

The purpose of this document is to set out Echogenicity's approach to provide a robust information governance framework. This is to promote a culture of good practice around the processing of information to ensure that information adheres to professional and quality standards in a secure and confidential manner.

3. Scope

This document applies to all information obtained and processed within Echogenicity either held electronically or in manual paper-based filing systems, relating (but not limited to):

- patient/client/service user information
- staff and personnel information
- organisational, business and operational information
- research, audit and reporting information.

4. Aims

The aims of this document are to ensure Echogenicity maintains a robust Information governance framework, in accordance with Department of Health standards, so that all information under its control is;

- held securely and confidentially
- obtained fairly and lawfully
- recorded accurately and reliably
- used effectively and ethically
- shared and disclosed appropriately and lawfully.
- protected against unauthorised access.

5. Roles & Responsibilities

5.1. Directors

Within Echogenicity Verity Williams-Curnow is ultimate responsible for Information Governance she notes that:

- Information Governance must be explicitly referenced within Echogenicity's Statement of Internal Controls;
- Echogenicity must baseline its performance within the IG Toolkit by the end of March each year, and should update the assessment with improvements at end of January each year, to enable performance and actions to be tracked.
- Echogenicity must sign the Information Governance Statement of Compliance (IGSoC) to provide assurance that key requirements are being met and robust improvement plans are in place to address any shortfalls;
- details of serious untoward incidents involving actual or potential loss of personal data or breach of confidentiality must be published in annual reports and reported to the Clinical Commissioning Group (CCG) and to the Information Commissioner, where appropriate;
- contractual arrangements with independent sector NHS providers also contain strengthened Information Governance requirements.

5.2. Senior Information Risk Owner (SIRO)

Echogenicity has appointed Verity Williams Curnow as the Chief Information Officer as the Senior Information Risk Owner (SIRO). The SIRO is responsible for;

- taking overall ownership of Echogenicity's Information Risk Management Policy;
- is responsible for content of the Statement of Compliance (IG SoC) in regard to information risk;
- ensuring that Information Governance risk assessments and management processes are embedded within Echogenicity.

5.3. Caldicott Guardian

The Caldicott Guardian acts as the "conscience" of an organisation, actively supporting work to facilitate and enable information sharing, advising on options for lawful and ethical processing of information as required.

The Guardian will:

- ensure that the Trust satisfies the highest practical standards for handling patient identifiable information;
- facilitate and enable information sharing and advise on options for lawful and ethical processing of information;
- represent and champion information governance requirements and issues
- ensure that confidentiality issues are appropriately reflected in organisational strategies, policies and working procedures for staff;
- ensure information sharing protocols and agreements are established with partner organisation where confidential patient information may be shared across organisational boundaries.

The Caldicott Guardian is Verity Williams-Curnow

5.4. Information Governance Department

Echogenicity is an extremely small independent community echocardiogram service we do not have an Information Governance Department we are simply too small. Verity Williams Curnow is responsible for all aspects of information governance to include;

- ensuring that there is top level awareness and support for IG resourcing and implementation of improvements;
- providing direction in formulating, establishing and promoting IG policies;
- ensuring annual assessments using the IG Toolkit and audits of IG policies and arrangements are carried out, documented and reported in line with the requirements of the NHS Standard Contract;
- ensuring that annual assessments and improvement plans are prepared
- ensuring that the approach to information handling is communicated to all staff and made available to the public;
- ensuring that staff understand the need to support the safe sharing of personal confidential data for direct care as well as the need to protect individuals confidentiality;
- developing and delivering Information Governance Training to all staff;
- liaising with other committees, working groups and programme boards in order to promote and integrate IG standards;
- monitoring information handling activities to ensure compliance with law and guidance;
- providing a focal point for the resolution and/or discussion of IG issues.

5.5. Information Asset Owners (IAO)

Information Asset Owner (IAO) is also Verity Williams-Curnow her role is to;

- lead and foster a culture that values, protects and uses information for the benefit of patients;
- know what information comprises or is associated with the asset, and understand the nature and justification of information flows to and from the asset;
- know who has access to the asset, whether system or information, and why, and ensures access is monitored and compliant with policy;
- understand and address risks to the asset, and providing assurance to the SIRO.

5.6. Information Asset Administrator (IAA)

Information Asset Administrator is also Verity Williams Curnow she will ensure that policies and procedures are followed, recognise actual or potential security incidents, consult their IAO on incident management.

The IAA will be a member staff responsible for one or more information assets as nominated by the IAO for the area of responsibility.

5.7. Divisions, Services and Departments

Are responsible for:

- implementing good IG practice into normal everyday activity;
- providing evidence for the IG Toolkit when necessary;
- adhering to Information Governance related procedures;
- ensuring breaches/ and near misses relating to Information Governance are reported using the internal incident reporting procedure.

5.8. All Staff

All employees and anyone working on behalf of Echogenicity, involved in the receipt, handling or sharing of personal identifiable information, must adhere to this policy to support the reputation of Echogenicity and where relevant of their profession. Everyone has a duty to respect a data subject's rights to confidentiality.

6. Information Governance (IG)

Information Governance comprises a set of requirements relating to how organisations should process information. The requirements cover personal information relating to patients and employees and corporate information, for example financial and accounting records.

The main 'Acts of UK Parliament' and guidance documents that relate to Information Governance are as follows;

- The Data Protection Act 1998.
- The Common Law Duty of Confidentiality.
- Confidentiality: NHS Code of Practice.
- NHS Care Record Guarantee for England.
- Social Care Record Guarantee for England.
- The international information security standards: ISO/IEC 27002: 2013, ISO/IEC 27001: 2013; BS 7799.
- Information Security: NHS Code of Practice.
- Records Management: NHS Code of Practice.
- The Freedom of Information Act 2000.
- The Human Rights Act
- Caldicott Report 1997 - Report on the review of patient-identifiable information
- The Caldicott Review -Information: To Share or Not to Share? The Information Governance Review (also known as Caldicott 2 Recommendations)
- Information Security: NHS Code of Practice.

6.1. IG Toolkit (IGT)

The Information Governance Toolkit (IGT) is an online tool hosted and managed by the Health & Social Care Information Centre (HSCIC) that enables organisations to measure their performance against the information governance requirements,

The four fundamental aims of Information Governance are:

- to support the provision of high quality care by promoting the effective and appropriate use of information;
- to encourage staff to work closely together, prevent duplication of effort and enabling more efficient use of resources;
- to develop support arrangements and provide staff with appropriate tools to enable them to discharge their responsibilities to consistently high standards;
- to enable organisations to understand their own performance and manage improvement in a systematic and effective way.

The IGT has two functional aspects:-

- to provide interpretative advice and guidance;
- to provide NHS organisations with a means of self assessing performance against key aspects of

information governance. The IG Toolkit contains a set of six initiatives or work areas as described later in Section 7.

6.2. IG Self Assessment

The purpose of the assessment is to enable organisations to measure their compliance against the law and central guidance and to ensure 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, (e.g. assign responsibility, put in place policies, procedures, processes and guidance for staff), with the aim of making cultural changes and raising information governance standards through year on year improvements. The ultimate aim is to demonstrate that organisations can be trusted to maintain the confidentiality and security of personal information. This, in-turn, increases public confidence that 'the NHS' and its partners can be trusted with personal data. Organisations that are achieving an adequate level of performance (i.e. attainment at level 2 or above) against each of the requirements within the IG Toolkit can be regarded as trusted organisations for information sharing purposes where the purpose of sharing is for direct care.

6.3. IG Assurance Statement

As part of the IG Toolkit assessment organisations are required to comply and accept the national IG Assurance Statement. This statement contains additional terms and conditions applicable to all organisations using HSCIC services such as N3, and signifies an organisations' agreement to abide by those terms.

The IG Assurance Statement includes:

- The requirement that no Patient Identifiable Data or other sensitive data be stored or processed offshore where the location is deemed non-compliant with the HSCIC Offshore Policy;
- The right to audit by HSCIC or nominated third parties;
- Change Control Notification procedures and approvals processes;
- The requirements for reporting security events and incidents.

The IG Assurance Statement is a required element of the Information Governance Toolkit (IGT) and is re-affirmed by organisations' annual submission of the toolkit

6.4. IG Statement of Compliance (IGSoC)

The Information Governance Statement of Compliance (IGSoC) is the process by which organisations enter into an agreement with HSCIC for access to HSCIC's services, including the NHS National Network (N3), in order to preserve the integrity of those services.

The terms and conditions of access are set out in the IG Assurance Statement which is a required element of the IG Toolkit. It is essential that every organisation meets the obligations of the IG Toolkit, and complies with the IG Assurance Statement to the required standards to safeguard HSCIC services and information for all.

7. IG Toolkit Requirements

The IG Toolkit contains the following initiatives or work areas which include a number of requirements that Echogenicity must meet at level 2 compliance.

7.1. Information Governance Management

Echogenicity will annually self assess against the following requirements relating to Information Governance Management.

These require Echogenicity to:

- have an adequate Information Governance Management Framework to support the current and evolving Information Governance agenda;
- have formal contractual arrangements that include compliance with Information Governance requirements with all contractors and support organisations;
- ensure all types of employment contracts include compliance with Information Governance standards and are in place;
- have an approved programme of Information Governance awareness and mandatory training procedures to ensure all staff are appropriately trained.

7.2. Confidentiality and Data Protection Assurance

Echogenicity will annually self assess against the following requirements relating to Confidentiality and Data Protection Assurance.

These require Echogenicity to:

- ensure patients have ready access to information relating to their own health care, their options for treatment and their rights as patients;
- ensure arrangements are in place to support and promote information sharing for coordinated and integrated care;
- policies are embedded to ensure compliance with the Data Protection Act, Human Rights Act and the common law duty of confidentiality and all associated guidance;
- have appropriate procedures for recognising and responding to individuals requests for access to their personal data.

7.3. Information Security Assurance

Echogenicity will annually self assess against the following requirements relating to Information Security Assurance.

These require Echogenicity to:

- have an appointed a Senior Information Risk Officer (SIRO) at Board level;
- maintain policies along with respective procedures for the effective and secure use and management of all information assets, resources and ICT systems;
- have standards and protocols for the disclosure of information, and for the effective and secure transfer of information into and out of the Trust;
- undertake annual assessments and audits of its information and ICT security arrangements;
- undertake an annual Data Mapping Exercise across the Trust where all inbound and outbound flows of personal identifiable information are identified and risk assessed;
- have appropriate Information Sharing Agreements with partner organisations;
- promote effective information security and confidentiality practice to all staff through policies, procedures and training;
- Have business processes and procedures that satisfy Echogenicity obligations as a Registration Authority;
- ensure monitoring and enforcement processes are in place to ensure NHS national application Smartcard users comply with the terms and conditions of use;
- have business continuity plans that are tested for all critical information assets;
- have procedures to prevent information processing being interrupted or disrupted through equipment failure, environmental hazard or human error;
- have documented incident reporting procedures and investigate all reported instances of actual or potential breaches of information security and confidentiality;
- have a formal information security risk assessment and management programme for key information assets.

7.4. Clinical Information Assurance

Echogenicity will annually self assess against the following requirements relating to Clinical Information Assurance within the Information Governance Toolkit.

These require Echogenicity to:

- have and maintain policies and procedures for information quality assurance and the effective management of records;
- undertake annual assessments and audits of its information quality;
- have procedures to ensure the accuracy of service user information on all systems and records that support the provision of care;
- undertake clinical record audits across all specialties.

7.5. Secondary Use Assurance

Echogenicity will annually self assess against the following requirements relating to Secondary Use Assurance within the Information Governance Toolkit.

These require Echogenicity to:

- use local and national benchmarking to identify possible data quality issues and analyse trends in information;
- incorporate national data definition, standards, values and validation programmes within key systems;
- use external data quality reports to monitor and improve data quality;
- undertake annual clinical coding audits based on national standards;
- ensure clinical staff are involved in validating information derived from the recording of clinical care activity;
- ensure training programmes for clinical coding staff are comprehensive and conform to national clinical coding standards.

7.6. Corporate Information Management

Echogenicity will annually self assess against the following requirements relating to Corporate Information Assurance within the Information Governance Toolkit.

These require Echogenicity to:

- establish and implement policies and procedures for the effective management of corporate records;
- establish procedures to ensure compliance with the Freedom of Information Act 2000;
- ensure non-confidential information about the Trust and its services is available to the public through a variety of media, in line with Echogenicity FOI Publication Scheme;
- undertake audits of corporate records as part of the information lifecycle management strategy;
- promote records management through policies, procedures and training.

8. Information Governance Training

Annual Information Governance training has been made mandatory by the Department of Health in line with the NHS Operating Framework 2010/2011 that states all staff must receive annual basic IG training appropriate to their role. Ongoing awareness and training will be provided to all staff, in all sections of Echogenicity.

All staff must undertake Information Governance awareness training annually with all new starters completing the training within eight weeks commencing their employment.

There are two methods available to staff, either e-learning or Department of Health approved classroom based training.

In addition to IG training Echogenicity routinely promotes awareness relating to Information Governance issues at Senior Team Briefs and electronically to all staff via internal communication methods.

8.1. Classroom Based Training

Information Governance Training is included in Corporate Induction for all new starters and in annual update training for all clinical and non-clinical staff.

8.2. E-learning

Staff can access e-learning from their PCs from anywhere as all courses are internet based. Usernames and passwords are required to access the online training.

Training compliancy reports are compiled for all staff members which stored in each staff members personnel file. All personnel files and training are reviewed every year.

9. Key Governance Bodies

Not applicable – Echogenicity has one member of management, two echocardiographer's at present, two cardiologist, one administrator and two part time office workers. We are too small a concern to justify having governance bodies inhouse.

10. Incident Management

Incident reporting plays a major role in helping Echogenicity maintain a safe and secure working environment. It helps protect the confidentiality, integrity and availability of information and systems and is an essential element for effective risk management. Analysis of reported incidents enables Echogenicity to highlight areas of weakness and, if necessary, take appropriate action to reduce specific threats and vulnerabilities.

All staff members have a responsibility to report information security incidents by following Echogenicity's Incident & Serious Incidents Reporting and Management Policy.

11. Evaluation Measures

This policy will be reviewed against the IG Toolkit (IGT) to identify key areas for continuous improvement. Compliance will be monitored by Verity Williams Curnow in accordance with Echogenicity Assurance Framework.

12. References

Health & Social Care Information Governance Toolkit [online]. (2014) Available from: https://www.igt.hscic.gov.uk/HomeLoggedIn.aspx?tk=419806725561924&uid=174&c b=b6a0f3b4-5f4a-40ce-bd37-d2fb4fefd4ec&lnv=7&clnav=YES

Verity Williams-Curnow is responsible for all aspects of information governance.

Frequency of Meetings: once every six months unless an incident has occurred.

Equality Impact Assessment

Yes/No Comments

1. Does the policy/guidance affect one group less or more favourably than another on the basis of:

Race: No

Ethnic origins (including gypsies and travellers): No

Nationality: No

Gender: No

Culture: No

Religion or belief: No

Sexual orientation including lesbian, gay and bisexual people: No

Age: No

Disability - learning disabilities, physical disability, sensory impairment and mental health problems: No

Marriage & Civil partnership: No

1. Pregnancy & maternity

2. Is there any evidence that some groups are affected differently? No

3. If you have identified potential discrimination, are any exceptions valid, legal and/or justifiable?

4. Is the impact of the policy/guidance likely to be negative? No

5. If so can the impact be avoided? n/a

6. What alternatives are there to achieving the policy/guidance without the impact? n/a

7. Can we reduce the impact by taking different action? n/a

If you have identified a potential discriminatory impact of this procedural document, please refer it to Verity Williams Curnow together with any suggestions as to the action required to avoid/reduce this impact.