echogenicity

September 2019

www.echogenicity.co.uk

Information Governance Policy

Scanning Cornwall's Hearts

Table of Contents

Introduction 3
Definitions 3
Duties 4
Standards and Practice. 4
Legal Compliance. 5
Information Security. 5
Information Quality Assurance 5
Openness 6
Risk Management Strategy Implementation 6
Implementation & Dissemination 6
Training and Support 6
Document Control & Archiving Arrangements 6
Equality Impact Assessment 6
Process for Monitoring Effective Implementation 6
Associated Documentation. 6
References 7

Please Note the Intention of this Document This Information Governance policy provides an overview of the organisation's approach to information governance (IG); details about the IG management structures within the organisation and a guide to the policies and procedures in use. Implementation of this policy will help to ensure: That the principles of Information Governance are clearly understood; Personal identifiable data is managed in accordance with legislation and national standards; Roles and responsibilities are clearly defined and staff informed of those who can provide advice and support.

Review and Amendment Log
March 2015, March 2018
Next review March 2021

Introduction

Information Governance is a framework to bring together all of the requirements, standards and best practice that apply to the handling of information. It allows organisations and individuals to ensure that information is accurate, dealt with legally, securely and efficiently in order to deliver the best possible care. Information is a vital asset, in terms of both the clinical management of individual service users and the efficient management of services and resources. It plays a key part in clinical governance, service planning and performance management. It is therefore of paramount importance that information is efficiently managed, and that appropriate policies, procedures and management accountability provide a robust governance framework for information management. Echogenicity aims to work collaboratively with partner agencies to ensure any information governance issues which span more than one organisation are handled effectively and appropriately. To support this policy, Echogenicity will create and maintain policies and procedures to support compliance with the requirements contained in the Department of Health's Information Governance Toolkit (IGTK) – see section 7 for details of relevant supporting policies. This policy covers all aspects of information within the organisation, including but not limited to: Patient/ client/service user information Personnel information Organisational information

This policy covers all aspects of handling information, including (but not limited to): Structured record systems – paper and electronic -Transmission of information – e-mail, post, fax and telephone

This policy covers all information systems purchased, developed and managed by or on behalf of the organisation, and any individual directly employed or otherwise by the organisation.

Definitions

Definitions Information Governance – a framework that details how organisations must manage information about people and business. Information Governance Toolkit

The IG toolkit a on line tool developed by the Department of Health (DoH) that all organisations delivering NHS services are required to complete on an annual basis and to achieve level 2 compliance across all requirements in line with the NHS standard contract.

The DoH provide the Care Quality Commission with an annual report of organisation's compliance results, from which the CQC may then carry out random audits of an organisation's toolkit submission. The results are also available to the public through the toolkit website, which provides the public with assurance that organisations manage their information in a secure manner. Statement of Internal Control - All organisations that wish to use NHS Connecting for Health services, including the N3 network, must complete the IG Statement of Compliance process. The IG Toolkit is part of this process, in that organisations must carry out an annual assessment, evidence their compliance with the requirements and accept the IG Assurance Statement which confirms the organisation's commitment to meeting and maintaining the required standards of information governance. Personal Identifiable Information (PID) - data relating to a living individual who can be identified either from the data, or from the data in conjunction with other information in the possession of the data controller. Sensitive Information Data Protection Act 1998 definition: means personal data consisting of information as to— (a) the racial or ethnic origin of the data subject, (b) his political opinions, (c) his religious beliefs or other beliefs of a similar nature, (d) whether he is a member of a trade union (within the meaning of the [1992 c. 52.] Trade Union and Labour Relations (Consolidation) Act 1992), (e) his physical or mental health or condition, (f) his sexual life, (g) the commission or alleged commission by him of any offence, or (h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings. Data Subject - the individual person who is the subject of any relevant personal. Data Controller - a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed. Data Processor - in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

Processing - means obtaining, recording, holding of the information or carrying out any operation or set of operations on the data including adapting, altering, retrieving, disclosing, dissemination, and consulting. Safe Haven – processes that ensure that person identifiable and commercially sensitive data is transferred in a safe and secure manner.

All information used in Echogenicity is subject to handling by individuals and it is necessary for these individuals to be clear about their responsibilities. Echogenicity must ensure that support and appropriate education and training are provided for all staff. To manage its obligations Echogenicity will issue policies and procedures ensuring information is processed and shared correctly. All staff, whether permanent, temporary or contracted, and contractors are responsible for ensuring that they are aware of and comply with the requirements of Echogenicity's procedural documents. Failure to follow this and the associated policies and procedures will result in Echogenicity enforcing its disciplinary procedure. Managers are responsible for ensuring that policies and supporting standards and guidelines are built into local processes and that there is on-going compliance. Key responsibilities include: Ensuring staff are aware of, and act upon, Echogenicity's procedural documents. Implementing the procedural documents for the areas in which they apply. Notifying all new and existing staff on how to access procedural documents and ensuring that access is easily available. Ensuring that all staff members are aware of their responsibility in maintaining compliance with Echogenicity procedural documents.

Echogenicity is an extremely small community Echocardiogram service and as such The Chief Executive has the following roles; Accountable Officer also responsible for confidentiality management and decisions on patient data. The Chief Executive provides the board-level lead on IG and is responsible for managing Echogenicity information risk. The Chief Executive is responsible for providing leadership and guidance to Echogenicity's Information Asset Owners and ensuring that the organisations Information Asset Register is maintained. The SIRO/Data Protection officer is also the Chief Executive. Information Governance Lead is responsible at Corporate level for Information Governance (Chief Executive). Information Governance/Records Manager (Data Protection Officer who is also the Chief Executive) is responsible at the operational level, providing guidance and advice on information governance, including records management, and data protection issues conforming with legislative requirements and national standards. Information Asset Owners (Chief Executive) is also responsible for the information assets in their Service/ Business Unit. Key responsibilities include: Maintain an Information Asset Register. Know what information the Asset holds, what enters and leaves it and why – information flow mapping. Annual written risk assessment for the Information Asset reported to the Chief Executive. Ensure that there is a Business Continuity Plan is in place and that staff have easy access to it. Access control to the information asset – approves/authorises individuals access to information and carries out regular checks on the access and use of information. Approves and minimises information transfers while achieving business purposes. The Chief Executive also approves and oversees disposal mechanisms for information when there is no further requirement for it.

Duties

IT Security Team (Cornwall IT Shared Services) – The IT Security Team is responsible for all aspects of information security and risk management.

The IT Security Manager – Information Governance, provides Policy/IG/Risk Management support on meeting the IT aspects of the IG Toolkit. The IT Security Manager – Operational (RA Manager), provides technical day to day support.

Echogenicity is responsible for ensuring that sufficient resources are provided to support the requirements of the IG Strategy and Policy

Standards and Practice

Echogenicity undertakes to implement information governance effectively and will ensure the following: Information will be protected against unauthorised access; Confidentiality of information will be assured; Integrity of information will be maintained; Information will be supported by the highest quality data; Regulatory and legislative requirements will be met; Business continuity plans will be produced, maintained and tested; Information governance training will be available to all staff as necessary to their role; All breaches of confidentiality and information security, actual or suspected, will be reported and investigated. Echogenicity recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. Echogenicity 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. Echogenicity 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. Echogenicity will ensure that when sharing information with another organisation that the patient has given consent and that we are assured that the organisation is handling the information in accordance with the legislative and national requirements, through one or more of the following ways:- Level 2 compliance of the Information Governance Toolkit; Data Protection Registration with the Information Commissioner; Information Sharing Protocol. Checks and agreements are managed through the Information Governance Team and Information Asset Owners. Echogenicity Safehaven Guidelines for transporting PID and sharing information by post are available through the intranet document library for staff to display in their area. Pseudonymisation is a method which disguises the identity of patients by creating a pseudonym for each patient identifiable data item. This allows patient linking analysis needed within secondary uses. Staff should only have access to the data that is necessary for the completion of the business activity which they are involved in. This is reflected in the Caldicott Principles; access should be on a need to know basis. This principle applies to the use of PID for secondary or non-direct care purposes. By de-identification users are able to make use of patient data for a range of secondary purposes without having to access the identifiable data items. Echogenicity believes that accurate, timely, and relevant information is essential to deliver the highest quality health care. As such it is the responsibility of all clinicians and managers to ensure and promote the quality of information and to actively use information in decision making processes. There are 5 key interlinked strands to the IG policy: Legal compliance, Information security, Quality assurance, Training and awareness, Openness.

Legal Compliance

Echogenicity legal compliance by: Treating all person identifiable information relating to service users as confidential except for occasions where it is in receipt of a Court Order or where it is deemed in the wider public interest, or for a statutory right; Understanding that service users have the right to request access to information relating to their own health care, their options for treatment and their rights as service users. Disclosure of such information will be in line with the Data Protection Act (for living individuals) and Access to Health Records Act (for deceased individuals); Treating all person identifiable information relating to staff as confidential except where national policy on accountability and openness requires otherwise or, except for occasions where it is in receipt of a Court Order or, where it is deemed in the wider public interest, or for a statutory right; Establishing and maintaining policies and procedures to ensure compliance with Data Protection, Common Law Duty of Confidentiality, the NHS Code of Confidentiality and Human Rights Legislation; Ensuring effective confidentiality and security practice of its staff through induction and annual mandatory training and contract of employment clauses; Undertaking or commissioning annual assessments and audits of its compliance with legal requirements.

Information Security

Echogenicity will: undertake risk assessments to determine appropriate security controls are in place for existing or potential information systems; promote effective confidentiality and security practice to its staff through policies, procedures, induction and training; ensure that all transfers of information into, and out of Echogenicity are in compliance with anonymisation/ pseudonymisation principles where appropriate, safe haven guidance and information security standards; establish and maintain incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and security; use and or commission through shared services BS ISO/IEC 27001: 2005, BS ISO/IEC 27002: 2005 BS 7799-2: 2005 as the basis of its information security management arrangements. Echogenicity will seek to undertake or commission annual assessments and audits of its information.

Information Quality Assurance

Echogenicity will establish and maintain policies and procedures for information quality assurance based on the principals of high quality information being: Complete, Accurate, Reliable, Accessible, Timely and Undertake or commission annual assessments and audits of its information quality. The Chief Executive will to take ownership of, and seek to improve, the quality of information within their services. Wherever possible, information quality should be contemporaneously recorded, or assured at the point

of collection. Set data standards through clear and consistent definition of data items, in accordance with national standards. Promote information quality and effective records management through policies, procedures, induction and training. Health records standards have been set through the identification of best practice and in accordance with national standards and initiatives. To undertake or commission annual assessments and audits of its health record management systems. The Chief Executive are expected to ensure effective records management within Echogenicity. Openness; Echogenicity is not a public body and as such is not subject to the Freedom of Information Act 2000. However, in the interest of the public and Echogenicity's Code of Openness, non-confidential information about the organisation and its services is available to the public through a variety of media, including the organisations web site. Echogenicity has also agreed to work with the Commissioning body to answer any requests placed on them under their statutory duty. All requests for information should be directed to the Chief Executive. Echogenicity will undertake or commission annual assessments and audits of its policies and arrangements for openness. Procedures will be put in place to ensure that patients have appropriate access to information relating to their own health care, their options for treatment and their rights as patients. Echogenicity will have clear procedures and arrangements for liaison with the press and broadcasting media.

Risk Management Strategy Implementation

Implementation & Dissemination

This document will be sent to staff via email for them to absorb. A copy of this document will also be held in the IG tool kit file which is kept in the chief executive's office and is available for review on request.

Training and Support

Under contract the organisation is required to achieve 95 % of staff trained in Information Governance each year. All staff carry out Induction training on appointment and part of that training covers Information Governance. Thereafter, staff complete annual refresher Information Governance training. Training is available via: e-learning either through the National Learning Management System (NLMS) or through the NHS IG Training Tool. Classroom based sessions delivered by the training department. Ad hoc bespoke training provided by the Chief Executive.

Equality Impact Assessment

Echogenicity aims to design and implement services, policies and measures that meet the diverse needs of our service, population and workforce, ensuring that none are placed at a disadvantage over others. As part of its development, this strategy and its impact on equality have been assessed. The assessment is to minimise and if possible remove any disproportionate impact on employees on the grounds of race sex, disability, age, sexual orientation or religious belief. No detriment was identified.

Process for Monitoring Effective Implementation

The IGSC will, through the Information Governance Toolkit, monitor information governance standards and processes across the organisation throughout the year and will develop an going work plan to address any areas for improvement or development. The IGSC will commission and review an annual external audit report and make any necessary improvements and or develop an action plan prior to final IGTK submission on 31st March each year. Ad hoc audits will be carried out across the organisation as and when required and or in response to IG related reported incidents.

Associated Documentation

The following list details the most relevant policies that support the IG Strategy and Policy. The list it is not exhaustive and further policies may be added to the document library according to legislative and national standard requirements. . Acceptable Use; This policy defines what is acceptable and not acceptable use when using the Cornwall IT systems and the consequences of failing to follow the policy.

Access Control

This policy provides a robust and effective access control management for IT systems within Echogenicity to support the Information Security agenda Audio, Photographic and Video Recordings To provide clear guidelines and associated template forms regarding audio, photographic and video recordings, in line with legal requirements, for the staff of Echogenicity to utilise Caldicott Workplan This policy will explain the Caldicott function and its interoperability with other policies in operation within Peninsula Community Health Confidentiality Code of Conduct for Employees The

Confidentiality Code of Conduct for Employees is a key document for all staff. The Code provides guidance for staff around the areas of consent, confidentiality and information sharing. Information about the Caldicott Principles and the Data Protection Principles is included. Consent This policy provides guidance to staff regarding consent in a clinical setting. Data Protection The Data Protection Policy details how the organisation will meet its legal obligations under the Data Protection Act 1998, and explains the eight principles of the Data Protection Act. The policy also provides guidance on individual's rights under the Act Data Quality; Details the organisations expectations of data quality management from all staff and the national standards the organisation is required to meet. Email; The Email Policy and Procedure details how to ensure effective and appropriate use of email to reduce the risk of adverse events by setting out the rules governing the sending, receiving, and storing of email, including patient identifiable and commercially sensitive data; establishing Echogenicity user rights and responsibilities for the use of the system ; promoting awareness of and adherence to current legal requirements and NHS information governance standards. Forensic Readiness; The Forensic Readiness Policy sets out the action that will be taken by the organisation in the event of an information security incident where digital evidence is required. Incident Management; This policy sets out the roles and responsibilities of all staff in relation to incidents and the arrangements for reporting and management of all incidents, including near misses and serious untoward incidents. Information Risk Management. This policy lays down the framework for a formal information risk management programme within Echogenic by explicitly establishing responsibility for information risk management and its oversight, information risk identification and analysis processes and planning for information risk mitigation. Information Security; The Information Security Policy sets out the security management arrangements for the protection of patient records and key information systems IT System Security; The IT Security Policy; sets out guidance on the secure use and installation of IT systems and network security. Mobile IT Security; the purpose of this policy is to prevent unauthorised disclosure, modification, removal or destruction of the organisations information assets, and disruption to business activities. NHS Number; The NHS Number policy sets out how the organisation will ensure that the correct NHS number is recorded for each active patient and used routinely in clinical communications and documentation. Privacy Impact Assessments; This policy sets out how the organisation ensures that changes to policy, procedures and commissioned services are assessed to ensure that they do not adversely impact upon patient confidentiality. A full assessment process, form and guidance note is attached. Records Management; This Policy sets out how the organisation will manage its records effectively and ensure procedures are in place for the creation, use, storage, retention, tracking, availability, audit, retrieval and disposal of both its corporate/business and health records, in whatever format and media they are presented Registration Authority The NHS Smart Card and Registration Authority Policy sets out the responsibilities of the Registration Authority which issues and maintains electronic smart cards. Subject Access Requests This Policy and Procedure sets out how staff will manage Subject Access Requests (SAR's) effectively and ensure procedures are in place to deal with subject access requests under The Access to Health Records Act 1990 (AHR), The Access to Medical Reports Act 1988 (AMR) and The Data Protection Act (DPA) 1998.

References

NHS Information Governance Toolkit (Connecting for Health) https://nww.igt.connectingforhealth.nhs.uk/

NHS Code of Confidentiality 2003 http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/codes/confcode.pdf

The Data Protection Act 1998 http://www.opsi.gov.uk/Acts/Acts1998/ukpga_19980029_en_1

The Freedom of Information Act 2000 http://www.opsi.gov.uk/Acts/acts2000/ukpga_20000036_en_1

Records Management: NHS Code of Practice http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAn dGuidance/DH_4131747

Information Security Management: NHS Code of Practice http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/codes/securityco de.pdf

NHS Care Record Guarantee (2009) http://www.nigb.nhs.uk/guarantee/2009-nhs-crg.pdf

The Human Rights Act 1998 http://www.opsi.gov.uk/ACTS/acts1998/ukpga_19980042_en_1

Access to Health Records Act 1990 http://www.opsi.gov.uk/acts/acts1990/ukpga_19900023_en_1

Caldicott review of Patient Identifiable Information 1997 http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAn dGuidance/DH_4068403

The Chief Executive is responsible for the following;

Ensuring that the organisation achieves a minimum level of compliance, within specified timescales, against all IG Toolkit requirements:

Information Governance Management, Confidentiality and Data Protection Assurance, Information Security Assurance, Clinical Information Assurance

And to 'sign off' the Information Governance Toolkit return prior to submission in line with the timetable issued each year.

To ensure that Echogenicity has effective policies and management arrangements covering all aspects of information governance in line with the current legislation, NHS guidance/policies and professional codes of practice.

To provide support, advice and assistance.

To receive and consider reports into breaches of confidentiality and security and where appropriate undertake or recommend remedial action and when appropriate recommend the declaration of a Serious Incident and participate in investigations.

Communicate and assist in embedding information governance developments and standards to staff and appropriate forums.

Scrutinise and review the corporate IG Risk Register.

Ensure effective reporting of information governance matters to the CQSC.

To review and approve policy in relation to IG prior to submission.

Ensure requirements of Information Governance are incorporated into training strategy and compliance is monitored.

To ensure there is a robust framework for management of Information Assets including clear processes for the addition and removal of assets accompanied by regular audit to provide assurance that an asset register is accurate.

To establish an Information Governance improvement plan, secure the relevant resources and monitor implementation of the plan.

To ensure that Echogenicity develops and maintains an appropriate framework for the management and protection of information which is appropriately supported by information asset owners and administrators.

Appendix 2:

The Data Protection Act & Caldicott Report Principles
The Data Protection Act Principles state that personal information:

- Shall be processed and used fairly & lawfully;
- Shall not be used in any manner incompatible with the purpose for which it has been obtained;
- Shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are used;
- Shall be accurate;
- Shall not be kept for longer than is necessary;
- Shall be used in accordance with the rights of the individual;
- Appropriate measures shall be taken against unauthorised disclosure;
- Shall not be transferred to a country or territory outside the European Economic Area with inadequate levels of protection for the rights and freedoms of the person in relation to their information.*
- Connecting for Health states that no PID is to be sent outside the UK without a separate further contract.

NHS Caldicott Report Principles

- Justify the purpose(s) for using confidential information;
- Only use it when absolutely necessary;
- Use the minimum that is required;
- Access should be on a strict need-to-know basis;
- Everyone will understand his or her responsibilities;
- Understand and comply with the law.