



v1.0

www.echogenicity.co.uk

Data Protection Policy 2019

Table of Contents

1	Introduction.....	3
2	Purpose.....	3
3	Definitions.....	3
4	Duties / Responsibilities.....	3-4
5	Process.....	4-6
6	Consultation.....	6
7	Implementation.....	6
8	Training and Support.....	6
9	Review.....	6
10	Monitoring Compliance.....	6
11	References.....	6
12	Echogenicity Associated Documents.....	6

Scanning Cornwall's Hearts

1. Introduction

Echogenicity must ensure it meets its legal requirements under the Data Protection Act 1998.

Personal identifiable information (PID) or Personal Confidential Data (PCD) held by Echogenicity is an important and valuable asset. Echogenicity recognises that the lawful and correct treatment of personal data is very important in delivering an effective health service and maintaining confidence with its patients and the wider public.

This policy applies to patient and staff information held by Echogenicity.

2. Purpose

This policy provides staff with a comprehensive explanation of the requirements under which all personal identifiable data will be acquired, stored, processed and transferred in accordance with the Data Protection Act 1998, Caldicott principles and the “Guide to confidentiality in health and social care: Treating confidential information with respect” Health and Social Care Information Centre Version 1.1 September 2013

3. Definitions

3.1 Personal Information

This is information that relates to an individual person.

3.2 Personal Confidential Data (PCD)

Personal Confidential Data (PCD) is information that if used alone or together with other information would identify a living individual i.e. name, address, date of birth, nhs number etc.

3.3 Sensitive Information

Information becomes sensitive if it includes any of the following types of information about an identifiable, living individual: -

- racial or ethnic origin
- political opinions
- religious beliefs
- trade union membership

- physical or mental health
- sexual life
- commission of offences or alleged offences

Sensitive data could also include information that could affect the commercial standing or reputation of Echogenicity. For example, corporate information could include planning reports, end of year accounts prior to being published/approved etc this information is referred to as ‘organisationally sensitive’ information.

3.4 Database

A database is any collection of personal information that can be processed by automated means. A few examples are detailed below: -

- Patient records (names and addresses etc) for appointments.
- Patient information used for research e.g. where only NHS number (or other personal identifier may be allocated) and clinical details may be held – this could be an Excel spreadsheet.
- Staff records held on Excel to monitor annual leave and sickness.

4. Duties / Responsibilities

4.1 Chief Executive

The Chief Executive (Verity Williams Curnow) has ultimate accountability for data protection within Echogenicity, ensuring that it meets its requirements under current legislation. The Chief executive ensures procedures are implemented to ensure that Echogenicity meets its requirements under current legislation.

4.2 Caldicott Guardian

The Caldicott Guardian (Verity Williams Curnow) is responsible for Data Protection and patient confidentiality and provides regular reports.

The Caldicott Guardian has a particular role in overseeing the provision of internal advice in relation to Data Protection, especially in relation to legislation and confidentiality and the use of patient related information.

Scanning Cornwall's Hearts

4.4 Senior Information Risk Owner (SIRO)

The SIRO is Verity Williams Curnow and is responsible for the reporting of information security risks.

4.5 Head of Information Governance

The Head of Information Governance (Verity Williams Curnow) is responsible for the day to day management of data protection, ensuring procedures are developed and implemented.

The Head of Information Governance responsibilities include: -

- Maintaining registrations
- Advising on content of training sessions
- Dealing with subject access requests
- Acting as initial point of contact for any data protection issues which may arise
- Providing staff support and guidance on a day to day basis in regard to handling confidential and sensitive data

4.6 Staff

All staff are responsible for ensuring they comply with the principles of the Data Protection Act 1998 and the Caldicott Principles, this must be done by adhering to the Information Governance policies and procedures.

A breach of the Data Protection requirements could result in disciplinary action and/or criminal investigation where this is a specific breach of the Data Protection Act 1998. Disciplinary action will be taken in accordance with Echogenicity's Disciplinary Policy. Criminal matters will be reported to the Police as appropriate.

5. Process

5.1 Data Protection Principles and Caldicott Principles

There are eight principles of good practice within the Data Protection Act 1998 and seven key principles for handling personal and sensitive information arising from the Caldicott2 Review 2013 and as endorsed by the Government in Autumn 2013. (see appendix 1 & 2).

To ensure compliance with these principles Echogenicity will do the following: -

5.2 Individual's Rights

The Data Protection Act 1998 gives individual's the following rights:

- Right of subject access;
- Right to prevent processing likely to cause harm or distress;
- Right to prevent processing for the purposes of direct marketing;
- Right in relation to automated decision taking;
- Right to take action for compensation if the individual suffers damage;
- Right to take action to rectify, block, erase or destroy inaccurate data;
- Right to make a request to the Information Commissioner for an assessment to be made as to whether any provision of the Act has been contravened.

5.2.1 Subject Access Requests

Individual's whose information is held within Echogenicity have rights of access to it, regardless of the media the information may be held.

Individuals also have a right to complain if they believe that Echogenicity is not complying with the requirements of the Data Protection legislation. This includes where a data subject considers that information is not accurate or up-to-date. See Point

5.2.3 Echogenicity's Access to Health Records Policy has further details on applying for access and also what to do if not satisfied with information held or how being processed.

5.2.2 Compensation / Complaints

Individuals have the right to seek compensation if they feel Echogenicity has breached their rights under the Data Protection Act 1998.

Individuals have a right to make a complaint for any breach or suspected breach of the Data Protection Act 1998 that may cause them damage and/or distress.

Complaints should be made in adherence with the Echogenicity's Complaints Policy.

Scanning Cornwall's Hearts

5.2.3 Rectify Inaccurate Data

Individuals have the right to ask for inaccurate data to be rectified. This applies to factual inaccuracies.

Where individuals disagree with clinical opinions the record / information will not be erased, however a note will be made.

5.3 Fair Obtaining / Consent

There is a requirement to make the general public, who may use the services of the NHS, aware of why the NHS needs information about them, how this is used and to whom it may be disclosed.

Echogenicity is obliged under the Data Protection Act 1998 and Caldicott Principles to produce patient information leaflets and posters which are customised to its own uses of patient information.

5.4 Patient Notification

Patients will be made aware of this requirement by the use of information posters in patient waiting areas, statements in patient handbooks/on survey forms and verbally by those health care professionals providing care and treatment.

All patients should be informed of the purposes for which their information is collected and how it will be used at the first point of contact with clinical/care services. Echogenicity also has a leaflet that can be used as appropriate. These will also be available in symbol or other format for patients and users with special needs as appropriate.

5.5 Staff Notification

There must also be procedures to notify staff, temporary employees (volunteers, locums) etc. of the reasons why their information is required, how it will be used and to whom it may be disclosed. This takes place during induction and/ by their individual manager.

5.6 Registration / Notification

All organisations that hold and/or process personal information about living individuals must be registered with the Office of the Information Commissioner. This process is known as Notification. If Echogenicity fails to complete this process and fails to keep the information up to date it has committed a criminal offence and could face criminal prosecution.

The Head of Information Governance (Verity Williams Curnow) will ensure that Echogenicity's registration notification remains up-to-date and payment is made as required annually.

5.7 Accuracy / Data Quality

Echogenicity has to ensure that all information held on any media is accurate and up to date.

The accuracy of the information can be achieved by implementing validation routines, some of which will be system specific and details must be provided of these validation processes to the system/information users.

Users of software will be responsible for the quality (i.e. accuracy, timeliness, completeness) of their data by carrying out their own quality assurance and participating as required in quality assurance processes.

Staff should check with patients on a regular basis that the information held by Echogenicity is kept up to date by asking patients attending appointments to validate the information held.

Staff information should also be checked for accuracy on a regular basis – either by the manager or by the HR/ Personnel department.

Echogenicity's Data Quality Policy has further details.

5.8 Retention of Information

All records have a retention period regardless of the media they are held on.

Echogenicity's Health Records Management Policy has further details on how records must be retained.

5.9 Staff Information

Any member of staff current, past or potential (applicant) has the right to have a copy of information Echogenicity holds about them.

This must be done in accordance with Echogenicity's Access to Personal Employment Records Policy.

5.10 Contracts of Employment

All Echogenicity's Contracts of Employment include a data protection and confidentiality clause.

Scanning Cornwall's Hearts

5.11 Information Security

All information relating to identifiable individuals must be kept secure at all times. Echogenicity's Information Security Policy and Safe Haven Policy must be adhered to.

5.12 Disposal of Information

Echogenicity has a legal obligation to maintain confidentiality standards for all information from receipt through to disposal. Information must be disposed of in accordance with the Health Records Management Policy

5.13 Disclosure of Information

Information must only be disclosed on a strict need to know basis.

Disclosure of health records / information held within health records must be done in accordance with the Access to Health Records Policy.

Disclosure of staff personnel records / information must be done in accordance with the Access to Personal Employment Records Policy.

5.14 Sending Information outside of the EEA

(European Economic Area) If you need to send person identifiable information to countries outside of the EEA you must seek approval from Echogenicity's Caldicott Guardian.

Approval must be sought due to the levels of protection in other countries possibly not being as comprehensive as those in the UK.

6. Consultation

This policy has been developed by Verity Williams Curnow – A copy is available in Echogenicity's head Office.

7. Implementation

The information governance policies and procedures are discussed at induction and updated whenever new changes are made.

8. Training and Support

Data Protection will be included in the staff Induction and during mandatory training which is held on a yearly

basis.

9. Review

This Policy will be reviewed at least every 3 years by Verity Williams Curnow.

Information Governance meetings

Information Governance Breaches (including breaches of the Data Protection Act 1998).

11. References

- Data Protection Act 1998
 - Access to Health Records 1990
 - Caldicott Guardian Principles
 - Human Rights Act 1998
 - Freedom of Information Act 2000
 - Regulation of Investigatory Powers Act 2000
 - Department of Health Confidentiality NHS Code of Practice
 - The Data Retention and Investigatory Powers Act 2014
 - Caldicott Guardian Regulations
- ### 12. Echogenicity Associated Documents
- Freedom of Information Policy
 - Information Security Policy
 - Access to Health Records Policy
 - Data Quality Policy
 - Access to Personal Employment Records Policy
 - Safe Haven Policy

Scanning Cornwall's Hearts