echogenicity

v1.0

www.echogenicity.co.uk

# Confidentiality Code of Conduct for Employees

Scanning Cornwall's Hearts

## Table of Contents

**Please Note the Intention of this Document**

Purpose

The Confidentiality Code of Conduct for Employees has been created to:

- Provide guidance for staff to ensure awareness of responsibilities with regard to confidentiality;
- Provide staff with detailed guidance on the use and disclosure or person identifiable information;
- Provide staff with guidance on seeking consent to use personal information for purposes other than direct care;
- Provide staff with guidance on respecting patient choice and decisions;
- Demonstrate due diligence and good governance of the organisations information assets.

Appendix B: Signatory sheet for all staff to sign once policy read, managers to retain in personnel file.

March 2015 1.2 Extend Review date March 2018 Extend review date.

**1 Introduction**

Please note that this document should be read and understood prior to the contract of employment or other confidentiality agreement being signed. If there is anything that is not clear please contact your manager.

Purpose of the Code

All employees working in/with the NHS are bound by a legal duty of confidence to protect personal information they may come into contact with during the course of their work. This is not just a requirement of their contractual responsibilities but also a requirement within the

Data Protection Act 1998 and, in addition, for health and other professionals through their own professions Code(s) of Conduct including Code of Conduct for NHS Managers. The rights and pledges of the NHS Constitution have been taken into account in the development of this policy to ensure that the values and principles of the NHS are upheld.

This means that employees are obliged to keep any personal identifiable information strictly confidential e.g. patient and employee records. It should be noted that employees also come into contact with non-person identifiable information which should be also be treated with the same degree of care e.g. business "in confidence" information.

Disclosures and sharing of personal identifiable information are governed by the requirements of Acts of Parliament and government guidelines.

The principle behind this Code of Conduct is that no employee shall breach their legal duty of confidentiality, allow others to do so, or attempt to breach any of the Trust security systems or controls in order to do so.

**2 Definitions**

Contained within the policy.

**3 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 reviewed in consultation with trade union and other employee representatives in line with the Equality and Diversity Policy. The purpose of 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.

The Equality Impact Assessment Tool has been used to help consider the needs and assess the impact of this policy and has been completed alongside this document.

**4 Good Corporate Citizen**

As part of its development, this policy was reviewed in line with the Good Corporate Citizen Action Plan. The implementation of this strategy promotes good governance.

**5 Duties**

This section includes an overview of individual roles, departmental and committee duties including levels of responsibility for the management of this policy.

**5.1 Duties within the Organisation**

Key duties and accountabilities of directors, committees, specialist staff, and authors with responsibility for procedural documents are identified as:

Chief Executive: responsible for managing the implementation of this policy, for developing the procedural document in line with this policy, for reviewing the procedural document and providing feedback as part of the consultation process, for the final approval of the document prior to ratification. And also responsible for considering implications and ensuring implementation is achieved.

**5.2 Communication with Stakeholders**

Not applicable.

**6 Code of Conduct**

This Code has been produced to protect staff by making them aware of correct procedures so that they do not inadvertently breach any of the requirements of the law, policies, procedures and NHS codes of practice.

The Caldicott Principles

Principle 1 – Justify the purpose for using confidential information

Principle 2 – Only use it when absolutely necessary

Principle 3 – Use the minimum that is required

Principle 4 – Access should be on a strict need to know basis

Principle 5 – Everyone must understand their responsibilities

Principle 6 – Understand and comply with the law

**6.1 Detailed provisions**

Confidentiality of Information

All employees are responsible for maintaining the confidentiality of information gained during their employment by the organisation.

Definition of Confidential Information

Confidential information can be anything that relates to patients, staff (including noncontract, volunteers, bank and agency staff, locums, student placements), their family or friends, in whatever format held and stored. It also includes any organisational confidential information.

For example, information may be held on paper, floppy disc, CD, computer file or printout, video, photograph or even heard by word of mouth.

It includes information stored on portable devices such as laptops, palmtops, blackberries, mobile phones, memory sticks and digital cameras (this list is not exhaustive).

It can take many forms including medical notes, audits, employee records, occupational health records etc.

Person-identifiable information is anything that contains the means to identify a person, e.g.

name, address, postcode, date of birth, NHS number, National Insurance number etc. These can be identifiers individually or a combination of one or more of the above. Please note even a visual image (e.g. photograph) is sufficient to identify an individual.

Certain categories of information are legally defined as particularly sensitive and should be most carefully protected by additional requirements stated in legislation (e.g. information regarding in-vitro fertilisation, sexually transmitted diseases, adoption information, gender reassignment, HIV and termination of pregnancy).

There are no clear legal obligations of confidentiality that apply to the deceased. However, the Department of Health and the General Medical Council agree that there is an ethical obligation to the relatives of the deceased in requiring that confidentiality obligations continue to apply.

Requests for Information on Patients and Patient consent

Never give out information relating to patients or staff to persons who do not “need to know” in order to provide health care and treatment;

All requests for identifiable information should be based on a justified need and will be agreed by the chief executive.

Consent cannot be implied for purposes other than healthcare. Non healthcare purposes

could include disclosure to the police, to government departments other than the Department of Health, to the courts, etc. In most cases, patients should be asked for their explicit consent for information to be shared for non-care purposes.

Patients have a right to expect that information about them will be held in confidence by all NHS and health-care staff. Confidentiality is central to trust between health providers and patients. Without assurances about confidentiality, patients may be reluctant to give staff the information they need in order to provide good care. If you are asked to provide information about patients you must:

- be satisfied that patients know about disclosures necessary to provide their care, or for local clinical audit of that care, that they can object to these disclosures but have not done so (use the patient information leaflet: Protecting Your Data in discussions with the patient);
- ensure that patients requiring information to be provided in different format are referred to the Patient Advice Liaison Service;
- seek patients' explicit consent to disclosure of information, where identifiable data is needed for any purpose other than the provision of care or for clinical audit – save in the exceptional circumstances described below.
- You must treat information about patients and clients as confidential and use it only for the purposes for which it was given. As it is impractical to obtain consent every time you need to share information with others, you should ensure that patients and clients understand that some information may be made available to other members of the team involved in the delivery of care. You must guard against breaches of confidentiality by protecting information from improper disclosure at all times.
- You should seek patients' and clients' wishes regarding the sharing of information with their family and others. When a patient or client is considered incapable of giving permission, you should consult relevant colleagues. The duty of confidentiality owed to a person under 16 is as great as that owed to any other person. But if the young person or another person, is at risk of serious harm, which disclosure to an appropriate person would prevent, that the need for this will be explained.

If you are required to disclose information outside the team that will have personal consequences for patients or clients, you must obtain their consent. If the patient or client withholds consent, or if consent cannot be obtained for whatever reason, disclosures may be made only where:

- they can be justified in the public interest (usually where disclosure is essential to protect the patient or client or someone else from the risk of significant harm)
- they are required by law or by order of a court

Where there is an issue of child protection, you must act at all times in accordance with national and local policies.

Observe the principle that information given for one purpose may not be used for a different purpose without the permission of the informant.

Be aware that patients have a right to restrict disclosure of their personal information and as far as possible you must ensure that this right is adhered to and respected. This means that no one can make decisions about sharing this information on the patient's behalf. There are exceptions to this for parents or legal guardians, or people with powers under mental health law, eg the Mental Capacity Act 2005. Before sharing personal information about a person lacking capacity, the information holder should consider the following questions:

- Is the person asking for the information acting on behalf of the person who lacks capacity?
- Is disclosure in the best interests of the person who lack capacity?
- What kind of information is being requested?

It should be borne in mind that a patient has the right to change their mind about a disclosure decision at any time before the disclosure is made and can do so afterwards to prevent further disclosures where an activity requires a regular transfer of patient information.

If you have any concerns about disclosing/sharing patient information you must discuss with The chief executive.

Telephone Enquiries

If a request for information is made by telephone,

- Always try to check the identity of the caller and;
- Check whether they are entitled to the information they request;
- Take a number, verify it independently and call back if necessary.

Remember that even the fact that a patient is in hospital, a patient of the hospital/practice or a member of staff, is in itself confidential information. If in doubt consult the chief executive.

Requests for Information by the Police and media

- With respect to the Police, please refer to the chief executive
- With respect to the Media please refer to the chief executive

Disclosure of Information to Other Employees of the organisation

Information on patients should only be released on a need-to-know basis.

- Always check the member of staff is who they say they are. This can be achieved by checking the employee's ID badge and/or their internal extension number or bleep number prior to giving them any information;
- If possible also check whether they are entitled to the information;
- Don't be bullied into giving out information;
- Only give as much information as is absolutely necessary.

If in doubt, check with the health care professional in charge of the patient's care.

Abuse of Privilege

It is strictly forbidden for employee's to look at any information relating to their own family, friends or acquaintances unless they are directly involved in the patient's clinical care or with the employees administration on behalf of the organisation. Action of this kind will be viewed as a breach of confidentiality and may result in disciplinary action.

If you would like to see your own Health Record, you should make a Subject Access Request to the Chief Executive.

If you have concerns about this issue please discuss with Chief Executive.

Carelessness

- Do not talk about patients in public places or where you can be overheard;
- Do not leave any Health Records or confidential information lying around unattended;
- Make sure that computer screens and other displays of information are positioned to avoid unauthorised viewing;
- When leaving your office, ensure you lock your PC, (Ctrl + Alt + Delete. Lock – Workstation or Windows Key + L) or VDU;
- Secure all portable forms of data by locking them in a drawer;
- Lock your office;
- You should not share your password with anyone, no matter how senior.

Use of Internal and External Post

Best practice with regard to confidentiality requires that all correspondence containing personal information should always be addressed to a named recipient. This means personal information/data should be addressed to a person, a post holder, a consultant or a legitimate Safe Haven, but not to a department, a unit or an organisation. In cases where the mail is for a team it should be addressed to an agreed post holder or team leader.

Internal mail containing confidential data should only be sent in a securely sealed envelope, and marked accordingly, e.g. 'Confidential' or 'Addressee Only', as appropriate. When received in the department only the Addressee may open the envelope unless others are authorised to do so.

External Mail must also observe these rules. Special care should be taken with personal information sent in quantity, such as casenotes, or collections of patient records on paper, floppy disc or other media. These should be sent by Recorded Delivery or by NHS courier, to safeguard that these are only seen by the authorised recipient(s). In some circumstances it is also advisable to obtain a receipt as proof of delivery e.g. patient records to a solicitor.

Electronic media should be protected. Advice on how to protect files is available from the chief executive.

Case notes and other bulky material should only be transported in the approved boxes/bags and never in dustbin sacks, carrier bags or other containers. These containers should not be left unattended unless stored; waiting for collection in a secure area. The containers should only be taken and transported by the approved carrier.

Please contact the Chief Executive for guidance.

Faxing; Echogenicity does not fax any information.

Storage of Confidential Information

Paper-based confidential information should always be kept locked away and preferably in a room that is locked.

PC-based information should not be saved onto local hard drives or onto removable media, but onto the network. Encrypted memory sticks can be provided in some exceptional circumstances with the authorisation of the chief executive.

Disposal of Confidential Information

When disposing of paper-based person-identifiable information or confidential information always use a shredders or incinerator. Keep the waste in a secure place until it can be collected for secure disposal.

Computer and Photocopier printouts should either be shredded or disposed of as paperbased confidential waste.

Floppy discs/CDs containing confidential information must be destroyed by IT Services.

Computer files with confidential information no longer required must be deleted from the server if necessary in line with Records Management: NHS Code of Practice retention schedules.

Computer hard disks are usually destroyed/disposed of by the IT experts within the organisation to ensure all information is deleted from the disk, as even after re-formatting it is possible to gain access to the original data.

Patient Identifiable Information must be kept for a set period of time. This is outlined within the Records Management: NHS Code of Practice. The code indicates the minimum time for which both medical and business NHS records should be retained and sets out the legal obligations for all NHS bodies to keep proper records and the rules on archiving or destruction. There is a Records Management Strategy which has been endorsed by the Chief Executive

Further information is available from the Chief Executive.

Confidentiality of Passwords, PIN numbers, etc

Personal passwords, PIN numbers, etc issued to, or created by employees should be regarded as confidential and they must not be communicated to anyone.

- Passwords, PIN numbers, etc should not be written down.
- Passwords, PIN numbers, etc should not relate to the employee or the system being accessed.

You will be given more information about their control and format etc. when you receive your training and/or password, PIN, etc.

No employee should attempt to bypass or defeat the security systems or attempt to obtain or use passwords, PINs, etc or privileges issued to other employees. Any attempts to breach security should be immediately reported to the chief executive and may result in disciplinary action and/or legal proceedings.

Emailing Confidential Information

Please refer to the Email policy and Cornwall IT Services for help.

Working at home

The Organisation does not advocate the taking of person identifiable information or records home for any reason. If you feel you have reason to do so, you MUST contact the gain authorisation from the chief Executive.

If you do have a justifiable reason to take patient or corporate records home, you must ensure they are securely stored to prevent accidental or malicious access by non authorised people. It will be your responsibility to ensure they are recorded as being in your possession and that they are safely returned.

Copying of software

All computer software used within the organisation is regulated by license agreements. A breach of the agreement could lead to legal action against the organisation and/or the offender (member of staff).

It is important that software on the PCs/systems used for work purposes must not be copied and used for personal use. This would be a breach of the license agreement and/or the IT Security Policy.

**6.2 General provisions**

Interpretation:If any person requires an explanation concerning the interpretation or the relevance of this Code of Conduct, they should discuss the matter with the chief executive.

Compliance: A record is kept of everyone who accesses information held electronically which is audited and can be made available to the patient.

Non-Compliance:Non-compliance with this code of conduct by any person working for Echogenicity may result in disciplinary action being taken in accordance with the disciplinary procedure, and may lead to dismissal for gross misconduct and/or legal proceedings.

To obtain a copy of the disciplinary procedures please discuss with the chief executive.

The chief Executive should use the form in Appendix B to ensure that staff have read and signed to say they have understood the content of this code of conduct.

Amendments: This code will be amended as necessary to reflect the organisational development of policies and procedures and the changing needs of the NHS.

**7 Risk Management Strategy Implementation**

**7.1 Implementation**

This document should be read and understood by all prospective employees prior to the contract of employment or other confidentiality agreement being signed. It will also be available to all current employees through the documents library.

**7.2 Training and Support**

No formal training and support has been identified. However, additional help and support can be accessed through the employees line manager if they have difficulties understanding the content of this Policy.

**7.3 Dissemination**

Once ratified this policy will kept in Echogenicity's head office.

Staff will be made aware of its existence through emailing.

Confirmation of receipt is not required for this procedural document.

**7.4 Storing the Procedural Document**

The signed procedural document will be stored (hard copy) centrally.

**8 Process for Monitoring Effective Implementation**

Monitoring of compliance with the code will be by random checks and/or patient satisfaction surveys. Confidentiality audits will also be performed by visits to Echogenicity head office by the chief executive to ensure physical security of information.

Regular usage reports will be requested from the CITS Security Services team.

Identified breaches will be dealt with under the Disciplinary/Capability processes and also referred to the relevant professional body, where appropriate.

**9 Associated Documentation**

This document references the following supporting documents which should be referred to in conjunction with the document being developed.

- Data Protection Policy
- Subject Access Request Policy and Procedure
- Safehaven Policy and Procedure
- IT Security Policy
- Mobile IT Security Policy
- Mobile Data Media Security Policy
- Server Back Up Documents and Procedures
- Records Management Policy, Procedure and Strategy
- Serious Untoward Incident (SUI) Policy
- Acceptable use policy
- Email Policy
- Data Quality Policy
- Information Sharing Protocols and Agreements
- Disciplinary Policy
- Information Governance Policy

**10 References**

- The Copyright Designs and Patents Act
- The Mental Capacity Act 2005
- NHS Act 2006
- Health and Social Care Act 2001
- The Data Protection Act 1998
- The Human Rights Act 1998
- The Computer Misuse Act 1990
- Common Law Duty of Confidentiality
- NHS Care Records Guarantee
- The Caldicott Guardian Manual 2006
- Confidentiality: NHS Code of Practice
- Records Management: NHS code of practice
- BS ISO IEC 27002 2005 BS 7799 1 2009 Code of Practice
- Information Security Management: NHS Code of Practice

**APPENDIX A**

PLEASE RETAIN FOR YOUR INFORMATION

Chief Executive, Echogenicity limited, Trannack House, Bal Road, Lowertown, Helston TR13 0DA

Tel: 01326 560481

**APPENDIX B**

Your personal responsibility concerning security and confidentiality of information (relating to patients, staff and Echogenicity)

During the course of your time within Echogenicity buildings, you may acquire or have access to confidential information which must not be disclosed to any other person unless in pursuit of your duties or with specific permission given by a person on behalf of Echogenicity. This condition applies during your relationship with the organisation and after the relationship ceases.

Confidential information includes all information relating to Echogenicity and it's patients/clients and employees. Such information may relate to patient/client records, telephone enquiries about patients/clients or staff, electronic databases or methods of communication including spoken conversations, hand-written notes made containing patient information etc. If you are in doubt as to what information may be disclosed, you should check with the chief executive.

The Data Protection Act 1998 regulates the use of all information in all formats identifying living individuals (patients/clients and staff). The organisation is registered in accordance with this legislation. If you are found to have made an unauthorised disclosure or have used your position to access records without authorisation you may face disciplinary action, dismissal and/or legal action.

I understand that I am bound by a duty of confidentiality and agree to adhere to this Code of Conduct and the requirements of the Data Protection Act 1998 and will safeguard all person identifiable information in line with organisational policy and procedures.

PRINT NAME:

SIGNATURE:

DATE:

ON BEHALF OF ECHOGENICITY

WITNESS NAME:

SIGNATURE

DATE

Equality Impact Assessment Tool

To be completed and attached to any procedural document when submitted to the appropriate committee for consideration and approval.

Yes √

No X

Comments

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

- Race X
- Ethnic origins (including gypsies and travellers) X
- Nationality X
- Gender X
- Culture X
- Religion or belief X
- Sexual orientation including lesbian, gay, transgender and bisexual people X
- Age X
- Disability - learning disabilities, physical disability, sensory impairment and mental health problems X

2. Is there any evidence that some groups are affected differently?

No

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

N/A

4. Is the impact of the document/guidance likely to be negative?

N/A

5. If so, can the impact be avoided? N/A

6. What alternative is there to achieving the document/ 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 the Chief Executive, together with any suggestions as to the action required to avoid/reduce this impact.

For advice in respect of answering the above questions, please contact the Chief executive.