echogenicity

September 2019

www.echogenicity.co.uk

Safe Haven Policy

Scanning Cornwall's Hearts

Purpose

The aim of this policy is to ensure that the use and transfer of personal information is subject to the same strict controls, which already apply elsewhere, when confidential information is handled.

There is a requirement to reassure patients, staff and the public that information will be handled securely and safeguards are in place to ensure its security.

Applicable to: All staff who handle patient identifiable information or records.

Document Author: Information Governance

Ratified by and Date: Verity Williams Curnow Chief Executive

Date March 2015, March 2018,

Review Date: March 2021

Table of Contents

1. Introduction

1.1. The NHS holds large amounts of confidential information about individuals. The information belongs to them and the NHS is merely the custodian. Information should be treated with respect and integrity. Handle with care – it is everyone's responsibility to protect that information from inappropriate disclosure and to take every measure to ensure that patient identifiable information is not made available to unauthorised persons.

1.2. Personal or sensitive information must not be disclosed for any other purpose than direct patient care. No identifiable information must be disclosed for secondary uses such as Performance monitoring without specific permission from the Chief Executive.

2. Scope

2.1. This policy is concerned with the security of staff and patient information and is relevant to all staff groups who have access to staff and/or patient information for both primary and secondary purposes.

2.2. There is a requirement to reassure patients, staff and the public that information will be handled securely and that safeguards are in place to ensure its security. The aim of this policy is to ensure that the use of personal information is subject to the same strict controls which already apply elsewhere where confidential information is handled.

3. Definitions

3.1. Personal Identifiable Data (PID)

3.1.1. Personal Identifiable Data is data which can identify a person – in which the person is the focus of the data and which links that that individual to data which would be considered as private – e.g. name and private address, name and home telephone number, NHS number etc

3.1.2. Personal Sensitive Data is where a data set includes any of the following examples:

(This is not an exhaustive but rather an illustrative list)

- Health or Physical Information
- Sexuality
- Religious Beliefs
- Political Beliefs
- Criminal History

3.2 Anonymisation

3.2.1. Data can be considered to be anonymous where clinical or administrative information is separated from details that may permit the individual to be identified such as name, date of birth and postcode.

3.3. Pseudonymisation

3.3.1. Pseudonymisation is sometimes referred to as reversible anonymisation. Patient identifiers, such as name, address or NHS number, are substituted with a pseudonym, code or other unique references to information so that the data will only be identifiable to those who have a legitimate relationship to the data.

3.4 Primary Use

3.4.1 The use of patient level data for purposes which directly contribute to the diagnosis, care and treatment of an individual or the audit/assurance of the quality of the healthcare provided. This also includes relevant supporting administrative processes and data quality.

3.5. Secondary Use

3.5.1. The use of data for purposes which do not directly contribute to healthcare purposes such as; preventative medicine, medical research, audits (including financial audit), commissioning, contract monitoring and reporting facilities and the management of health and social care services. When Personal Identifiable Data is used for secondary use this should be limited and de-identified so that the secondary use is confidential.

3.6. Safe Haven

3.6.1. Although „Safe Haven" originally referred to the siting of secure fax machines, the meaning has since been expanded to encompass all secure points at which confidential information is received, held, processed, transferred and communicated securely. A Safe Haven could be a post room, reception office, a fax machine, or a virtual Safe Haven such as email address or data warehouse.

3.6.2. Where there are new Safe Havens, such as data warehouses, access must be strictly controlled and authorised by the Chief Executive. The new Safe

Haven will provide the means of restricting access to authorised users of identifiable data for secondary use purposes and will support de-identification of the identifiable data.

3.6.3. Echogenicity is committed to the principles of Safe Havens, and all efforts should be made to comply with these principles.

4. Duties

4.1. The Chief Executive has overall responsibility for confidentiality and data protection within the Echogenicity.

4.2. The Chief Executive has responsibility for ensuring the confidentiality of patient information.

4.3. The Chief Executive has overall responsibility for ensuring that this guidance is implemented and adhered to by all staff.

4.4. The Chief Executive is responsible for implementing Data Protection procedures within the Trust.

4.5. The Chief Executive is responsible for maintaining a Data Flow register, in line with New Safe Haven requirements, detailing all flows of patient identifiable information.

4.6. All managers are responsible for ensuring that their staff are fully informed of this guidance and practice the principles.

4.7. All staff who process personal identifiable information have a responsibility to ensure the movement of information is carried out in a secure manner in line with all Trust policies and procedures.

5. Requirements for a physical Safe Haven

5.1. In order to constitute a Safe Haven, the following location/security arrangements should be in place for all Trust areas which receive, process or hold confidential information:

- It should be a room that is locked or accessible only to authorised staff or;
- The office or workspace should be sited in such a way that only authorised staff can enter that location
- If sited on the ground floor any windows should have locks on them
- The room should conform to health and safety requirements in terms of fire, safety from flood, theft or environmental damage
- Manual paper records containing person identifiable information should be stored in locked cabinets when not in use
- Desks should be cleared of any personal information at the end of every working shift
- Computers should be not left on view or accessible to unauthorised staff, and should have a secure screen saver function and be switched off when not in use
- Equipment such as fax machines, printers or copiers, in the Safe Haven should have an access code and be turned off out of office hours

6. Before Information is shared

6.1. Before sending information, staff must consider the security of the information when it reaches its destination. This is particularly relevant when sending information outside of the Trust. If there is any doubt regarding the security of the information, staff need to stipulate the basis upon which the information was provided, if there are any conditions attached to the release and what the recipient is to do with the information when it's agreed use has been completed e.g. the information is destroyed, deleted or returned etc.

6.2. If information is being provided for a specific purpose, a process should be put in place before the transfer of data detailing the procedure for the documentation to be returned by a set time frame. It is the sender's responsibility to review this process and ensure all documentation is returned as agreed.

7. Communications by Post

When sending correspondence that contains sensitive or confidential information sufficient measures should be taken to minimise the likelihood of the information being accessed by an unauthorised recipient.

7.1. Addressing Letters

7.1.1. When addressing a letter, sufficient care should be taken to ensure that the name and address of the recipient has been written correctly.

7.1.2. If the letter is being sent to a patient, the address should be checked against the Health Record (RiO/KITS or the paper records for services that do not use RiO/KITS), to ensure accuracy. If there is discrepancy or uncertainty about the accurate address, the recipient should be contacted by telephone for confirmation.

7.1.3. If the letter is being sent to a recipient other than a patient, if there is a telephone number or email address for the recipient, contact them to confirm address details.

7.1.4. If you have partial details but not the full address, use Royal Mail Postcode and Address Finder to find the full details: http://www.royalmail.com/postcode-finder

7.2. Checking and Signing

7.2.1. Particular care should be taken when a letter has been handwritten and is then typed by another member of staff. Misinterpretation of the details could lead to the letter being incorrectly addressed.

7.2.2. Where a letter has been typed, the member of staff who typed the letter should ensure that is checked for accuracy and signed by the author. Clinicians are expected to check the address as well as the content of the letter when signing. A record should be kept on the file copy of who checked and signed the letter.

7.2.3. If this is not possible, or the letter is a standard appointment letter etc., another member of staff should be asked to check the typed letter against the draft/template for accuracy and on behalf of the author. If the letter contains medication information, it must always be checked and signed by a clinician.

7.3. Envelopes

7.3.1. Where possible, window envelopes should be used. Incidents have occurred in the past where letters have mistakenly been put inside envelopes addressed to another person, leading to a breach in confidentiality. Using a window envelope negates this risk.

7.3.2. Care should be taken to ensure only the recipient and address is displayed in the window.

7.3.3. If it is not possible to use a window envelope, for example where the recipient has been copied into the letter, specific attention must be paid to ensure that the envelope is correctly addressed and only the intended letter inserted.

7.3.4. The envelope must be labelled above the addressee details, with the words „Private and Confidential. The envelope must also be marked with the following message:

If undelivered please return to:

Echogenicity, 2 Beacon House, Beacon Road, St. Agnes.
TR5 0NE

7.4. Bulk Transfers

7.4.1. Bulk transfer of confidential information (which means 50 personal details or more). This occurs twice a month. Firstly, when Echogenicity sends information regarding statistic's and patient waiting times to the Department of Health. The administrator compiles the information on an encrypted computer, these statistic are then emailed to the DoH via Kernow CCG via the NHS email system. Kernow CCG uses an N3 secure network.

Secondly when we send our monthly invoice is emailed to Kernow CCG via the secure NHS email system, all patient identifiable information is removed accepting the patients NHS patient number.

8. Use of Fax Machines

Echogenicity does not fax information due to its lack of security. Echogenicity's head office has a scanner, information is then electronically sent by NHS secure email, or the required information may be typed into the body of an email. If this is not possible the information would have to be posted.

9. Use of Email

9.1. Sending Confidential Information by Email

9.1.1. Any emails containing confidential information must be titled in the subject bar as 'Confidential Patient Information'.

9.1.2. Staff should avoid using numerous patient identifiers, such as full name, address, etc, and should limit the identifiable information to NHS Number or patient initials where possible.

9.1.3. Staff should consider whether confidential information needs to be sent by email or whether alternative options are available, such as saving the data onto a mutually accessible shared drive.

9.1.4. You should never include a patient identifier (such as name, initials or NHS Number) in the subject bar of an email.

9.1.5. Personal Email Accounts - All Trust employees are provided with an NHS email account.

The use of personal emails, such as Hotmail, Yahoo or Gmail is strictly forbidden for all Echogenicity business

9.1.6. It is the sender" s responsibility to ensure that all the information being sent is correct and that the recipient" s details are correct.

9.2. Use of Groupwise

9.2.1. The Cornwall Health Community presently uses Groupwise as an email solution. All emails sent within the local Groupwise environment (i.e., ending in cornwall.nhs.uk) are automatically encrypted end to end, and are secure.

9.2.2. When emails leave the Cornwall Health Community Network (outside of Groupwise), the security cannot be guaranteed. To resolve this, all emails leaving the community are scanned for information that may contain personal information. Any identified emails are automatically encrypted using the Cisco Registered Envelope Service. Recipients have to register using the link that is provided in an initial e-mail to decrypt the email before being able to read it and view any attachments. However, not all such emails may be identified.

9.2.3. Users should encrypt their own emails by including [encrypt] in the subject header. Such e-mails are encrypted in the same manner and the recipient can register for and decrypt these messages in the same way as described above.

9.3. Use of NHS.net

9.3.1. Some staff or departments may have an additional NHS Mail (nhs.net) account which may be used for the secure transfer of person identifiable information to other nhs.net recipients.

If an individual or department regularly shares information through email with public authorities including; other NHS Trusts that use nhs.net, the Police, Cornwall Council or schools, they should consider using an NHS.net email account for
these transactions.

Emails from these accounts are secure if they are sent to the following:

- nhs.net nhs.net
- nhs.net gsi.gov.uk
- nhs.net pnn.gov.uk
- nhs.net police.uk
- nhs.net gse.gov.uk
- nhs.net gsx.gov.uk
- nhs.net cjsm.net
- nhs.net sch.gov.uk
- nhs.net gcsx.gov.uk
- nhs.net mod.uk

9.3.2. To establish an NHS.net email account, staff should contact Cornwall IT Services:

CITS.Servicedesk@Cornwall.NHS.UK or telephone 01209 881717.

9.3.3. You must confirm that the recipient has received your email, by either of the following:

- Include a message asking for confirmation of receipt of the email
- Use the tracking status within the email software
- Once the email has been sent look at the properties to see if it has been opened

9.4. Emailing Clinical Information to GP Practices

9.4.1. E-mailing clinical correspondence to surgeries within Cornwall from Cornwall Partnership NHS Foundation Trust clinical teams has been established. Each GP practice has a generic email account and all incoming confidential email for the practice should be sent to this address. The e-mail account will be in the style letters.mysurgery@cornwall.nhs.uk e.g. Letters.Alverton@Cornwall.NHS.UK

9.4.2. Each surgery may have more than one e-mail address so it is important to check the correct address with the surgery before sending if in doubt.

9.4.3. Clinical email should only be sent to the generic letters accounts, NEVER to the personal account of a doctor. The generic accounts are monitored at least once a day by practice staff. However personal accounts may remain unopened for weeks on end if the doctor is on leave or sick leave. In effect email sent to personal accounts lands in a "locked box" to which only one person has the key (password). Until that person opens the box, no one even knows the email exists.

10. Use of Computers / Laptops

10.1. Access to any PC or laptop must be password protected, passwords must not be shared.

10.2. Computer screens must not be left on view so members of the general public or staff who do not a justified need to view the information can see personal data.

10.3. PCs or laptops not in use should be switched off or have a secure screen saver device in use.

10.4. Information should be held on the organisation's network servers, not stored on local hard drives. Departments should be aware of the high risk of storing information locally and take appropriate security measures.

10.5. All laptops and data-sticks must be issued and encrypted by Cornwall IT Services.

11. Unacceptable Electronic Communication

11.1 The applications detailed below cannot guarantee the adhesion to Safe Haven Principles, and have additional controls placed upon them.

11.2 Social Networking Sites - The Use of Social Networking sites such as Twitter or Facebook to exchange personal information relating to Trust service users, staff or business is strictly forbidden. Please refer to the Trust Social Media Guidelines for more guidance on the use of Social Networking Sites.

11.3 Instant Messaging - The use of applications such as Yahoo Messenger or MSN Messenger to exchange personal information relating to Trust service users, staff or business is strictly forbidden.

11.4 Personal Email Accounts - All Trust employees are provided with an NHS email account.

The use of personal emails, such as Hotmail, Yahoo or Gmail is strictly forbidden for all Trust business.

11.5. Personal Web Servers – The use of personal or third party web sites, including sites that offer a commercial file transfer service, sometimes referred to as FTP, to exchange person identifiable information relating to Trust service users, staff or business is strictly forbidden.

12. Personal Responsibility

12.1. All staff have a personal responsibility to ensure that all personal or sensitive information is sent and received in a secure and confidential manner.

12.2. Before sending information, staff must consider the security of the information when it reaches its destination, e.g. will it be held securely, destroyed, etc. This is particularly relevant when sending information outside of the Trust. If there is any doubt regarding the security of the information, staff need to stipulate the basis upon which the information was provided, if there are any conditions attached to the release and what the recipient is to do with the information when this has concluded.

12.3. Any incidents regarding a breach of this should be reported immediately in line with the

Echogenicity's Incident Reporting Policy.

12.4. It is the sender's responsibility to ensure that all the information being sent is correct and that the recipient's details are correct.

12.5. Staff may face disciplinary procedures if they knowingly send patient information to an inappropriate person or a non-Safe Haven.

13. Monitoring Compliance

13.1. The Chief Executive is responsible for the overall monitoring of compliance with and effectiveness of this policy.

13.2. The Chief Executive will maintain a current register of all data flows containing personal identifiable information and will develop and implement new processes, procedures and guidance as appropriate.

13.3. All breaches in confidentiality are to be reported via Echogenicity's incident reporting system, Safeguard. Incidents will be reviewed by the Chief Executive for review and action as appropriate.