CONTROLLED DOCUMENT

University Hospitals Birmingham
NHS Foundation Trust

Safe Haven Procedure
(Transferring Information Securely)

CATEGORY:	Procedure
CLASSIFICATION:	Information Governance
PURPOSE:	Trust's approach to the management of safe haven. It details how staff should transfer person identifiable information into and out of the Trust. This procedure also includes transfers between wards and departments.
Controlled Document Number:	1153
Version Number:	1_01
Controlled Document Sponsor:	Director of Corporate Affairs
Controlled Document Lead:	Information Governance Lead
Approved By:	Director of Corporate Affairs
On:	November 2018
Review Date:	November 2020
Distribution: • **Essential Reading for:** • **Information for:**	All staff

Contents

1. Procedure Statement

1.1 The purpose of this procedure is to maintain the privacy and confidentiality of the personal information held and transferred by the Trust. The implementation of these procedures facilitates compliance with the legal requirements placed upon the organisation, especially concerning sensitive information.

1.2 The NHS has used the concept of Safe Havens for over 20 years to ensure the secure transfer of Patient Identifiable information by post, email etc. The new safe haven principles include the concept of restricting access to patient identifiable information by de-identifying records used for secondary use purposes – through anonymisation or pseudonymisation of the information.

1.3 The procedure aims to set out practical guidelines for staff to ensure that the transfer of person identifiable information is undertaken according to the Caldicott Principles, confidentiality code and Data Protection Act.

2. Scope

2.1 Safe haven principles should be applied to information captured and transferred using any method of transfer, including but not limited to:

- Email
- Post (surface mail)
- Manual records (including message books, diaries etc.)
- Computers and computer systems
- Facsimile Machines (Fax), Photocopiers and Printers
- Answering machines

3. Definitions

3.1 Safe Haven

The term safe haven is a location (or in some cases a piece of equipment) situated on Trust premises where arrangements and procedures are in place to ensure personal identifiable information can be held, received and communicated securely.

3.2 Personal Information/ Data

Personal information is information which can identify a person – in which the person is the focus of the information and which links that

individual to details which could be regarded as private e.g. name and date of birth, NHS number, next of kin's details, carer details, address, postcode, etc. This also includes pseudonymised data.

3.3 **Special Category** (**Sensitive**) **Personal Information**

Special category personal information is where the personal information contains details of that person's:

a) Physical and/ or mental health

b) Sexual orientation and sexual life

c) Ethnic origin

d) Religious beliefs

e) Political views

f) Criminal convictions

g) Generic material

3.4 **Anonymised Data**

Data is "effectively anonymised" when the recipient is unable to infer the identity of individuals from the data without the application of effort or resource where it would be unreasonable to anticipate in the circumstances that apply.

3.5 **Pseudonymised Data**

The process of replacing person identifiers in a dataset with other values (pseudonyms) from which the identities of individuals cannot be intrinsically inferred/ identified. Examples of this process are replacing an NHS number with another random number, replacing a name with a code or replacing an address with a location code. The correct application of this process will produce the same pseudonym for a patient across different data sets and time so that patient data can still be linked.

3.6 **Secondary Uses (Non-Healthcare Medical Purposes)**

A secondary use of data is any use which is not covered in the definition of a primary use. In essence it relates to the use of patient identifiable information which does not directly contribute to the safe care of the individual concerned. Examples of secondary use of patient data include performance management, commissioning and contract monitoring.

4. Standards

4.1 Secondary Use

Person Identifiable Data (PID) may only be used for Non-Healthcare Purposes ("Secondary Uses") where there is explicit consent, use is covered by legislation, or where Section 251 approval (of the NHS Act 2006) has been obtained.

4.2 Sharing Secondary Use Information with Other Organisations

4.2.1 Where information is required to be shared for secondary use purposes and a legal basis exists, it is essential that this is done securely. Information should be de-identified for Non-Healthcare Medical Purposes (Secondary Uses).

4.2.2 Business processes requiring the secondary use of information must be undertaken with de-identified information. Any business processes using patient identifiable information must be modified to ensure compliance with this policy and associated pseudonymisation procedure.

4.3 De-identification of Data

4.3.1 Anonymisation: Individuals should only have access to identifiable information relating to the business process that they are directly involved in. This is covered in the Caldicott principle 'access should be on a need to know basis'. This principle also applies to secondary use of that information. The aim of anonymisation is to obscure the identifying items so that the individual cannot be identified. De-identification can be achieved by: Removing patient identifiers; the use of identifier ranges, for example; value ranges instead of age etc.

4.3.2 Pseudonymisation: To effectively pseudonymise data the Trust pseudonymisation procedure must be followed. Two key rules are:

a) **Each field of PID (data subject) must have a unique pseudonym;**

b) Pseudonymised data should have the same security as PID.

CAVEAT: Careful consideration must be given to fields that whilst not individually identifiable data, once combined could become identifiable. For example a data set regarding patients diagnosis at a particular GP practice- the GP practice provides a geographical area, an age range could further minimise numbers and ethnicity where there may only be

a couple of data subjects of that ethnicity. Good practice is not to release information where figures are less than 5.

4.4 Physical Security/ Storage Requirements

4.4.1 The physical security of areas is of utmost importance and there are some key principles that must be considered:

a) Personal, confidential, and sensitive records must be stored in locked drawers or cabinets, in a locked office area with secure entry security system e.g. locked or accessible via a coded key pad known only to authorised staff, limited to staff working for the Service or approved on behalf of the Trust.

b) The office or workspace should be sited in a way that only authorised staff can enter that location i.e. not an area which is readily accessible to any member of **staff** who work in the same building or office, or any visitors

.

c) If sited on the ground floor any windows should have locks on them

.

d) Consider if windows need to be obscured to prevent people viewing personal data through them, e.g. privacy screens.

e) Unauthorised people will not be allowed access to areas where **personal** and confidential information is kept unless supervised. ID badges will be checked before access is permitted.

4.5 Good Practice

4.5.1 Communicating by Email

- Always consider first if email is the best way to send the information. The transfer of personal identifiable data is only permitted via approved email routes to ensure the security of that information.

NB: Whilst HGS and **QE align systems following the merger there will be** some **differences in how staff ensure secure email communication.**

- **Trust** provided email accounts should not be used to send personal information to another email, as these although low risk will not be secure (i.e. those ending in .nhs.uk).

- Within the Trust use your standard email account:
  - heartofengland.nhs.uk to heartofengland.nhs.uk
  - uhb.nhs.uk to uhb.nhs.uk
  - uhb.nhs.uk to heartofengland.nhs.uk – and vice versa (This is an exception to the above rule as additional security has been put in place to ensure this transfer is secure despite being 2 external systems)
- When emailing externally use:
  - NHS.net. (To set up an account contact ICT. Both sender and recipient must use an NHS.net account if in the NHS).

or,

  - Encryption/Data Loss Prevention (DLP) facility built within UHB email system or NHS.Net

If staff need to send personal information to an external party they must always look to send from an NHS.Net account or encryption tool/DLP to another secure email system. If the external organisation does not have access to a secure system (as detailed below) staff should use an encryption solution as appropriate.

The following systems are able to process emails securely from NHS.Net mail accounts:

Secure email system	**Email Addresses**
Public sector organisations connected to the GSI, GSX and xGSI systems	*.gsi.gov.uk *.gcsx.gov.uk *.gsx.gov.uk
NHS Organisations	*.nhs.net
Private sector organisations connected to the GSI who meet the required security standards	*.gse.gov.uk
English and Welsh local authorities connected to the GCSX community through the Government Connect Programme	*.gcsx.gov.uk
The Police National Network or Criminal Justice Exchange	*.pnn.police.uk *.pnn.gov.uk
Private sector organisations connected to the Police National Network (scn.gov.uk)	*scn.gov.uk
The Criminal Justice Secure eMail service provided by CJIT and Ministry of Defence	*cjsm.net *.mod.uk *.mod.gov.uk

- Personal/ Confidential information should only be sent externally if essential and legitimate. (See the Trust Data Protection Policy).

- Only send the minimum information required (e.g. use initials, Date of Birth, reference number such as NHS number that the recipient can verify) instead of full client name and address details where possible.

- Internet Service Provider (ISP) e-mail accounts, e.g. Hotmail and Yahoo, must not be used for sending/ receiving ANY Trust business.

- If using a distribution list, always ensure that the distribution lists contains only those individuals who are authorised to receive the information.

- Do not send or forward person identifiable, information by email to any person or organisation that is not specifically authorised to receive and view that information.

- Do not set up auto forward of e-mail to an unsecure e-mail address.

4.5.2 **Computers and the Use of Electronic Systems**

- Access to any computer must be password protected in line with current IT access control rules.

  - Logins and passwords must not be shared.[1] This is a possible disciplinary offence.

- Computer screens must not be left where information can be seen by the public or staff who do not have a justified need to view the information.

  - The 'Ctrl/Alt/Delete'/ 'Return combination will lock a computer and must be used when staff are logged in but absent from their computer.

- Trust information should be saved to relevant Trust networks/ servers/system, and must not be stored on local hard drives or personal drives.

- Only Trust issued/ approved equipment can be used by staff when dealing with Trust business, e.g. Trust issued encrypted memory sticks.

[1] Users should have individual logins and not shared logins so that access can be audited

- Electronic **media** (e.g. CDs) being transported **must be approved by ICT and** encrypted**,** be properly packaged and clearly labelled.

4.5.3 **Fax Machines**

- Given the number of incidents relating to the use of Fax that have been reported to the Information Commissioner (and where fines have been issued) the use of Fax is actively discouraged unless absolutely necessary.

Person identifiable, confidential and sensitive information should only be sent by fax in exceptional **circumstances where other transfer methods are deemed unavailable.**

- It is the responsibility of line managers in their individual departments to identify safe haven fax machines, and to ensure that there is a label stating both the asset number, and the words 'Safe Haven' affixed to each machine. Safe haven fax machines should be located in a secure area away from public access.

- The steps below will help ensure confidentiality is maintained:

  a) Make a telephone call to the recipient to inform them that a fax containing person identifiable, confidential and/ or sensitive information is being sent, and request confirmation of receipt of the fax.

  b) Double check the fax number before sending and request a report sheet to confirm the transmission was successful and for regular recipients programme the fax number into the machine.

  - If it is the first time you are sending a fax to a new number or the number is not already pre-programmed into your machine, you need to pre-programme the number and then send a test fax and ask the recipient to confirm that they have received it before sending the fax containing personal sensitive information.

  c) The standard Trust cover sheet should be sent with the fax, which contains a confidentiality disclaimer to the effect of 'This fax is confidential and is intended for the person whom it is addressed.' State who the intended recipient is, and how many pages are being transmitted.

d) Don't leave the information unattended whilst it is being transmitted

e) Never send a fax to an unsupervised fax machine, unless it is a designated 'safe haven' or 'secure' machine and ensure that an appropriate person is available to receive the fax.

f) Do not send large amounts of information containing person identifiable, confidential information by fax. Only send the minimum amount of data required, and if possible anonymised by using reference numbers etc…

CAVEAT: Staff must not fax discharge summaries to GP's as this is a breach of national contract. Discharge summaries should either be sent via Electronic Document Transfer or NHSMail to NHSMail. If these are not available to staff they should send the summaries via post.

4.5.4 **Portable Electronic Devices**

- Reference should be made to the Trust's Mobile Computing Policy which makes it clear that person identifiable information must not be held or transported on portable devices unless they are encrypted.

- Staff should only be using devices supplied by the Trust; this includes laptops and desktops connecting to the network on-site or from home.

- Encryption also applies to any USB sticks, CDs or DVDs, PDA, Blackberry or smartphone that can store PID/sensitive data.

- For further clarification staff should contact ICT and they will arrange a visit to encrypt or collect your portable device.

4.5.5 **Communicating by Mail**

- Confidential information including health records information, letters and other documents are commonly moved around the organisation and between different organisations, it is essential that it is protected from unauthorised access and environmental damage at the time it is in transit.

- The steps below should help with sending confidential information, including health records, by post.

a) Confirm full name, department and address of recipient (always send to a named individual or role, e.g. Information Governance Lead, and not just UHB Trust or Mr Joe Bloggs, 1 Acacia Avenue, and not just an address)

b) Packing records:

Internal:

- The Trust supplies a number of envelopes - when personal/ confidential information is being transferred internally, envelopes which can be sealed must be used; not internal envelopes.

- If health records of any nature, they should be transported in secure containers to protect from loss, unauthorised access or accidental viewing (e.g. lockable satchels, boxes, robust bags etc).

- Ensure 'Internal' is printed on the front of envelopes.

External:

- Ensure appropriate envelopes are used that are suitable for the volume of data, they are secured and if needed taped.

  - Use strong devices/ pouches where information is of high volume, e.g. copies of clinical records to service users as a result of a Subject Access Request.

Addressing*:*

- Ensure the full name and address is clearly visible within the window (if used) and no other information is viewable.

- If using non-windowed ensure the full address is written and is accurate.

- Mark envelopes as 'Private and confidential'.

- If sending to a patient, do not mark the envelope as coming from the Trust or a hospital as this could be a breach of confidentiality.

  - A return address can be used but keep it generic, e.g. a return PO Box or Number, road and postcode only.

NB All envelopes used should be robust and securely sealed, and staff **must** check only the correct correspondence is placed in the envelope.

- To avoid uncertainty, always include a covering letter saying why you have sent the information and who you are.

CHECK THE ADDRESS IS CORRECT AND ONLY THE APPROPRIATE INFORMATION IS PUT IN THE ENVELOPE.

- Ensure the package is clearly addressed (as detailed above).

- Where appropriate send the information via recorded post. Routine appointment letters or mail to individual patients do not need to be sent by recorded or special delivery, except where the information is particularly sensitive (such as copies of medical records).

NB: This guidance is not 100% prescriptive due to varying type of information the Trust sends. Staff should treat each situation on a case by case basis and the security applied to the communication should be in keeping with the content of the information, using this guidance as the minimum requirements.

4.6 **Receiving Information via Post**

There are some key rules those who handle incoming post should bear in mind:

a) Incoming mail should be opened away from public areas and date stamped (include details of team opening).

b) Incoming post should be efficiently and quickly given to the recipient. If the recipient is unavailable a deputy must take responsibility for that post.

c) If post is marked private and confidential to a named recipient, only they should open (unless prior arrangements/ delegation have been made).

d) Any confidential post not immediately given to the recipient must be locked away until they can receive it. The holder of the information is responsible for it until it is handed over.

4.7 **Communication by Telephone**

If the use of a telephone is essential to convey personal information the following protocols must be adhered to.

4.5.2 **Incoming**

When speaking with individuals in person over the telephone it is important to confirm their identity before any confidential or sensitive information is disclosed.

Patients

Staff should ensure they gain the best level of assurance of the patient's identity by obtaining confirmation of (for example) certain personal details:

a) Date of birth

b) Address and Post Code

c) Appointment Dates

d) Treatment / Clinic Details

e) Hospital or NHS Number

Relatives and Friends

Information should generally only be disclosed to a next of kin, relatives or friends when the consent of the patient has been obtained.

It is important to note that next of kin do not have any automatic right to patient data. Parents or those with parental responsibility have a right to information about their children unless the child has sought treatment independently of their parents. Personal information relating to outpatients should only be disclosed to the patient. For inpatients, all calls are directed to the ward / department where the patient is located.

Where the patient is conscious and competent their consent should be sought before information is disclosed. If this is not possible then decisions on whether to disclosure should be made on a case by case basis taking into account what are the best interests of the patient involved and any legal authority in place. It is advised that decisions involving disclosures should always be documented.

Other Individuals

Where other individuals (e.g. NHS organisations, health and social care providers, the police) request information about a patient, the individual must verify their identity and provide evidence that they are authorised to receive the information (such as the patient's consent, legal authorisation etc.). Where possible a written request should be provided.

4.5.3 **Outgoing**

The patient's right to privacy means that when making outgoing calls we need to speak to the patient directly, unless it is justifiable to speak to someone else – e.g. the patient has provided their consent for us to do so, or it is in their vital interests.

Wherever possible, if you think you may need to contact a patient by phone, ask them in advance if they have any preferences:

a) Would they prefer to be called at work?

b) Would they prefer to be called at home?

c) Would they like information to be left with a family member if they know they cannot be contacted directly?

d) Are they happy for messages to be left on their answer phones?

Leaving Answer Phone Messages

- The use of answer phone messages with patients is not a preferred method of communication. There are privacy risks with leaving messages unless the patient has provided consent to do so. There is a balance to be struck between respecting the privacy of the patient, not unduly worrying them with an obscure message, and ensuring the recipient understands it is a genuine message.

- Staff should consider whether any particular issues exist that could affect whether it is appropriate to leave an answer phone message. Consider the following:

  - If you leave a message, the patient may not be the first to hear it.

  - Who else might hear the message?

  - Are you sure you have dialled the correct number?

  - Will the patient fully understand the content of the message?

  - How can you be certain the message has ever been received?

- You may inadvertently breach confidentiality because the patient's friends or relatives may not know the patient is receiving health care.

4.5.4 **Contacting patients by Email**

- Many patients contact clinicians by email asking a variety of questions from confirmation of appointments to more in depth requests for clinical information.

- If your service/ department use email as a means of contacting patients, then you have a duty to inform your patients that the Trust cannot guarantee the information contained within the email will not be confidential or secure and can potentially be intercepted.

Disclaimer- "Please be aware the Trust cannot guarantee the security of information whilst in transit, and by requesting this service you accept this risk."

The Trust will then add a generic disclaimer to all outgoing emails.

- When responding to patients, the patient will have contacted us using a non secure email e.g. Hotmail. Personal data must only be sent to these accounts if the patient has confirmed they want this information emailed to them and have been made aware of the risks (as above). This should be documented.

- If a patient's request is for more detailed clinical information the patient should be offered a face-to-face or telephone conversation to discuss their issues. The 'reply' option must not be used to email the patient as this would further increase the risks to personal confidential data and a new email should be composed.

4.8 **Transporting Personal Information (e.g. community workers)**

- Person identifiable information (staff and patient) should only be taken off site when absolutely necessary and a line manager has approved this as an authorised business need, or in accordance with local policy.

- Record what information you are taking off site and why, and if applicable, where and to whom you are taking it. If it is a health record ensure it is tracked on the Trust system.

- Information must be transported in a Trust approved secure/ tamper proof devices. The approved mechanisms are available to order:

  - https://my.supplychain.nhs.uk/Catalogue/search?LastCartId=&LastFavouriteId=&HideMaskedProducts=false&QueryType=All&Query=mailing+pouch

  - WYQ206- bags xA4

  - WYQ210- bag xA3

  - WYU732- tags

NB: If these mechanisms are not available for any reason and the information MUST be transported then the staff member must utilise a device that can be sealed / locked as an interim arrangement and immediately escalate or order the approved mechanisms.

- Never leave person identifiable information unattended, e.g. in the boot of a car.

- Remember you are bound by the same rules of confidentiality whilst away from your place of work as you are when you are at your desk.

- While at home the person has personal responsibility to ensure the records are kept secure and confidential. This means locked away or out of sight from other members of your family including your friends and colleagues

- Ensure the information is returned back to site as soon as possible.

- **The person handling/ moving the information has responsibility for their safety and ensuring they are kept** secure **at all times.**

4.9 **Face to Face**

- Face-to-face communication is often the most appropriate, however there are safeguards to follow. These largely relate to environmental considerations:

- Only have conversations in appropriate places, e.g. who could overhear your conversation; e.g. are there patients or visitors about or staff from other departments?

- Discussions of a confidential nature should be dealt with in a 'private' area (e.g. ward office), where the conversation cannot be overheard whenever possible. If this is not possible staff should minimise the risk of conversations being overheard as much as possible by using initials and lowered voices.

5. References

Data Protection Act 2018/ General Data Protection Regulations

Department of Health Caldicott Manual

Records Management: NHS Code of Practice

NHS Code of Practice: Confidentiality

Department of Health: Information: To Share or not to Share Government

Response to the Caldicott Review, September 2013 Available at:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251750/9731-2901141-TSO-Caldicott-Government_Response_ACCESSIBLE.PDF

6. Associated Policy and Procedural Documentation

Information Governance Policy

Data Protection and Confidentiality Policy

Acceptable Use of ICT Policy

APPENDIX 1- Process when receiving a Phone Call