# Transportation of Health Records Within and Outwith Organisation Boundaries Policy

Document Control

| Date | Version | Contents/Changes | Author |
|---|---|---|---|
| April 9th 2009 | 0.1 | Initial draft. | Kathleen Carolan, Assistant Director of Clinical Services |
| April 23rd 2009 | 0.2 | Revisions to the detail for electronic data encryption and postal delivery | Information Support Group |
| May 7th 2009 | 1.0 | Final | Information Support Group |
| 31/03/2020 | 1.1 | Updates to bring in line with current legislation and Board structure | Information Governance Team |

**Contents**

## 1. Opening Statement

The Health Records of patients contain personal and sensitive information and are highly confidential documents. Care must be taken when transporting them within or outwith the hospital, health centre or care setting.

### 1.1. Purpose of the Policy

NHS Shetland Health Board (the Board) has put in place an Information Governance Policy which sets out the minimum policy standards for confidentiality, integrity and available of information.

It covers the overlapping areas of data protection compliance, information security, data quality and confidentiality.

The purpose of this **Transportation of Health Records Within and Outwith Organisation Boundaries Policy** is to build on the guidance contained within that IG policy and provide guidance for the security and transportation of confidential information with specific reference to manual and electronic health records.

All clinical and non-clinical areas should observe and implement the Data Protection Act 2018 principles when handling information about identifiable individuals.

For the purposes of this policy, confidential information will include personally identifiable information. However the same procedures can apply to 'sensitive' information and other information that could be classified as 'confidential' which is also held by the Board such as information held in work diaries.

The following guidance is based on the Scottish Government Records Management: NHS Code Of Practice (Scotland) Version 2.1 January 2012.

### 1.2. Information Governance and Data Protection – General Principles

Patient's health information and their interests must be protected through a number of measures:

- Procedures to ensure that all staff, contractors and volunteers are at all times fully aware of their responsibilities regarding confidentiality
- Recording patient information accurately and consistently
- Keeping information private
- Keeping information physically secure
- Disclosing and using information with appropriate care

In practice, individuals employed by the Board are responsible for any health records they create or use. This responsibility is established at, and defined by, law.

All staff employed by the Board (or who are contracted by the Board) are obliged to observe a personal common law duty of confidence and work within the framework and principles set out in the Data Protection Act 2018 (the Act). The Act places statutory restrictions on the use of personal information, including health information.

All members of the healthcare team have a responsibility to:

- Maintain high standards of record keeping
- Ensure that records are stored safely and securely (including use of an appropriate filing convention)

### 1.3. Information Security

The following occurrences concerning a health record, x-ray or personal patient information should be subject to the completion of an incident form[1] and an investigation carried out:

- Where correspondence or the health record has been wrongly addressed/delivered
- Where correspondence or the health record has not been securely delivered
- Where correspondence or the health record has been lost in transit
- Where correspondence or the health record has been found in an inappropriate location

## 2. Transportation of Health Records within the Hospital

The following procedure, shown as a checklist, applies to all staff involved in the transportation of health records or who have access to health records within the hospital.

**All staff must observe the rules shown below to ensure the security of health records:**

- Shut/lock doors and cabinets as required
- Store records appropriately so that they are not viewable by unauthorised persons.
- Wear ID badges
- Challenge the status of strangers
- Inform their manager or senior manager (as appropriate) if they witness anything suspicious or worrying (e.g. records not properly stored)
- Not inform unauthorised personnel how security systems/procedures within their department operate.
- Not breach confidentiality and security themselves
- Be aware of the procedure by which incidents relating to breaches of patient confidentiality and information security are reported
- Be aware of the procedure by which patients can request access to their health record.

**Manual records must be:**

- Formally booked out of their filing system
- Tracked appropriately using the relevant system (e.g.TrakCare)
- Returned to its filing location as soon as possible after use

[1] The Learning from Adverse Events through Reporting and Review Policy can be found at the following link: https://www.shb.scot.nhs.uk/board/policies/AdverseEventPolicy-Nov2019.pdf

- Stored securely within the clinic, ward or office environment, arranged so that the record can be found easily if urgently needed.
- Stored closed when not in use so that contents are not seen accidentally
- Inaccessible by members of the public and not left even for short periods where they might be overlooked by unauthorised persons.
- Held in secure storage with clear labelling.
- Transferred between clinical areas either in a sealed records transfer pouch (the zipped green pouches) or in a medical records trolley.

**With electronic records staff should:**

- Always log out of any computer system or application when work on it is finished.
- Not leave a PC unattended and logged in
- Not share passwords with other staff. If other staff need to have access, the appropriate access should be organised for them via the systems administrator[2]
- Not reveal passwords to others
- Change passwords at regular intervals to prevent anyone else using them
- Avoid obvious passwords like names, addresses.
- Always clear the screen of previous patient information before seeing another.
- Use a password protected screen saver and move monitors to prevent casual viewing of patient information by others.

The Information Security Policy sets out the security arrangements for electronic records in detail. The policy set can be found at the following link:
https://www.shb.scot.nhs.uk/board/policies/InformationSecurityPolicy-May2019.pdf

### 2.1. Transportation of Health Records, Out of Hours

Between 9am and 5pm on weekdays, Medical Records personnel are available to assist with the tracking and transportation of health records between hospital departments if required. If a set of case notes is needed out of hours, then the case notes will be retrieved by the night Porter. Reception and Nursing staff (who are trained to use the tracking system) are also authorised to track and transport case notes out of hours – the procedural rules apply to both core working hours and 'out of hours'.

[2] For most situations this will be the IT Department for PCs and Information Services for clinical systems (e.g. TrakCare)

## 3. Transportation of Health Records between Sites and Locations within the Health Board Area

Where patient identifiable information or patient records are taken off site, the following guidance must be observed.

Staff should not leave portable computers, medical notes or mobile data devices (e.g. Dictaphones, PDAs, digital cameras) that are used to store patient records/patient identifiable information in unattended cars or in easily accessible areas. Ideally, all files and portable equipment should be stored under lock and key when not in use.

Staff should not normally take health records home (either in hard copy or electronically) and where this cannot be avoided, procedures should be in place to safeguard that information effectively.

This includes the following actions:

1. Undertaking a risk assessment regarding the storage and safety of the records

Putting in place systems to ensure the records can be accessed in an emergency if needed

2. Ensuring that the records are tracked out and traceable
3. Ensuring that permission has been given by the Caldicott Guardian for health records to be stored away from a recognised base for health records storage (e.g. a records library or health centre records store).

Any records taken offsite must be properly secured preferably within a container in the boot of the car; they should never be on open view on a seat.

Staff should not use their own equipment to store any patient identifiable data. In exceptional circumstances staff may use their own equipment to store patient identifiable data, but only with the express written permission of the Caldicott Guardian who will be satisfied of the need to do so and that appropriate safeguards are in place.

Any such permission should be specific in terms of what information may be stored, for how long and how it will be protected. Failure to comply with these conditions may result in disciplinary proceedings.

All portable devices must be registered with the IT Security Officer, via the IT Department. Portable computing devices (e.g. data sticks) will be issued with encryption software for use by staff with the requirement to transfer data.

The Board policy for the use of portable devices can be found at the following link: https://www.shb.scot.nhs.uk/board/policies/MobileProtectionPolicy.pdf

### 3.1. Physical Controls

Health records should be transported in either sealed boxes or sealed pouches when being transported between hospital sites and locations within the Health Board area.

Health records should be hand delivered for internal transfer and not put into the internal mail. All records should be tracked from the current location to the new location on the patient administration system to ensure traceability at all times.

## 4. Transportation of Original or Copy Health Records to Hospitals or Authorised Agencies outwith the Internal Mail Delivery Service

The Board policy is not to send original health records outside the Board except in strictly defined circumstances. The exceptional circumstances include case notes accompanying patients who are transferred to another hospital out of hours or records requested by the Court.

Wherever possible, copies of paper notes or copies of data held in electronic format should be transferred using NHS Scotland's Secure File Transfer (SFT) service. Information on how to access and use SFT can is available on the NHS Shetland Intranet:

https://intranet.nhsshetland.scot.nhs.uk/corporate/ig/SWANSecureFileTransferSFT.html

Where original or copy case notes are sent via external mail, high grade envelopes or two envelopes must be used to provide adequate protection for the contents, and they must be sent via special delivery or registered mail.

If health records held in electronic format are being sent by post, then the data must be encrypted (e.g. sending data such as diagnostic tests or images etc on a CD via special delivery or courier). Heads of department responsible for sending electronic data in hard copy format, should contact IT to discuss how to put in place processes for encryption and decryption.

If a Courier service is being used, then it is essential to confirm that the Courier service has tracking systems in place, including recorded delivery and traceability of packages.

In these circumstances, and for other personal information sent by external mail, the addressing must be accurate, and the senders name and address must be given on the reverse of the envelope.

## 5. Lifting and Handling of Health Records

Health records should be handled safely and in accordance with the Board's manual handling policy.[3]

In terms of general principles, to avoid injury health records should be transported by trolley between locations. Health records should be kept to a maximum thickness of 2 inches and additional volumes created for oversized files. All volumes should be tracked and traceable as per the guidelines set out in this policy.

## 6. Staff Transportation of Health Records

Health records should be transported in sealed envelopes or pouches (whether this is personal delivery by staff or porter). If health records are being transported in larger numbers, then they should be sealed in boxes or safely moved around using the medical records trolleys.

Health records which are being moved by Board vehicle (e.g. car or van) must be stored in a sealed container (either an envelope, pouch or box). Health records should never be left unattended in a vehicle or visible to the public. Also see the previous sections for information about physical security of health records

[3] https://www.shb.scot.nhs.uk/board/policies/ManualHandlingPolicy.pdf

## 7. Roles and Responsibilities

All staff are responsible for ensuring the safety and security of health records, which are tracked out to them. Maintenance of data protection principles and confidentiality are requirements set out at a contractual level for all staff employed by the Board (including independent contractors).

In terms of general principles, service managers also need to be aware that they have specific responsibilities for the security of health records held in their areas. When health records are tracked out from the main file store, the service manager is responsible for ensuring the traceability of the health records held in their clinical area or department.

The responsibility for the security of health records held in the main records library and satellite libraries sits with the Health Records Manager. All staff accessing records library areas are responsible for ensuring that areas remain secure following legitimate access (e.g. locking doors once health records have been retrieved from archive stores or main library areas etc).

## 8. Access to Medical Records Procedure

Requests from patients to access their health record can be made to any part of the organisation. If a request is received, it should be sent in the first instance to the Information Governance Team.