THE STATE HOSPITALS BOARD FOR SCOTLAND

INFORMATION GOVERNANCE

CONFIDENTIALITY IN COMMUNICATIONS POLICY

Policy Reference Number	IG14
Issue Number	4.0
Lead Author	Information Governance and Data Security Officer
Contributing Authors	Members of the Information Governance Group Record Services Manager
Advisory Group	Information Governance Group
Approved By	Policy Approval Group (PAG)
Implementation Date	26 February 2025
Next Review Date	26 February 2028
Accountable Executive Director	Director of Finance and eHealth

The date for review detailed on the front of all State Hospital policies/procedures/guidance does not mean that the document becomes invalid from this date. The review date is advisory and the organisation reserves the right to review a policy/procedure/guidance at any time due to organisational or legal changes.

Staff are advised to always check that they are using the correct version of any policy, procedure or guidance rather than referring to locally held copies.

The most up to date version of all State Hospital policies, procedures and guidance can be found on the Hospital's Intranet policies page.

REVIEW SUMMARY SHEET

Changes required to policy (evidence base checked) **Yes ☒** **No ☐**

Summary of changes within policy: Review 2024

- **Section 2** - updated to make it explicit that all personal data used by the State Hospital is in scope.
- **Section 3** - updated to advise that local procedures need to be put in place.
- **Section 10** - Physical Mail section added and later sections renumbered.
- **Section 10** - added the explicit advice not to send letters with staff home addresses anywhere except the mailroom for delivery.

CONTENTS

1 INTRODUCTION / PURPOSE

Information governance legislation imposes obligations on the use of all personal data held by The State Hospital (TSH), whether it relates to patients and their families, employees, complainants, contractors or any other individual who comes into contact with the organisation.

TSH and its employees are bound by a legal duty of confidentiality to all data subjects which can only be set aside to meet an overriding public interest, legal obligation, or similar duty.

This policy sets out how TSH can meet some of its legal obligations and requirements under confidentiality, data protection and information security standards.

2 SCOPE

This policy applies to all staff, contractors and volunteers at TSH and applies to all personal data used by the organisation.

3 GENERAL WORKING PRACTICES

TSH needs to process confidential information for a wide range of activities on a daily basis, without which it would not be possible to effectively manage staff employment or deliver patient care. Our duties to keep information confidentiality applies to staff, visitors and carers, just as much as it applies to patients.

4 EMERGENCIES

The duty to share information, particularly where doing so protects the vital interests of an individual, can be as important as the duty of confidence.

Staff following Information Governance procedures (and where appropriate, The Caldicott Principles) should have confidence in sharing information during an emergency.

5 TELEPHONES

Patient identifiable information should only be divulged by telephone where:

- The identity of the requestor has been clarified, and
- There is a genuine reason for requiring the information.

Personal identifiable information should only be divulged by telephone where:

- The identity of the requestor has been clarified, and
- There is a genuine reason for requiring the information.

When an unknown caller is requesting information, staff should independently obtain a land line main switchboard number to confirm the identity of the individual/organisation requesting the information by calling the person back on the land line. Mobile numbers are not acceptable for purposes of clarification of identity.

Where an individual only has a mobile number another method of clarification of identity should be used, such as email.

5.1 Answering Machines / Voice Mail

Care should be taken when leaving messages on answer machines or voice mail so that personal information is not inadvertently divulged and distress is not caused to recipients.

Messages should only be left where the identity of the owner of the voice mail or answer machine is known.

A message should give the name of the staff member calling, the name of the organisation they are calling on behalf of and a contact telephone number. If leaving these details could cause distress, **do not leave a message**.

6 FAX MACHINES

The use of fax machines in NHS Scotland for sending and receiving personal identifiable information has been withdrawn.

Where there is no alternative to using a fax machine, strict protocols and procedures should be put in place. These controls must be approved by the Senior Information Risk Owner prior to transmissions commencing.

If patient information is to be transmitted both the Senior Information Risk Owner and the Caldicott Guardian must approve the controls prior to transmissions commencing.

7 EMAILS

TSH uses NHS Scotland email as its email service.

NHS Scotland email is the only authorised method of sending patient confidential information to other NHS Scotland email accounts.

Further information about Information Security & Governance is available at:
NHSS - 365 Champions SharePoint site.

7.1 Email Disclaimer

It is good practice to include a disclaimer at the end of the emails which give brief description of actions to be taken if a recipient receives the email in error.

When sending emails between @nhs.scot, NHS Scotland mail does not automatically attach a disclaimer.

An example disclaimer:

"This message may contain confidential information. If you are not the intended recipient, please inform the sender that you have received the message in error before deleting it.
Please do not disclose, copy or distribute information in this e-mail or take any action in relation to its contents. To do so is strictly prohibited and may be unlawful. Thank you for your co-operation.

NHS Scotland email is the secure email available for all NHS staff in Scotland. NHS Scotland email is approved for exchanging patient data and other sensitive information with NHS Scotland email and other accredited email services."

8 DIRECT DISCLOSURE

Patient identifiable information should only be divulged directly where:

- The identity of the requestor has been clarified, and
- There is a genuine reason for requiring the information.

Personal identifiable information should only be divulged directly where:

- The identity of the requestor has been clarified, and
- There is a genuine reason for requiring the information.

At times direct requests for confidential information can be challenging because of the circumstances in which they occur. Appendix 1 shows a flowchart of decisions for verbal requests for confidential information.

9 HOSPITAL RADIOS

Under normal circumstances confidential information, such as patient names, should not be transmitted via the hospital's radio system.

In exceptional circumstances (e.g. the telephone system failing) it may be necessary to transmit confidential information to protect the vital interests of staff, visitors, volunteers and patients. When doing so only use the minimum amount of information required. Where possible, other more secure methods of communication should be used.

10 PHYSICAL MAIL

10.1 Collection of Mail

Physical mail can be used to make time sensitive requests or serve legal papers to the organisation. These must be opened and actioned promptly.

All department must put in place processes to ensure that mail is collected and reviewed within 2 working days.

10.2 Sending Mail

All communications should be clearly marked with the recipient's full address and a return address in case the communication is undeliverable.

To protect staff privacy it is not permitted to send letters that show the home addresses of staff on the envelope to internal locations within TSH.

Letters addressed to a staff member's home address MUST be sent to the mailroom for external delivery.

10.2.1 Sensitive and Confidential Information

Some communications contain 'Confidential' or 'Sensitive' information. This is any information that if disclosed inappropriately could result in:

- Court action for breach of confidentiality.
- Harm to an individual.

- Distress to an individual.

These communications should have a higher level of security than standard communications.

PO boxes are used to hide the senders address, but still permit Royal Mail returning a communication that can't be delivered without needing to open the envelope/container.

A PO box that is used as the return address for patient information **must not** be used as the return address for staff communications.

Confidential packaging is used to protect the contents of a communication from accidental disclosure using two containers. The confidential communication is placed in an inner container and sealed. The inner container is fully addressed, including a return address.
The inner container is then placed in an outer container. The outer container is also fully addressed, including a return address.

This means that even if the outer container is damaged the confidential information is still protected from casual observance.

Common containers are envelopes, bags or boxes that can be sealed.

Encryption can be used as a method to ensure that digital data cannot be read without a password. This can be used as a replacement for confidential packaging's inner container when sending physical media containing confidential information. The password required for decryption must be sent separately from the encrypted information.

Condition	Security Solutions	Example
Identifying TSH as the sender on the envelope is not appropriate.	Use a PO box as the return address.	A letter from HR to a member of staff. A letter to a Named Person. A letter to an ex-patient.
Communication contains sensitive / confidential information (health data, etc.).	Use Confidential packaging.	A communication containing patient paper notes. A letter about a staff members health conditions.

Mail Delivery Services

Condition	Solutions	Example
The confidential / sensitive information can be read if the outer and inner containers are removed.	Send using Royal Mail Special Delivery.	A set of patient paper notes requires to be set to a solicitor.
The confidential / sensitive information cannot be read if the outer and inner containers are removed.	Send using Royal Mail Signed for (1st or 2nd class).	An encrypted CD with patient notes requires to be sent to a solicitor.

Example: When sending a letter to a member of staff's home address about their health condition. The letter should:

- Placed in confidential packaging.
- Be sent using Royal Mail Special Delivery.
- Have a staff PO box return address.

Example: When sending a letter to a patient's relative about a visit. The letter should;
Have a patient PO box return address

Example: When sending a DVD with patient notes to a solicitor. The letter should:

- Have the DVD encrypted.
- Placed in confidential packaging (encryption is the inner container).
- Be sent using Royal Mail Signed for first or second class.
- Have a patient PO box return address.

11 ADVICE AND GUIDANCE

Members of the Hospital's Information Governance Team are available to provide specific advice on good practice on request.

Please contact the team via email at TSH.DataProtection@nhs.scot or by phone on Extension 2113.

12 EQUALITY AND DIVERSITY

The State Hospitals Board (the Board) is committed to valuing and supporting equality and diversity, ensuring patients, carers, volunteers and staff are treated with dignity and respect. Policy development incorporates consideration of the needs of all Protected Characteristic groups in relation to inclusivity, accessibility, equity of impact and attention to practice which may unintentionally cause prejudice and / or discrimination.

The Board recognises the need to ensure all stakeholders are supported to understand information about how services are delivered. Based on what is proportionate and reasonable, we can provide information/documents in alternative formats and are happy to discuss individual needs in this respect. If information is required in an alternative format, please contact the Person-Centred Improvement Lead on 01555 842072.

Line Managers are responsible for ensuring that staff can undertake their role, adhering to policies and procedures. Specialist advice is available to managers to ensure that reasonable adjustments are in place to enable staff to understand and comply with policies and procedures. The EQIA considers the Protected Characteristic groups and highlights any potential inequalities in relation to the content of this policy.

Carers / Named Persons are encouraged to highlight any barriers to communication, physical disability or anything else which would prevent them from being meaningfully involved in the patient's care (where the patient has consented) and / or other aspects of the work of the Hospital relevant to their role. The EQIA considers the Protected Characteristic groups and highlights any potential inequalities in relation to the content of this policy".

The volunteer recruitment and induction process supports volunteers to highlight any barriers to communication, physical disability or anything else which would prevent them from contributing meaningfully to patient care and / or engage in other aspects of the work of the Hospital relevant to their role. The EQIA considers the Protected Characteristic groups and highlights any potential inequalities in relation to the content of this policy.

13 STAKEHOLDER ENGAGEMENT

Key Stakeholders	Consulted (Y/N)
Patients	N
Staff	Y
Carers	N
Volunteers	Y

14 COMMUNICATION, IMPLEMENTATION, MONITORING AND REVIEW OF POLICY

This policy will be communicated to all stakeholders within the State Hospital via email, the hospital's intranet and through the staff bulletin. The Person Centred Improvement Team will facilitate communication with Volunteers.

The Information Governance Group will be responsible for the implementation and monitoring of this policy.

Any deviation from policy should be notified directly to the policy Lead Author. The Lead Author will be responsible for notifying the Advisory Group of the occurrence.

This policy will be reviewed every three years, and when appropriate to take into account changes to legislation that may occur, and/or guidance from the Government and/or the Information Commissioner's Office.

APPENDIX 1: VERBAL REQUEST FOR CONFIDENTIAL INFORMATION

Verbal Request for Confidential Information