



# STANTON TERRITORIAL HEALTH AUTHORITY

## POLICY/PROCEDURE

<b>CATEGORY:</b>	Confidentiality	<b>PAGE NUMBER:</b>	1 of 5
<b>SUBJECT:</b>	Security and Storage of Patient Personal Information	<b>DISTRIBUTION:</b>	Hospital Wide
<b>CURRENT EFFECTIVE DATE:</b>	May 2014	<b>NEXT REVIEW DATE:</b>	May 2017

The overall purpose of this policy at Stanton Territorial Health Authority (STHA) is:

- To ensure personal information, regardless of media (electronic form, paper file, or radiological/digital image) is properly stored in a secure environment.
- To ensure that security measures are in place and followed in order to protect the confidentiality and integrity of personal information within the STHA.
- To ensure the security and integrity of personal information during transmittal by any means including internal and external delivery networks, voice mail, wireless technology, e-mail and the Internet.

### SPECIAL POINTS

STHA is a Public Body under the *Access to Information Protection of Privacy Act* (the 'Act').

It is expected that all STHA staff and physicians shall report any breach of patient confidential information in the Risk Monitor Pro incident reporting system.

Any security breach in which an unauthorized individual has access to personal information must be reported. Incidents may range from unauthorized individuals being able to view a computer screen or paper file, to theft or loss of STHA computer equipment including electronic storage media, to unauthorized destruction of information through a water-main leak, fire etc.

See other related policies: "Release of Patient Information", "Release of Employee Personal Information", "Facsimile of Patient Information"

### DEFINITIONS

**Breach of Security:** occurs whenever personal information is collected, used, disclosed or accessed other than as authorized, or its integrity is compromised.

**STANTON TERRITORIAL HEALTH AUTHORITY  
POLICY DOCUMENT**

Confidentiality: Security and Storage of  
Patient Personal Information

H-0560

---

**Integrity of Personal Information:** means the preservation of its content throughout storage, use, transfer and retrieval so that there is confidence that the information has not been tampered with or modified other than as authorized.

**Personal Information:** "Personal Information" under the Act means information about an identifiable individual, including:

- a. the individual's name, home or business address or home or business telephone number
- b. the individual's race, colour, national or ethnic origin or religious or political beliefs or associations
- c. the individual's age, sex, sexual orientation, marital status or family status
- d. an identifying number, symbol or other particular assigned to the individual
- e. the individual's fingerprints, blood type or inheritable characteristics
- f. information about the individual's health and health care history, including information about a physical or mental disability
- g. information about the individual's educational, financial, criminal or employment history
- h. anyone else's opinions about the individual
- i. the individual's personal opinions, except where they are about someone else

**Secured Place:** means a physical environment for the temporary or permanent storage of, or for the use, processing or transmittal of, personal information that has the following characteristics:

- not readily accessible by unauthorized users;
- supervised or monitored by authorized users;
- keyed to allow entrance to authorized users only;
- locked when authorized users are not in attendance;
- protected by controls to minimize loss, destruction or deterioration caused by fire, water, or humidity damage; and
- proper containers and adequate labeling are used to reduce accidental loss or destruction.

**Security:** means the consistent application of standards and controls to protect the integrity and privacy of personal information during all aspects of its use, processing, disclosure,

**STANTON TERRITORIAL HEALTH AUTHORITY  
POLICY DOCUMENT**

Confidentiality: Security and Storage of  
Patient Personal Information

H-0560

---

transmittal, transport, storage, retention, including conversion to a different medium, and destruction.

**POLICY**

STHA staff and physicians shall ensure that recorded personal information will be properly secured and maintained in the appropriate manner to protect its confidentiality and integrity. Recorded personal information includes information that is written, photographed, recorded or stored in any manner, on any medium or by any means, including by graphic, electronic, audio, radiological, digital or mechanical means.

Personal information is to be collected, used, disclosed or accessed only by individuals who are authorized for that purpose. Individuals thus authorized must have a clear understanding of the authority, parameters, purposes and responsibilities of their access, and of the consequences of failing to fulfill their responsibilities.

Security safeguards shall include both physical and human resource safeguards to prevent unauthorized personal information collection, use, disclosure and access.

Physical security measures include such safeguards as locked filing cabinets, restricted access to certain offices or areas, the use of passwords, encryption and lock-boxes. Human resource security measures include security clearances, sanctions, training and contracts.

**PROCEDURE:**

**STHA Staff and Physicians:**

1. All written personal information shall be placed in an appropriately secured file. Paper files (both patient and employee) containing such information shall be kept in a secure place at all times within the resources available other than when being updated or used by authorized personnel as a necessary function of their work.
2. Personal information stored in electronic form on a fixed computer server or terminal shall be properly secured from unauthorized access. Personal information stored on electronic media (diskettes, magnetic tape, CD ROM'S, disk drives, laser disks, etc.) shall be kept in a Secured Place at all times and shall be used only by authorized personnel having access to a protected system. Prior to removal from an office, any personal information contained within the computer hardware or on electronic storage media shall be secured or removed.

**STANTON TERRITORIAL HEALTH AUTHORITY  
POLICY DOCUMENT**

Confidentiality: Security and Storage of  
Patient Personal Information

H 0560

- 
3. Individuals who sign on to a computer must not leave the computer on in accessible areas when they leave their workstation. User password protocols must be in place and utilized. Where possible, automatic shut offs after a prescribed period of disuse should be programmed for all workstations.
  4. All personal information that is mailed through regular postal service, interdepartmental mail or sent via courier must be marked confidential and have reasonable safeguards put in place to ensure security and integrity of the information.
  5. Personal information shall not be transmitted via electronic mail without appropriate safeguards such as encryption or transmittal within a secure firewall where practicable.
  6. Persons leaving voice messages containing personal information should be discreet. Personal information should never be left on a patient's voicemail unless the individual whom the information is about has authorized it. Any personal information relayed by voice message should be kept to the minimum required for the purpose of the communication. Persons receiving voice messages containing personal information should listen to the message in private, and delete the message as soon as possible. Appropriate passwords and security measures should be in place for access to voice mail.
  7. Fax machines shall be located in a Secured Place where they can be used and monitored only by authorized persons. A cover sheet, with approved STHA logo, should be attached to all documents stating that the transmittal is confidential and that any unintended receiving party is prohibited from reading or disclosing the information to anyone else (i.e. a Confidentiality Clause). Users of fax machines shall follow the *STHA Policy: Facsimile Transmission Patient Information*.
  8. If personal information is removed from the STHA's premises by an authorized person for purposes authorized by STHA that person(s) shall carry the file/electronic media with them or ensure secure storage at all times. Personal information shall not be left in vehicles. The removal of any health record shall be recorded in the red out guide.
  9. Personal information files/electronic media shall be returned to its designated and secured storage location and not allowed to accumulate or be left unattended on desktops, nursing stations, patient bedside, treatment rooms or any other location in a non-secured place.
  10. Everyone dealing with personal information in any manner shall take reasonable precautions to protect personal information from fire, theft, vandalism, deterioration, accidental destruction or loss and any other hazards.
-

**STANTON TERRITORIAL HEALTH AUTHORITY  
POLICY DOCUMENT**

Confidentiality: Security and Storage of  
Patient Personal Information

H-0560

- 
11. No personal information shall be transported, stored or left in a location that could result in the destruction or deterioration of the personal information. For example, computer disks could be destroyed if left in a locked trunk on a hot day; paper records could be destroyed in a damp area.

**Manager/Supervisor:**

1. The manager/supervisor shall ensure that all employees be made aware of the policy respecting security and storage of personal health information.
2. Managers/supervisors shall review practices of employees to ensure these standards are being maintained and that there are no breaches of security.
3. When standards are not being maintained or when a security breach occurs, such situations shall be brought to the attention of the immediate supervisor then the Quality & Risk Management Coordinator in order that recorded and corrective steps are taken.
4. When the CEO is advised, in writing, of an electronic security breach from electronic systems (for example iEHR, XERO Viewer) from the Department of Health & Social, this will be forwarded to the appropriate Director and Manager, in consultation with the Quality & Risk Management Coordinator to investigate and provide a response to the CEO of the findings. The Quality & Risk Management Coordinator will track these incidents.


**Quality & Risk Management Coordinator:**

1. Conduct periodic surveys of building security with regard to potential for unauthorized access to personal health information, document findings and recommendations. Provide findings and recommendations to Manager and Director for follow up action and response.

**Manager or Designate Information Services:**

1. To ensure appropriate procedures and safeguards are in place to safeguard the confidentiality, security and integrity of personal information used, processed, stored or transmitted electronically.

Reviewed and approved by:

  
\_\_\_\_\_  
Chief Executive Officer (signed and dated)      MAY 1 2014

Reviewed and approved by:

  
\_\_\_\_\_  
Chairperson of CPAC (signed and dated)      MAY 1 2014