STANTON TERRITORIAL HEALTH AUTHORITY

POLICY/PROCEDURE

CATEGORY: Confidentiality	**PAGE NUMBER:** 1 of 4
SUBJECT: Reporting Confidentiality/ Privacy Breaches of Patient and/or Employee Information	**DISTRIBUTION:** Hospital Wide
CURRENT EFFECTIVE DATE: November 2012	**NEXT REVIEW DATE:** November 2015

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

- To ensure that all security breaches pertaining to the privacy, confidentiality and integrity of personal information are reported, assessed, investigated and recorded.
- To ensure that corrective procedures are in place to remedy any breach of the confidentiality, security and integrity of personal information.
- To ensure that the corrective procedures are followed.

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 alleged or actual breach of patient confidential information. This is done to secure the confidentiality and integrity of all personal information. 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.

Accessing one's own or one's family members' personal information is an abuse of position and process. When staff or their family members are being treated as patients, they shall request information in the same manner as any other patient. Accessing the personal information of one's family members is also a breach of privacy and confidentiality.

See other related policies: "H-0550 Health Records - Release of Patient Information", "C-0220 Confidentiality - Release of Personal Information about STHA Employees ", "H-0500 Health Records - Facsimile of Patient Information".

Alleged breaches of the Healthnet Viewer are reported by The Department of Health & Social Services to the Chief Executive Officer.

DEFINITIONS

Breach of Confidentiality/Privacy: Unauthorized access to patient information and/or unauthorized disclosure of patient information.

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

PROCEDURE

STHA Staff and Physicians:

1. An allegation of a breach of confidentiality or privacy of patient or personal information may be made to any staff member, volunteer, or physician of the STHA. Any individual receiving an allegation of a breach or having knowledge or a reasonable belief that a breach of personal information may have occurred shall immediately notify his/her supervisor or, where this is not possible, shall notify the STHA Quality & Risk Management Coordinator, or designate.
2. The initial notification can be verbal however it must be followed up in writing.

3. The person so notified shall in turn notify the Manager of the alleged violator of this Policy.
4. All written allegations of a breach must be sent to, and retained by, the Quality & Risk Management Coordinator.
5. The Manager, shall discuss the next steps with the Quality and Risk Management Coordinator (or designate) and the Department of Human Resources Client Services Manager. It may be decided that a complaint does not require investigation if, after consultation, the consulters are of the opinion that:
    - the length of time that has elapsed since the alleged incident makes an investigation no longer practicable or desirable;
    - the subject matter of the complaint is trivial or the complaint is not made in good faith or is frivolous.
6. If the decision is made to proceed with an investigation, it shall be the responsibility of the Manager, in consultation with the Quality & Risk Management Coordinator, or designate, and the Human Resources Client Services Manager, to investigate the allegation (including obtaining the alleged violator's version of events), consult with the appropriate resources, document findings and make a determination as to whether there has been a breach of confidentiality or privacy of personal information.
7. If it is determined that a breach has occurred, appropriate remedial action shall be taken. Such action may include disciplinary action up to and including termination of employment, contract, association or appointment with the STHA. The Manager shall consult with their Director and the Client Services Manager. The Client Services Manager shall, if required, consult with Labour Relations to establish the appropriate level of disciplinary action to be applied. Further education may be provided to the individual if appropriate.
8. The Quality & Risk Manager shall be sent all documented follow up and track confirmed breaches in Quarterly Reports that are provided to Senior Management and the Public Administrator.

Manager:

1. Upon receiving a report of a confidentiality/privacy breach, consults with the Quality & Risk Management Coordinator and Human Resources Client Services Manager to determine next steps.
2. Is responsible to advise their Director of the complaint, investigation and outcome.

Quality & Risk Management Coordinator:

1. Acts as a resource to managers and all STHA employees regarding appropriate action, following a breach of confidentiality/privacy (eg including the need to contact police, insurers, etc.).
2. Advises the Chief Executive Officer of the allegation and provides known details.
3. Receives the original complaint/allegation and reviews it on an incident by incident basis, making recommendations for measures to prevent future breaches.
4. Notifies affected individual(s) with a formal letter except when notice is not appropriate or possible (e.g., identities of the individuals affected by the breach are unknown, contact information is unavailable, or if notice would interfere with a law enforcement investigation). The letter should include:
    - The information about them that was breached; and
    - The contact information including name, address and phone number of the Quality & Risk Management Coordinator.
5. Collects, assesses and documents information on security breaches for Quarterly Reports.
6. Identifies what needs to be done to prevent future breaches. Develops a strategy for ensuring the breach does not reoccur.
7. Implements measures as appropriate to prevent future privacy breaches, such as:
    - Staff training;
    - Access controls;
    - Secure destruction procedures.

Reviewed and approved by: H. Pender 5 Nov. 2012
Chairperson of CPAC (signed and dated)

Reviewed and approved by: [signature] NWT 5/12
Chief Executive Officer (signed and dated)