Thunder Bay Regional Health Sciences Centre

St. Joseph's Care Group

Policies, Procedures, Standard Operating Practices

No. IS-SEC-005-A

Title: Confidentiality – Use of Electronic Systems	☒ **Policy** ☒ **Procedure** ☐ **SOP**
Category: Security **Department:** Informatics **Program:** Information Systems **Division:** Applications	**Distribution:** Thunder Bay Regional Health Sciences Centre, St. Joseph's Care Group and Regional Partners
Approved: Senior Director, Informatics **Signature:**	**Approval Date:** March 17, 2021 **Reviewed/Revised Date:** March 17, 2021 **Next Review Date:** March 17, 2024

CROSS REFERENCES: *HR-tec-03 Confidentiality and Release of Information (TBRHSC)*
AD 6-105 Privacy of Personal Health Information (SJCG)
IS-SEC-009-A – Password – Standards

1. PURPOSE

The purpose of this policy is to ensure that everyone working within Thunder Bay Regional Health Sciences (TBRHSC), St. Joseph's Care Group (SJCG) or one of the Regional Partner sites is aware of their responsibilities regarding the protection of confidential information when utilizing any systems maintained and supported by the Informatics Department.

2. POLICY STATEMENT

Confidentiality is a critical component of professional conduct for all staff. All professional staff, employees, students, partners, volunteers, fellows, observers and any other person working at/or on behalf of TBRHSC, SJCG or Regional Partner sites have an obligation to keep information designated as confidential including but not limited to, information regarding patients that may come to their attention either inadvertently or in the normal performance of their duties. Confidential information must not be divulged, either inside or outside of the corporation(s) unless the person is required to do so in the performance of their duties or as expressly authorized by law or by the corporation(s). All persons will be required to sign a "Protection of Confidential Information & Accountability" form (attached) before access to any system is granted.

Confidentiality responsibilities and obligations extend outside normal working hours, premises and networks, and continue after employment or affiliation with a site has ended.

There is a zero tolerance policy regarding any violation of the security and confidentiality of any information concerning patients/clients, corporate personnel and confidential corporate business. This policy is designed to protect professional staff, employees, students, partners, volunteers, fellows, observers, and patients/clients by clarifying what is and what is not acceptable practice when viewing, disclosing or otherwise utilizing the corporation(s) or patient/client information. Access to corporate, patient and client information is audited regularly.

All persons working within the Corporation, Partners, Fellows, Observers, and any other person working at/or on behalf of the member sites:

- May not search for, access or divulge any corporate, patient/client information that is not required in the performance of their duties.
- May not search for or access patient/client information for personal or family use.

This material has been prepared solely for use at Thunder Bay Regional Health Sciences Centre (TBRHSC) and St. Joseph's Care Group (SJCG). TBRHSC/SJCG accepts no responsibility for use of this material by any person or organization not associated with TBRHSC/SJCG. No part of this document may be reproduced in any form for publication without permission of TBRHSC/SJCG. A printed copy of this document may not reflect the current electronic version on the TBRHSC/SJCG iNtranet.

- May not search for or access one's own medical record. Information pertaining to one's own medical record must be obtained through a physician or by following policies in Health Records pertaining to accessing a personal record.
- Must not leave their computer session unattended without first suspending or logging off.
- Must ensure that their **passwords** remain protected in order to ensure no unauthorized or unmonitored use of their account as per hospital policies.

Authorization to Access Information *(*Reminder: Access does not equal authorization*)*
Persons working at or on behalf of the sites may have authorization to access certain information. This access is limited and strictly confined to information required for the performance of their current hospital duties in accordance with hospital policies and procedures.

Breach of Confidentiality
Breach of confidentiality includes any unauthorized access to or intentional or inadvertent disclosure of confidential information. Every effort should be made to ensure that confidential information is not inadvertently disclosed (for example: leaving computer screens unattended with confidential information displayed; improper storage, disposal, or deletion of confidential information; or failure to ensure that cases used for teaching purposes are anonymous).

Any employee who violates this policy will be subject to disciplinary action up to and including immediate suspension or termination of employment, or in the case of members of the medical staff, up to and including suspension or termination of privileges. Violation of this policy by students and partners may result in their access being revoked.

Computer Data Security
All Corporate computer systems and much of the data residing on them are vital corporate assets. Since individuals are responsible for protecting corporate data and patient information entrusted to them, it is their responsibility to keep confidential the automated systems access codes (passwords) that give access to this data and information. The Corporation retains the exclusive right to and use of all data and information stored on computers that are used to carry out corporate duties.

Access to corporate data and patient information must be properly authorized and will be granted based on the requirement for carrying out corporate responsibilities. To access automated systems, all users must use their personal access code and/or password.

Security responsibilities and obligations extend outside normal working hours, premises and networks, and continue after employment or affiliation with a site has ended.

Audits
Audits will be conducted to monitor compliance with the corporate policy.

3. SCOPE

This policy applies to all staff that have access to confidential patient and/or corporate information and to anyone who is authorized to work within the sites premises and/or may be required to have access to or make use of confidential information. Any person in possession of confidential information must be diligent in protecting against inappropriate access to the information and ensuring the copy of the record is not lost.

Individuals must read and adhere to any related privacy, security and confidentiality policies and any member site-specific privacy and security policies.

4. DEFINITIONS

Corporation	• Professional Staff are staff members who have a current appointment at Thunder Bay Regional

	Health Sciences Centre, St. Joseph's Care Group, or are credentialed at any of the regional northwestern hospitals. • Employees/Staff include, but is not limited to Nursing, Allied Health, Clerical, Managers, Supervisors, Clergy, Housekeeping, Laundry, Dietary Staff, and Volunteers. • Students refers to Medical Students, Nursing Students, Allied Health Students, and all other students who must, in the course of their study, utilize systems and work within the hospitals to meet the requirements of their particular program.
Regional Partners	Any organization that uses one or more of the Informatics shared systems in the North West Region, including the 12 member hospitals and any other affiliated organizations.
Fellows & Observers	Medical professionals who are provided access to the systems for the purpose of clinical trials, research, etc.

5. PROCEDURE

a) At the time of the staff onboarding process, this Policy and the Protection of Confidential Information & Accountability Form will be reviewed, signed and retained by the applicable area as follows:

- Employees: Signed forms are retained on file in Human Resources.
- Medical staff: Signed forms are retained on file in Medical Staff Office.
- Volunteers: Signed forms are retained on file in Volunteer Services.
- Nursing students: Signed with their program lead at Lakehead University or Confederation College. Signed forms are retained on file in Information Systems.
- Other students: Signed with their preceptor/manager. Signed forms are retained on file at the facility where the placement is being completed.
- TBRHSC only: Medical learners and Allied Health students review and sign with their academic placement coordinators. Signed forms are retained on file in Academic Affairs.
- SJCG only: All Allied Health students and any other individual conducting work on behalf of the organization reviews the policy with the manager of the respective areas. Signed forms are retained on file with the respective manager.

b) If users are working at more than one site, a completed "Protection of Confidential Information & Accountability" form must be completed for each site.

6. RELATED PRACTICES AND/OR LEGISLATIONS

None.

7. REFERENCES

a) HR-tec-03 Confidentiality and Release of Information (TBRHSC)
b) AD 6-105 Privacy of Personal Health Information (SJCG)
c) Any member site-specific privacy and security policies.
d) IS-SEC-009-A – Password – Standards

Protection of Confidential Information & Accountability

I, _____

(*Please print your first and your last name*)

agree and understand that my employment, privileges, or affiliation with

_____

(Please print name of the facility)

is based on the following terms:

1. I understand that I am responsible for the protection of the confidential nature of information concerning patients/clients, corporate personnel and other confidential types of corporate information. I will respect the confidential nature of all information.

2. I will exercise all reasonable care and caution in protecting printed, written, electronic and verbal confidential information from casual observation, unauthorized perusal or other abuse.

3. I undertake and agree at all times to treat as confidential all information acquired through my employment, and not to disclose same except as required in the performance of my normal duties or expressly authorized by law or the corporation(s). I will not discuss such information with any party nor will I participate in or permit the release, publication, or disclosure of such information.

4. I understand that I will limit my Internet access to official corporate business during hours of work. Whether accessing the Internet during paid hours or for personal use during unpaid hours, I will comply with all the terms of the policy. I will exercise all reasonable care and caution in the privacy and confidentiality of information that I transfer over the Internet. I will not access, download or transmit objectionable material that could damage the reputation of the member sites.

5. I understand that my responsibility for the protection of patient information extends to all external data repositories and third-party applications that I have been granted access to.

   Note: Access to eHealth Ontario provincial repositories and assets such as the ConnectingOntario ClinicalViewer requires a request for an elevated level of access and is granted and tracked on a per user basis by both the member site and eHealth Ontario. This access must be requested for each facility for which I am providing care and require access to patient data.

6. Access is the sole responsibility of each user and can be revoked at any time if not in compliance with the privacy and security requirements outlined in all the Regional Partner member sites privacy and security policies and procedures and privacy legislation.

I further understand that this agreement and undertaking includes:

a. Never discussing or disclosing patient, client or corporate information unless required for the performance of my normal duties.

b. Protecting the security of my computer/device by ensuring that my passwords are known only to myself, as disclosure could provide opportunity for unmonitored and unauthorized use. Should I feel that my password has been compromised, I will contact the Help Desk at (807) 684-6411 or toll free at 1-888-291-9636 and request to have my password reset.

c. I understand that I am responsible for all access under my password and that I am responsible to always log off or suspend my computer/device before leaving it unattended.

d. I understand that the confidentiality responsibilities and obligations extend outside normal working hours, premises and networks, and continue after my employment or affiliation with the Hospital has ended.

e. I have read and understand the relevant policies and procedures on privacy and security as referenced below.

Noncompliance with any of the above will result in disciplinary action, up to and including dismissal as provided for in hospital policies and/or loss of privileges from any of the Regional Partner member sites.

To complete this form, fill out the information below:

Please identify your role in the organization (check all that apply):

☐ Employee

☐ Medical Staff

☐ Resident

☐ Student – Please specify type: _____

☐ Physician Clinic/Agency (non-hospital employee)

☐ Clergy or Equivalent

☐ Volunteer

Position/Title	Witness Name (print)
Department	Witness Signature
Employer	Date
Signature	