Care. Connected.

Policy and Procedure

Section: Finance and Administration - Privacy	**Number:** 18.80.PP.v2
Subject: Requesting an Audit of the Scheduling Software	**Associated Document Form Number:** 18.80.F
Effective Date: May, 2008	**Last Reviewed Date:** July, 2014
Last Revised Date: March, 2015	**Next Review Date:** March, 2017

PURPOSE

OTN maintains data in its Scheduling Software that tracks all access and transfers of personal health information at a Member site. As a health information network provider, OTN has obligations under the Personal Health Information Protection Act (PHIPA) to make this information available to its Members.

SCOPE

This policy applies to all OTN Employees, Students, and Contractors.

POLICY

OTN will make available upon written request and where practical to do so, an electronic record of all accesses and transfers of personal health information (i.e. Audit log) generated within its scheduling software (Telemedicine Service Manager (TSM)) that is associated with a Health Care Organization that is a Member. The policy and procedure describes how a Member site may request an audit log from OTN.

Suggested authorized requestors from an Organization that is a Member include:
1. Chief Executive Officer
2. Risk Manager
3. Privacy Officer
4. Designed "Contact Person" As Defined In PHIPA

The purpose for which Organizations may require audits are as follows:
1. Review Users' access to the scheduling software;
2. To review a possible privacy incident; and
3. To support a patient request.

PROCEDURE

1. Complete a "Scheduling Software Audit Request From," ensuring the following information is completed on the form:
   - Name and Address of Organization;
   - Name of individual requesting audit log;
   - Contact information for individual requesting audit log;
   - The unique patient identifier or the name of the scheduling software User; and
   - The period for which accesses and/or transfer information is required.
   - E-mail to the Privacy Office at privacy@otn.ca.

2. Incomplete information will necessitate follow-up from the Privacy Office.
3. The Privacy Office will acknowledge receipt of the request and inform the requestor about the number of days it will take to meet the request and the secure method by which the report will be provided.
4. When the request is urgent, OTN will fulfill the request as soon as reasonably possible.
5. A Member of the Privacy Office will use registered mail to send the Requestor at the Organization, the audit log on an encrypted media format, clearly marked as "Confidential."
6. Organizations can contact OTN Technical Support Staff to deactivate or change access to the scheduling software based on audit report results if a User at that Site accessed personal health information he/she was not authorized to access.
7. The Privacy Office will notify every applicable HIC of a privacy breach (If the result of an OTN activity) at the first reasonable opportunity and will document as per the process outlined in OTN's "Privacy Breach Management" policy.
8. Patients who contact OTN to request an audit will be referred to the appropriate Organization in order for that Organization to support the patient's request.

VIOLATIONS

OTN individuals must notify the Manager, Privacy and Risk (or designate) and/or the Information Security Officer at the first reasonable opportunity, in accordance with Privacy Breach Management Policy and/or Information Security Incident Response, if he/she breaches or believes there may have been a breach of this policy or its procedures. The Manager, Privacy and Risk (or designate) and the Information Security Office must notify the each other of potential breaches and incidents that come to their attention.

Issues of non-compliance will be dealt with on an individual basis by the appropriate authority within OTN. Employees who willingly and deliberately violate this policy will be subject to disciplinary action up to and including termination of employment or contract and depending on the circumstances, OTN may seek legal recourse through civil courts.

EXCEPTIONS

Under rare circumstances, there may be exceptions to this policy. All such exceptions must be approved in advance, by email, by the Manager, Privacy and Risk, as appropriate. Any exception that does not have prior written approval will be considered a violation.

DEFINITIONS

Contact Person - Health Information Custodian that is a natural person may designate a contact person described in subsection (3). 2004, c. 3, Sched. A, s. 15 (1). Functions of include;
(a) facilitate the custodian's compliance with this Act;
(b) ensure that all agents of the custodian are appropriately informed of their duties under this Act;
(c) respond to inquiries from the public about the custodian's information practices;
(d) respond to requests of an individual for access to or correction of a record of personal health information about the individual that is in the custody or under the control of the custodian; and
(e) receive complaints from the public about the custodian's alleged contravention of this Act or its regulations. 2004, c. 3, Sched. A, s. 15 (3).

Personal Health Information (PHI) - Identifying information about an individual in oral or recorded form, if the information, relates to the physical or mental health of the individual, including information that consists of the health history of the individual's family, relates to the providing of health care to the individual, including the identification of a person as provider of health care to the

individual, is a plan of service within the meaning of the *Long-Term Care Act, 1994* for the individual, relates to payment or eligibility for health care in respect of the individual, relates to the donation by the individual of any body part or bodily substance of the individual or is derived from the testing or examination of any such body part or bodily substance, is the individual's health number or identifies an individual's substitute decision-maker.

Telemedicine Service Manager - Telemedicine Service Manager ("TSM") is proprietary software to Ontario Telemedicine Network ("OTN") allowing both clinical and education/administrative events to be scheduled over OTN's virtual private network. It is a secure, password-protected Web application designed to help Member Designated Site Contacts schedule and manage their videoconferencing system(s) and participate in scheduling OTN events, giving the scheduler full access to the TSM patient database.

REFERENCES

Personal Health Information Protection Act, 2004 (PHIPA) and Ontario Regulation 329/04 of PHIPA
The Personal Health Information Protection Act, 2004, s.2, 15

RELATED DOCUMENTS

Subject	Number
Information Security Policy	21.42.P
Privacy Breach Management Policy	18.71.PP
Scheduling Software Audit Request Form	18.80.F