Mohawk Diagnostic Imaging Repository: Privacy Auditing Procedure
Version 2.0
April 2011
# Table of Contents

1  Purpose.................................................................................................................................................. 3
2  Terminology............................................................................................................................................... 4
3  Privacy Auditing Procedure .................................................................................................................. 6
   3.1 Randomly Selected Patient Audits ................................................................................................. 6
   3.2 Randomly Selected User Audits ..................................................................................................... 7
   3.3 Patient or Clinician Requested Audits ......................................................................................... 7
   3.4 Administrator Requested Audits .................................................................................................. 7

Appendix A: Request for Audit Form ....................................................................................................... 9
Appendix B: Privacy Audit Schedule ....................................................................................................... 10
1 Purpose

The Ontario Personal Health Information Protection Act, 2004, (PHIPA) governs the collection, use, disclosure, and destruction of personal health information in Ontario, including in relation to the Mohawk Shared Services (Mohawk) Diagnostic Imaging Repository (DI-r). Hospitals and other health care organizations participating in the Mohawk DI-r are classified as “health information custodians” (HICs) under PHIPA. As such, they and are required by law to take reasonable steps to ensure that personal health information in their custody or control is protected against theft, loss and unauthorized use, disclosure, copying, modification or disposal. These organizations are required to notify individuals when their personal health information is stolen, lost or accessed by unauthorized persons. Section 6(3)4 of the PHIPA Regulation requires Mohawk, as the health information network provider of the DI-r, to keep an audit log of “all accesses to all or part of the personal health information” in the DI-r. In order to meet these requirements, health information custodians must implement an audit logging and monitoring processes.

The purpose of the auditing procedure is to enable HICs participating in the Mohawk DI-r in meeting these requirements as well as the privacy and security requirements identified in Schedule E of the DI-r Services Agreement that all HICs are required to sign as a condition of participation in the Mohawk DI-r.
## 2 Terminology

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator Requested Audit</td>
<td>A Privacy Audit completed in response to an issue or situation that may lead to a higher risk of unauthorized access to personal health information (e.g. suspicious user activity or a privacy complaint).</td>
</tr>
<tr>
<td>Agent</td>
<td>Defined in section 2 of the Ontario Personal Health Information Protection Act, 2004 (PHIPA) as a person who, with the authorization of a health information custodian, acts for, or on behalf of, a health information custodian in respect of personal health information for the purposes of the custodian, and not the agent’s own purposes, whether or not the agent has the authority to bind the custodian or is employed by or receives remuneration from the custodian. This includes staff physicians, employees, contract staff, learners and volunteers.</td>
</tr>
<tr>
<td>Diagnostic Imaging (DI) Information</td>
<td>Diagnostic images and related information, such as patient identifying and demographic information, diagnostic orders and reports.</td>
</tr>
<tr>
<td>Disclose</td>
<td>Defined in section 2 of PHIPA as making personal health information “available” or “to release it to another health information custodian or to another person.” For the purposes of the DI-r, a clinician accessing personal health information from the DI-r where the information was entered into the DI-r by a site other than the clinicians is considered to be a disclosure.</td>
</tr>
<tr>
<td>Health Information Custodian (HIC)</td>
<td>Defined in section 3(1) of PHIPA as a person or organization who is described in that section and who has custody or control of personal health information as a result of, or in connection with, the person’s or organization’s powers or duties. Health information custodians listed under section 3(1) of PHIPA include, among others, public hospitals, medical laboratories, independent health care practitioners and community care access centres.</td>
</tr>
<tr>
<td>Mohawk Shared Services (MSS)</td>
<td>A not-for-profit organization that serves clients in the health care, public and volunteer sectors with business support solutions that standardize processes, increase efficiencies and contain costs. It operates four independent business streams that focus on supply chain services, central laundry, employee assistance services and a diagnostic imaging repository.</td>
</tr>
<tr>
<td>Privacy Officer</td>
<td>An individual appointed by a custodian to facilitate the custodian’s compliance with PHIPA, ensure that agents of the custodian are appropriately informed of their duties under PHIPA, respond to inquiries and complaints from the public regarding the custodian’s privacy and information practices, and respond to requests from an individual for access to or correction of the individual’s personal health information.</td>
</tr>
<tr>
<td>Random Audits</td>
<td>Privacy audits where there is no specific reason for selecting the staff or patient. Patients/staff are randomly chosen from sources, e.g. other audits, discharge lists, or staff access lists.</td>
</tr>
<tr>
<td>Regional Shared Service (RSS)</td>
<td>The Regional Shared Service (RSS) is a program of London Health Sciences Centre that provides direction and support for implementing a shared IT solution at sites throughout Southwestern Ontario. RSS is Governed through a Memorandum of Understanding between participating organizations in LHINs 1 &amp; 2. RSS provides the diagnostic imaging technical infrastructure and support services used by MSS.</td>
</tr>
</tbody>
</table>

---

1 This definition is based on the functions of a “contact person” at section 15(3) of PHIPA.
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>support of the Mohawk DI-r.</td>
<td></td>
</tr>
<tr>
<td>Requested Audits</td>
<td>Privacy audits that are requested by a patient or SDM or a participating HIC.</td>
</tr>
<tr>
<td>Substitute Decision Maker</td>
<td>A person who is authorized under section 5 of PHIPA to consent on behalf of the individual to the collection, use or disclosure of personal health information about the individual. As such, all references to an “individual” or “patient” made in this document also apply to authorized SDMs.</td>
</tr>
<tr>
<td>Use</td>
<td>Defined in section 2 of PHIPA “to handle or deal with personal health information.” The definition of use does not include disclosing the information.</td>
</tr>
</tbody>
</table>
3 Privacy Auditing Procedure

In order to ensure compliance with PHIPA and the DI-r Services Agreement, HICs participating in the Mohawk DI-r must conduct regular privacy auditing of their clinicians’ (i.e. “agents”) activities in relation to the DI-r. It is the responsibility of the Privacy Officer of each HIC participating in the Mohawk DI-r to regularly and routinely perform such audits. Where the Privacy Officer identifies a potential or actual privacy breach relating to the Mohawk DI-r, he/she must immediately initiate the Mohawk DI-r Privacy Breach Management Policy. Privacy Officers must complete audits on:

- Randomly selected audits of patients;
- Patients or clinicians (in their role as patients) at the individual’s request; and
- Administrator Requested audit.

Each of these categories of privacy audits are discussed in detail in the following sections.

The following diagram provides a high level overview of the audit process (with the exception of the randomly selected user audits, which are initiated by RSS).

### 3.1 Randomly Selected Patient Audits

The Privacy Officers of HICs participating in the Mohawk DI-r will perform regular audits on randomly selected patients’ records as set out in the approved auditing schedule (see appendix C for approved schedule). The process for completing random patient audits is as follows:

- The Privacy Officer or delegate for the HIC/HINP will randomly select a patient to be audited.
- The Privacy Officer or delegate will complete the Request for Audit Form (see Appendix A) and forward the completed form by secure file transfer (preferred) or via fax to the Mohawk DI-r Privacy Lead (DPL).
- The DPL will work with RSS to generate the audit report from registration date up to and including 14 days post discharge date.
- The audit report will be forwarded to the Privacy Officer or delegate using secure file transfer.2
- The Privacy Officer will review and interpret the audit report and follow up with clinicians or managers to verify appropriate access and/or to identify all inappropriate or suspicious accesses.
- If the Privacy Officer identifies suspicious accesses, he/she will initiate the Privacy Breach Management Policy and Procedure for further investigation.

---

2 The secure file transfer containing the audit report has an expiration date of 7 days therefore requiring the Privacy Officer or delegate to view and save the report by another means within 7 days of being notified of the audit report being available.
The date range for all patient audits will be from Registration Date to Discharge Date adding Two Weeks following discharge or death, unless patient requests otherwise.

### 3.2 Randomly Selected User Audits

RSS will complete regular audits on randomly selected DI-r users in compliance with the audit Schedule (see Appendix B). The process for completing random user audits is as follows:

- RSS will select a random user from a DI-r User List.
- RSS will generate an audit report covering a one month period of time.
- The audit report will be forwarded to the Privacy Officer at the HIC where the user is registered for DI-r access using secure file transfer.
- The Privacy Officer will review and interpret the audit report and follow up with clinicians or managers to verify appropriate access and/or to identify all inappropriate or suspicious accesses.
- If suspicious access has been identified the Privacy Officer will initiate the Privacy Breach Management Policy and Procedure for further investigation.

The date range for all user audits will be for a One month period of time, unless otherwise requested/required, ending on date of audit request or by audit schedule date.

### 3.3 Patient or Clinician Requested Audits

Patients, including health care providers that receive care, are permitted to request a copy of their audit records within the Mohawk DI-r by contacting their HIC’s Privacy Officer and requesting a copy of accesses to their record.

The process for completing patient requested audits is as follows:

- Upon receiving a request, the Privacy Officer will complete the Request for Audit Form (see Appendix A) and/or forward the completed form by secure file transfer (preferred) or via fax to the DPL.
- The DPL will work with RSS to generate the audit report within the time period specified on the request for audit form.
- The audit report will be forwarded to the Privacy Officer or delegate using secure file transfer.
- The Privacy Officer will review and interpret the audit report and follow up with clinicians or managers to verify appropriate access and/or to identify all inappropriate or suspicious accesses.
- If suspicious access has been identified the Privacy Officer will initiate the Privacy Breach Management Policy and Procedure for further investigation.
- The patient will be contacted and provided with a copy of the audit report.

### 3.4 Administrator Requested Audits

Trigger audits will be performed on an as needed basis and can be requested by the Privacy Officer, Manager or Administrator from a HIC participating in the Mohawk DI-r. Trigger audits may be requested on:

- staff who have already received disciplinary action as a result of a privacy issue;
- patient, or a situation that the patient has been involved in, has resulted in media coverage;
• patient is a public figure likely to attract media attention, i.e. celebrity, politician, media personality, police investigation; or
• staff in the event of death or illness.
To request an administrator request audit, administrators should direct an audit request to their Privacy Officer who will complete the Request for Audit Form (see appendix A).
From this stage, the process for completing patient requested audits is as follows:
• Privacy Officer forwards the completed form by secure file transfer (preferred) or via fax to the DPL.
• The DPL will work with RSS to generate the audit report within the time period specified on the request for audit form.
• The audit report will be forwarded to the Privacy Officer or delegate using secure file transfer.
• The Privacy Officer or delegate in collaboration with the Service Area Leader will review and interpret the audit to verify appropriate access and/or to identify all inappropriate access.
• If suspicious access has been identified the Privacy Officer will initiate the Privacy Breach Management Policy and Procedure for further investigation.
Appendix A: Request for Audit Form

NAME of HOSPITAL: _________________________________________________

Requests a
☐ RANDOM AUDIT
☐ REQUESTED AUDIT BY____________________________________________
☐ ADMINISTRATOR AUDIT

Date of Request:_________________ Requested Date of Completion________________

PATIENT:

PIN# ______ Reg. Date_______ Discharge Date ______ Date of birth: _________________

Patient/Client Name: _____________________________________________________________

<table>
<thead>
<tr>
<th>Last Name</th>
<th>Given Name</th>
<th>Middle Name</th>
</tr>
</thead>
</table>

Health Card #: ____________________________________________

USER/STAFF/AGENT:

User/Staff/Agent Name: ________________________________________________

<table>
<thead>
<tr>
<th>Last Name</th>
<th>Given Name</th>
<th>Middle Name</th>
</tr>
</thead>
</table>

Role/Position: ____________________________ Username _______________

Service Area: ___________________ Name of Manager (if known): ______________________

Date range for audit: (FROM: __________________________ TO:___________________

Additional Information if applicable:

Forward completed form to Mohawk DI-r Privacy Officer, Diane Larwood, by Secure File Transfer (Preferred) or secure email at dlarwood@mohawkssi.com or via fax at 905-639-6688

FOR REGIONAL PRIVACY SPECIALIST USE ONLY

☐ Ran Audit on Date: __________________________
☐ Logged in Audit Stats and Audit Flowsheet
☐ Sorted and Interpreted
☐ Transferred to PO by SFT on ________________
Appendix B: Privacy Audit Schedule

Regional Shared Service will complete privacy audits on Mohawk DI-r patients and users on request and on a random basis as follows:

- **LHIN 3** – Random user audit once every 6 months on the 15th day of April and October.
- **LHIN 4** – Random user audit once every 6 months on the 15th day of May and November.