Summary of Privacy Impact Assessment Update

Hospital Report Manager Expansion Project
OntarioMD

Version: 0.1
Last Revised: August 14, 2013

Table of Contents

1 Introduction 1
1.1 The Hospital Report Manager 1
1.2 HRM Expansion Project 1
2 Legislative authority 2
2.1 Personal Health Information Protection Act, 2004 2
3 Key findings of the PIA 2
3.1 Accountability Mechanisms 3
3.1.1 Agreements 3
3.1.2 Policies and procedures 3
3.1.3 Training 4
3.1.4 Assurance 4
3.2 Limiting Use, Disclosure and Retention 5

1 Introduction

This document provides a summary of a privacy impact assessment (PIA) update conducted for OntarioMD (OMD) by MD+A Health Solutions. The PIA update was conducted on the Hospital Report Manager (HRM) product provided to health care providers by OntarioMD.

OMD engaged MD+A to update a previous privacy impact assessment on the HRM that MD+A had completed in September 2012. The analysis in the PIA update focused on OMD's role within the HRM initiative, and addressed changes to the HRM solution and hosting environment since the previous PIA.

The PIA update also addressed changes to HRM business processes supporting the management of system users and of Personal Health Information (PHI) in the HRM system, the OMD privacy program for HRM, and administrative and technical safeguards for PHI that were developed and implemented since the last PIA was completed.

The PIA update identified only new privacy risks, and did not carry forward risks from the previous PIA that OMD has mitigated or is in the process of mitigating. The PIA update also provides recommendations for reducing the privacy risks that were identified.

1.1 The Hospital Report Manager

OMD developed the HRM to enable clinicians using Electronic Medical Records (EMRs) specification 4.1a (or higher) to receive hospital or Independent Health Facility (IHF) reports electronically. Through the HRM solution, hospitals or IHFs that send such reports (sending facilities) are able to transmit electronic copies of key text-based reports (i.e., medical records and diagnostic imaging reports) directly into a patient's record within the clinician's EMR at designated practices that have registered to receive the reports through the HRM (receiving facilities).

The HRM provides a variety of benefits: reports can be delivered and inputted into the patient chart much more quickly than paper reports which are mailed or faxed. Electronic reports offer greater flexibility to clinicians, since it can be queried and searched by EMRs, and it reduces the administrative overhead associated with such activities as the scanning of paper reports into a clinician's EMR.

Other benefits associated with electronic hospital reports via HRM include the potential to improve the continuity of care from hospitals to community-based clinicians (who can follow-up more quickly with patients since they receive the hospital reports sooner) and to increase the adoption of EMR systems by clinicians.

1.2 HRM Expansion Project

OMD has piloted the HRM solution with a limited scope of sending and receiving facilities in Ontario, and now intends to expand access to the solution, as part of the broader provincial

strategy to promote more efficient sharing of clinical information. OMD will launch a first production release of the HRM – the HRM Expansion Project – which will extend the HRM service to 1560 newly registered clinicians, along with 3-6 new hospitals or service hubs, by March 2014, and will also provide continued support to the HRM pilot sites.

OMD has engaged eHealth Ontario to provide supporting technical and business services for the Expansion Project, including managed hosting of the HRM solution, and provision of help desk services for HRM subscribers both at sending facilities and receiving facilities.

2 Legislative authority

2.1 Personal Health Information Protection Act, 2004

The PIA indicates that OMD is a health information network provider (HINP) under PHIPA, and specifically under O. Reg. 329/04. The regulation defines a HINP as:

> *s.6(2)(3) … a person who provides services to two or more health information custodians where the services are provided primarily to custodians to enable the custodians to use electronic means to disclose personal health information to one another, whether or not the person is an agent of any of the custodians.*

The regulation goes on to define the requirements that a HINP must meet. These requirements are meant to provide the health information custodians to which the HINP provides its services with assurance that the HINP is appropriately managing PHI. OMD has agreed to meet these requirements in its agreements with the sending and receiving facilities, and has developed privacy safeguards to support it in meeting these requirements.

3 Key findings of the PIA

MD+A's assessment of the HRM Expansion Project in the PIA update was based on the following activities:

- review of relevant program and technical documentation, including agreements, policies and procedures, training, operations manuals, and technical documentation;
- interviews with the HRM project team at OMD to address HRM business processes and PHI information flows, HRM program governance, the HRM privacy framework developed by OMD, and information security safeguards within the HRM solution;
- documentation of the MD+A privacy analysis organized by the ten principles in the Canadian Standards Association's Model Code for the Protection of Personal Information.

Based on this assessment process and MD+A's associated privacy analysis, MD+A considers the privacy posture for the HRM initiative to be, in general, sound.

OMD has conducted work in key areas on the remediation of issues identified in the previous HRM PIA. This work includes development of agreements to govern the participation of the HRM

stakeholders and of eHealth Ontario as service provider to OMD; and the development of HRM policies and procedures that address privacy protection for the initiative. The HRM solution is also subject to robust technical and administrative safeguards that have been implemented by the OMD solution development team.

MD+A nonetheless identified a range of privacy issues in the PIA update that OMD should address before launching the Expansion Project. The key issues (i.e., those rated at Medium or High priority in the PIA) have been summarized in the sections below.

3.1 Accountability Mechanisms

MD+A identified a series of issues related to the accountability mechanisms that OMD has put in place for the HRM Expansion Project.

3.1.1 Agreements

For the Expansion Project, OMD has agreed to route reports to receiving facilities on behalf of some of the sending facilities; this represents a change from the pilot implementation, in which sending facilities routed their reports using a locally-hosted component (an interface engine to the HRM). In the new model, OMD will receive from some sending facilities not just the reports intended for clinicians who are HRM subscribers, but all reports that are intended for a clinician (a physician or nurse practitioner), regardless of whether or not the clinician is enrolled in HRM.

OMD will then, on behalf of these sending facilities, determine which of the report recipients are HRM subscribers, and route these reports to the appropriate receiving facilities. This represents a new PHI-management service that will be provided by OMD as part of the overall HRM offering. However, the service is not described in the version of the sending facility agreements with OMD provided to MD+A for review.

> *M+D recommends that OMD should describe this service in its relevant agreements and describe the privacy safeguards it will deploy when offering the service. MD+A also recommends that OMD seek legal counsel regarding its role under PHIPA when providing this service, since this role may be an Agent role rather than a HINP role.*

3.1.2 Policies and procedures

OMD has not developed any shared procedures for privacy incident management between itself and the sending and receiving facilities. While in general all parties will rely on their own privacy incident management procedures to address privacy incidents, there may be times when OMD and one or more sending or receiving facilities will need to work together to address an HRM-related privacy incident. OMD and the facilities should be able to rely in documented procedures that, primarily, identify the points in the incident management process where parties should communicate with one another to ensure timely resolution of incidents.

MD+A recommends that OMD develop these shared privacy incident management procedures and include them in the Operations User Guide that will be provided to the sending and receiving facilities.

OMD has developed a procedure for the sending and receiving facilities to request logs to support auditing and access requests. However, it has not developed an internal procedure for making log information available to the facilities. OMD's internal Logging and Auditing Procedure specifies the types of logs that are available from the HRM solution environment, but the procedures for making the logs available to sending and receiving facilities have not been included.

Without such procedures, OMD may not properly fulfill a request for logs, or may leave such a request unfulfilled. Providing this log information is a PHIPA requirement for OMD; therefore, a failure to do so could result in OMD being non-compliant with PHIPA.

MD+A recommends that OMD develop internal procedures for making HRM logs available to sending and receiving facilities that request the logs.

3.1.3 Training

While OMD provides its employees with general privacy training as a condition of employment, it has not developed HRM-specific privacy training for employees who have HRM-related responsibilities. However, OMD should develop such training to ensure that the HRM-specific privacy responsibilities of its employees have been made clear.

Such training would provide these employees with an overview of the HRM privacy policy and the privacy safeguards and processes that OMD has established for the program. The training should address the reasons for which OMD staff on the HRM program can access PHI, the requirement to protect the privacy of the data on behalf of the sending and receiving HICs, and the obligation to notify the OMD privacy officer should they suspect an incident.

The training should also provide more information on OMD's obligations as a HINP under PHIPA, and the processes that have been established for working with the HICs to address incidents or complaints.

MD+A recommends that OMD develop this HRM-specific privacy training for the Expansion Project.

3.1.4 Assurance

Under O. Reg. 2329/04 of PHIPA, OMD as a health information network provider is required to provide the HICs to which it provides services with the results of privacy and security assessments of those services. In OMD's case, this would include assessments of the hosting and support services provided by eHealth Ontario. However, eHealth Ontario has indicated that it is not prepared to share the privacy and security assessments it has conducted on its hosting environments with OMD. Without this information, OMD will not be able to provide assurance to participating HICs regarding the services that are provided to support HRM.

OMD is currently in discussion with eHealth Ontario to receive attestation from eHealth Ontario that these assessments have been conducted and the identified risks have been managed. Ideally, such an attestation should be accompanied by summaries of the relevant assessments; eHealth Ontario is obligated under PHIPA to support OMD in meeting its HINP obligation in this regard.

MD+A recommends that OMD secure from eHealth Ontario attestation that eHealth Ontario has recently conducted privacy and security assessments of its hosting facilities and services; this attestation should include summary of the risks that these assessments identified and the measures taken to address the risks.

OMD should be able to provide assurance to sending and receiving facilities regarding its own compliance and that of its service providers with HRM-related privacy obligations. Given the relatively limited scope of the solution itself, and of OMD's expected access to PHI, such assurance could be provided through reporting on the audit logs that OMD will implement for the HRM solution.

However, although OMD has defined the logging that will be implemented to support privacy auditing of the HRM solution, it has not documented the procedures that it will follow to review audit logs related to the HRM solution, and provide reporting on this review to the sending and receiving facilities as an assurance mechanism. This review should include relevant logs from the eHealth Ontario environment. OMD should develop this reporting process with input from the HRM steering committee, and the process should be approved by the OMD privacy officer before it is implemented.

MD+A recommends that OMD develop procedures for reviewing audit logs and reporting on this review to the sending and receiving facilities.

3.2 Limiting Use, Disclosure and Retention

MD+A identified some additional issues related to OMD's appropriate limitation of use, disclosure and retention of PHI. Specifically, these issues pertain to the documentation of OMD's documentation of its access rights for its own employees, and to the information provided by eHealth Ontario about the access of its employees to PHI managed by the HRM solution.

Although OMD has identified by name the employees with access to HRM system components, and to PHI, this information has been documented the HRM Logging and Auditing Procedure. However, this solution access information should be documented in an internal information management guideline for the HRM program, and list the roles and individuals with access to the system in this guideline. The guideline should additionally identify the reasons for the access that any OMD employee has to any component of the HRM system.

MD+A recommends that OMD create this guideline before the launch of the Expansion Project.

The agreement between OMD and eHealth Ontario clearly indicates that eHealth will not allow any access by its employees to PHI in the HRM "unless necessary in connection with the Hosting

Services." However, eHealth Ontario has not provided any documentation that MD+A was aware of that indicates the roles and/or individuals within the eHealth Ontario managed hosting environment who will have access to PHI within the HRM system.

MD+A recommends that OMD requests this information from eHealth Ontario. The information should indicate the high-level contractual responsibilities associated with each identified role.