

Answers to Frequently Asked Questions on the Privacy Practices of Enterprise Master Patient Index

Privacy Officers

Table of Contents

1.0	What privacy laws apply to the EMPI?	1
2.0	How does PHIPA apply to the EMPI?	1
3.0	Who is responsible for the privacy practices of the EMPI?.....	1
4.0	What are hospitals’ privacy responsibilities for the EMPI?.....	2
5.0	For what purpose does the EMPI collect personal health information?	2
6.0	Under what authority can hospitals disclose personal health information to eHealth Ontario via the EMPI?	2
7.0	What safeguards are in place to protect personal health information in the EMPI?	2
8.0	How long does the EMPI retain personal health information and how is record destruction handled?	3
9.0	How much personal health information is collected, used, or disclosed for identification management purposes?	3
10.0	How will the MOHLTC avoid unnecessary access by physicians, hospitals and other staff to personal health information?	3
11.0	Are hospitals required to obtain patient consent to send personal health information to the EMPI for patient identification purposes?	4
12.0	How does the EMPI assist hospitals in ensuring that personal health information is kept as accurate, complete and up-to-date as necessary for the purpose for which it was collected?	4
13.0	What is a privacy breach?.....	4
14.0	What is the obligation to notify an individual of a privacy breach?	4
15.0	What is the procedure for responding to a EMPI-related privacy breach or complaint?	5

1.0 What privacy laws apply to the Enterprise Master Patient Index?

The collection, use, and disclosure of personal health information via the Enterprise Master Patient Index (EMPI) are subject to Ontario's Personal Health Information Protection Act, 2004 (PHIPA). The term "personal health information" includes any identifying information relating to a patient's health or health history, including his or her health number. Therefore, all data flows relating to the EMPI will be governed by PHIPA. More information on PHIPA is available on the Information and Privacy Commissioner/Ontario's (IPC) website at: <http://www.ipc.on.ca>.

2.0 How does PHIPA apply to the EMPI?

PHIPA provides specific "privacy rules" relating to the collection, use, and disclosure of personal health information by "health information custodians" (e.g. hospitals) and their "agents," those individuals acting on behalf of health information custodians (e.g. physicians, nurses, registration clerks). The EMPI is operated by eHealth Ontario, effective January 1, 2008, acting as an "agent" of the Ministry of Health and Long-Term Care (MOHLTC). The MOHLTC is classified as a health information custodian under PHIPA.

Furthermore, under PHIPA, a "health information network provider" is an organization that provides services to two or more health information custodians (e.g. hospitals and the MOHLTC) to enable the custodians to use electronic means to disclose personal health information to one another. eHealth Ontario, which is providing network services for the EMPI, also serves as the "health information network provider" for the EMPI.

PHIPA sets out specific rules for "health information custodians", "agents" and "health information network providers". A detailed analysis of these rules, as they relate to the EMPI, is available in the EMPI privacy impact assessments.

3.0 Who is responsible for the privacy practices of the EMPI?

PHIPA requires a health information custodian to designate a contact person (sometimes referred to as a Privacy Officer) to be accountable for the custodian's overall compliance with PHIPA, including responding to access and correction inquiries and privacy complaints from the public. The MOHLTC has designated the Manager of the Access and Privacy Office as the contact person to oversee the MOHLTC's information practices. More information, including contact information, is available online at http://www.health.gov.on.ca/english/public/legislation/bill_31/stat_info_practices.pdf).

eHealth Ontario has also designated an EMPI Privacy Lead to act as the EMPI Operations Team's "privacy contact". Any questions or concerns pertaining to the EMPI or its information practices can be directed to the EMPI Privacy Lead at: EMPIPrivacy@eHealthOntario.on.ca, who will work with the Manager of the Access and Privacy Office at MOHLTC to respond to privacy-related questions and/or complaints.

4.0 What are hospitals' privacy responsibilities for the EMPI?

All Ontario hospitals are classified as health information custodians under PHIPA and are subject to the privacy rules contained within the Act. PHIPA requires hospitals to develop and implement PHIPA-compliant information practices and inform their patients about the purposes for which the hospital collects, uses, or discloses their patients' personal health information. To that end, where requested by the patient, a hospital must provide their patients with adequate information about the EMPI, including a description of the legal authority under which it releases patient information for the purpose of the EMPI. The EMPI Operations Team has developed a set of frequently asked questions (FAQs) about the EMPI's privacy practices tailored to patients which can be used by hospitals to answer patients' questions.

Hospitals may also direct all EMPI-related inquiries to their own EMPI site representative or by contacting the EMPI Privacy Lead at: EMPIPrivacy@eHealthOntario.on.ca.

5.0 For what purpose does the EMPI collect personal health information?

The EMPI collects personal health information relating to individuals receiving health services in Ontario in order to accurately identify records of personal health information that relate to that unique individual. EMPI data elements include, for example, patient names, addresses, medical record numbers, date of birth, health card numbers and other demographic information.

6.0 Under what authority can hospitals disclose personal health information to eHealth Ontario via the EMPI?

Section 43(1)(h) of PHIPA permits hospitals to disclose personal health information without a patient's consent if permitted or required by law. In addition, section 23(b) of Regulation 965 made under the Public Hospitals Act, 1990, permits hospitals to provide personal health information upon the request of the Minister to a person identified by the Minister (such as eHealth Ontario) for purposes of information and data collection, organization and analysis. In combination, these two statutory provisions permit hospitals to release personal health information to eHealth Ontario via the EMPI.

7.0 What safeguards are in place to protect personal health information in the EMPI?

Personal health information in the EMPI is protected by administrative, technical and physical safeguards. Administrative safeguards have been implemented through contractual means and include an agency agreement between the MOHLTC and eHealth Ontario that addresses how the privacy rules under PHIPA will be met. This agreement provides specific privacy protective steps that eHealth Ontario must take as an agent of the MOHLTC to keep personal health information confidential and secure. Contractual privacy safeguards have also been included in the licensing agreement between eHealth Ontario and the EMPI software vendor to prevent unauthorized access to and disclosure of personal health information.

Technical safeguards, such as passwords, role-based access to information, and encryption, are used to protect the EMPI from unauthorized access.

The eHealth Ontario data centre, where the EMPI data is housed, incorporates a number of physical safeguards including restricted access to its operational environment, video monitoring and a security guard on duty 24 hours a day, 7 days a week. In addition, eHealth Ontario has facilities policies, which outline the physical controls in place to protect the EMPI Operations Team environment.

8.0 How long does the EMPI retain personal health information and how is record destruction handled?

PHIPA does not provide specific retention periods or disposal methods for personal health information stored in the EMPI. However, it does specify that records must be kept as long as needed to allow patients to exhaust any legal recourse relating to access requests and requires such records to be disposed of in a secure manner. The EMPI only collects data elements that contribute to accurately resolving the identity of an individual who has received health care services in Ontario and to link this information with previous health system encounters in order to support the delivery of health care services. To this end, the EMPI retains personal health information for at least the lifetime of the patient.

If the EMPI Operations Team retains paper copies of personal health information for any reason, they are stored in secure locations, which are physically locked when unattended (e.g. locked drawers). Paper copies that are no longer required are immediately shredded.

9.0 How much personal health information is collected, used, or disclosed for identification management purposes?

PHIPA requires that hospitals and physicians restrict the collection, use, or disclosure of personal health information to the minimum amount necessary for the identified purpose. As such, the EMPI only collects, uses, or discloses the minimum data required to fulfill its mandate of accurately identifying individuals receiving health care services and treatment in Ontario. The EMPI data elements include, for example, patient names, addresses, medical record numbers, dates of birth and health card numbers. A complete listing of the EMPI data elements is included in the EMPI privacy impact assessments.

10.0 How will the MOHLTC avoid unnecessary access by physicians, hospitals and other staff to personal health information?

The EMPI utilizes role-based access control, which is maintained administratively by the EMPI Operations Team and technically by the EMPI application server. All individuals who directly access the EMPI must be registered users of eHealth Ontario.

11.0 Are hospitals required to obtain patient consent to send personal health information to the EMPI for patient identification purposes?

No. Personal health information collected by hospitals may be disclosed to the EMPI under the legal authority of section 43(1)(h) of PHIPA which permits hospitals to release patient information without consent where it is required by law. Hospitals are required by law, under section 23(b) made under the Regulation of the Public Hospitals Act, to release personal health information to a person identified by the Minister for data collection, organization and analysis. Accordingly, where requested to do so by the Minister this provision, in conjunction with section 43(1)(h) of PHIPA, allows hospitals to disclose personal health information directly to eHealth Ontario on behalf of the MOHLTC without consent for the purpose of the EMPI. This means that patients may not “lock” their personal health information from being disclosed to the MOHLTC for the purpose of the EMPI.

12.0 How does the EMPI assist hospitals in ensuring that personal health information is kept as accurate, complete and up-to-date as necessary for the purpose for which it was collected?

Under PHIPA, health information custodians (i.e. hospitals) are required to take reasonable steps to ensure that their patients’ personal health information is as accurate, complete and up-to-date as necessary for the purpose for which it is used or disclosed. The quality and completeness of information that is collected by the EMPI from hospitals determines the integrity and reliability of the EMPI data. To ensure the accuracy of record linkages, the EMPI engine conducts a probabilistic assessment of whether the data elements received from multiple source information systems represent the same individual. In addition, the EMPI Operations Team performs manual corrections and merges and unmerges records, where required, to ensure the accuracy of EMPI data.

13.0 What is a privacy breach?

A privacy breach refers to a situation, whether accidental or intentional, involving the unauthorized collection, use, or disclosure of personal health information. For example, a privacy breach has occurred if personal health information is stolen, deleted, or modified improperly in an electronic information sharing system.

14.0 What is the obligation to notify an individual of a privacy breach?

PHIPA requires hospitals to notify patients as soon as reasonably possible where personal health information is stolen, lost, or accessed by unauthorized persons. This notification requirement also applies to administrative and clinical staff working at hospitals and the EMPI Operations Team that handles personal health information on behalf of the MOHLTC.

15.0 What is the procedure for responding to an EMPI-related privacy breach or complaint?

Hospitals are responsible for ensuring that their EMPI users use and access the EMPI in compliance with their hospital's security and privacy policies. Hospitals are also responsible for responding to privacy breaches caused by their EMPI users in a timely manner. Similarly, the EMPI Operations Team is responsible for ensuring that all personal health information that staff have access to is not inadvertently or intentionally stolen, lost, or accessed by unauthorized persons. Where a privacy breach occurs, the EMPI Operation Team will immediately contain, investigate, and resolve the breach in coordination with the MOHLTC.

Privacy or security questions or concerns relating to the EMPI may be directed to each participating hospital's EMPI site representative or to the EMPI Privacy Lead at: EMPIPrivacy@eHealthOntario.on.ca, or