eHealth Ontario
www.ehealthontario.on.ca

User Registry

Privacy Impact Assessment Summary

Ontario
eHealth Ontario

Copyright Notice

All rights reserved

Trademarks

Introduction

As required under eHealth Ontario's Privacy Impact Assessment Policy, eHealth Ontario has completed a Privacy Impact Assessment (PIA) on eHealth Ontario's user registry (UR) initiative in October 2011.

The following is a summary of the PIA, including a brief background on the UR initiative, key findings, and eHealth Ontario's progress in implementing the recommendations identified in the PIA.

Background

The user registry is a key component of eHealth Ontario's cornerstone information systems, and was designed and built by the identity, access, and privacy program at eHealth Ontario. The UR initiative was developed to provide a single solution to control user access to eHealth services and track the electronic identities of prospective individuals and provider organizations that interact with eHealth Ontario's systems. The UR acts as an authentication and authorization service for end-user access to eHealth services such as the chronic disease management system-diabetes registry (CDMS-D), the Ontario laboratories information system (OLIS), and the Ontario drug benefits (ODB) database.

The cornerstone of the UR is the federation concept. A federation is an association of organizations that have taken on roles of identity provider or service provider. Service providers, such as eHealth Ontario, provide services for users, and trust the identity providers to authenticate users and provide accurate user information to the service provider, which is used for authorization to the services. The UR is a key component in enabling the federated trust model with partnered organizations, and ensuring secure access to personal health information (PHI).

As providers submit service requests to access eHealth services, the UR validates and records the requests and maps the federated user identities (as asserted in the request) to the real identities of the providers, found in eHealth Ontario's provider registry (PR). If this validation step is successful, then a service authorization request is made to the UR for access to eHealth Ontario services. The UR authorizes service entitlement by verifying that the user has the right level of trust to access the requested service, in accordance with appropriate legislation, regulation and policy (as represented by the entitlement rules stored in the UR). The UR assigns users to pre-defined roles based on their attributes and issues permission or denial for the given service request.

The UR does not collect, use or disclose any PHI as defined by Ontario's *Personal Health Information Protection Act, 2004* (PHIPA). The information used by the UR for validation and service entitlement includes provider information, such as license number, last name and standing with their regulatory colleges. The information received and used by the UR for authorization purposes includes a limited amount of personal information (PI), as defined in the *Freedom of Information and Protection of Privacy Act* (FIPPA). A physical PIA is required because the UR is receiving and using PI from the PR; it interfaces with systems that collect, use, or disclose PI/PHI; and it is ultimately responsible for authenticating/authorizing end-user access to PI and PHI within eHealth Ontario's infrastructure.

Summary of Privacy Impact Assessment

The UR Physical PIA considers all components and features in the UR production environment, including the version currently in use (release 1), and up to and including UR release 2, as will be deployed as part of the CDMS-D (scheduled for November 2011). Specifically, the scope of the UR PIA includes the flow of information to, within, and from the UR to connected systems; business processes that involve the acquisition, recording, storage, usage or sharing of information in the UR; and the legislative authority under which eHealth Ontario may operate and manage the UR. The PIA also considers the technical, administrative and physical safeguards which have been put in place to ensure that all flows of data occur in a secure and privacy-protective manner, and are in compliance with legislative requirements, relevant agreements, best practices as represented in the Canadian Standards Association Privacy Code and eHealth Ontario's privacy policies.

The PIA concludes that eHealth Ontario has the overall legislative authorities for operating and managing the UR. Additionally, eHealth Ontario has a robust infrastructure for the processing and protection of sensitive data, with policies and practices to protect the privacy of Ontarians and the security of the information retained by eHealth Ontario.

The PIA recommends several measures to ensure that, for the UR initiative, eHealth Ontario is in compliance with relevant legislation, as well as eHealth Ontario policies, procedures and privacy best practices.

Summary of the Implementation Plan for the Privacy Impact Assessment Recommendations

The physical PIA provides a number of recommendations associated with the UR initiative, as summarized below:

1. eHealth Ontario to use the enhanced provider profile information (EPPI) (consisting of gender and date of birth) obtained from the PR in accordance with the terms of the agreement between the College of Dieticians of Ontario and eHealth Ontario, or amend the agreement as required.

2. eHealth Ontario's privacy and security groups should be consulted in the definition and implementation of entitlement rules in the UR to check that the access to PHI or PI granted by the rules is appropriate.

3. eHealth Ontario should ensure that its personal information bank is up-to-date with respect to the PI used by the UR.

eHealth Ontario is currently in the process of implementing each of the recommendations identified in the 2011 UR Physical PIA.

Glossary

CDMS-D	chronic disease management system -diabetes registry
EPPI	enhanced provider profile information
FIPPA	*Freedom of Information and Protection of Privacy Act*
MOHLTC	Ministry of Health and Long-Term Care
ODB	Ontario drug benefits
OLIS	Ontario laboratories information system
O.Reg.	Ontario Regulation
PHIPA	*Personal Health Information Protection Act, 2004*
PHI	personal health information
PI	personal information
PIA	Privacy Impact Assessment
PR	provider registry
UR	user registry

Contact Information

Please contact the eHealth Ontario privacy office should you have any questions about the UR PIA summary:

eHealth Ontario
Privacy office
777 Bay Street, Suite 701
Toronto Ontario M5B 2E7
Tel: (416) 946-4767
privacy@ehealthontario.on.ca