eHealth Ontario

Privacy and Security Frequently Asked Questions for Users

ONE Mail Services

Version: 1.1

Document ID: 3826

Document Owner: Manager, ONE Mail

Ontario
eHealth Ontario

Copyright Notice

All rights reserved

Trademarks

Document Control

The electronic version of this document is recognized as the only valid version.

Revision History

1.1	2015-03-16	Minor Revisions as per Manager, ONE Mail	Promila Gonsalves, Sr. Privacy Business Analyst
1.0	2014-06-16	Final Draft	Promila Gonsalves, Privacy Analyst

Document ID

3826

Document Sensitivity Level

Low

Overview

The ONE Mail service is comprised of ONE Mail, ONE ID, and ONE Pages (the ONE Mail directory) to facilitate the exchange of encrypted email between healthcare organizations. eHealth Ontario follows best practices and legislative requirements (the *Freedom of Information and Protection of Privacy Act, 1990* and the *Personal Health Information Protection Act, 2004*).

The following information describes eHealth Ontario's privacy requirements and outlines the policies and practices implemented at eHealth Ontario to provide ONE Mail services to users.

Frequently Asked Questions

What privacy legislation is eHealth Ontario subject to when providing ONE Mail Services?

eHealth Ontario is subject to the Ontario Regulation 43/02 under the *Development Corporations Act (DCA), 1990*, the *Personal Health Information Protection Act, 2004* (PHIPA) and the *Freedom of Information and Protection of Privacy Act, 1990* (FIPPA).

How is privacy and security governed at eHealth Ontario?

Approval bodies and privacy-related committees oversee the protection of privacy at eHealth Ontario. The Chief Privacy Officer at eHealth Ontario is accountable for ensuring compliance with privacy legislative requirements and oversees the design of eHealth Ontario products and services to ensure the inclusion of privacy protective features. eHealth Ontario also maintains a suite of privacy policies that foster a culture of privacy protection. The *eHealth Ontario Privacy and Data Protection Policy* is the overarching privacy policy. These policies are made available to the public at http://www.ehealthontario.on.ca/en/privacy.

The Chief Security Officer at eHealth Ontario is accountable for ensuring compliance with security policies and oversees the design of eHealth Ontario products and services to ensure the inclusion of security protective features. The *eHealth Ontario Information Security Policy* and safeguards implemented at eHealth Ontario can be found at http://www.ehealthontario.on.ca/en/security.

What information does eHealth Ontario collect to provide the ONE Mail service and how is it used?

To provide the ONE Mail service, the following information is collected:

- Registration Information: personal information is collected to register a user to establish a unique identity for the registrant.
- Mail directory Information: business contact information for registered ONE Mail users to allow the look-up and secure transmission of PI/PHI to other ONE Mail users.
- Mailbox metadata: mailbox usage information that assists in the operation and planning of the ONE Mail service.

How does eHealth Ontario safeguard my personal information?

eHealth Ontario implements and maintains a number of physical, administrative and technical safeguards to protect the privacy and security of information collected.

These safeguards include but are not limited to:

1. Administrative Safeguards

- eHealth Ontario privacy and security policies, procedures and practices are in place to meet legislative and contractual requirements;
- All personnel and service providers must sign confidentiality agreements and undergo criminal background checks prior to joining or providing services to eHealth Ontario.
- eHealth Ontario has a security screening policy that requires personnel to have an appropriate level of clearance for the sensitivity of the information they may access.
- eHealth Ontario has mandatory privacy and security awareness and training programs for personnel, which includes a quiz to confirm that the main concepts and behaviour requirements were understood.
- eHealth Ontario personnel and service providers generally have no ability or permission to access PHI. If access to PHI is required in the course of providing eHealth Ontario services, individuals are prohibited from using or disclosing such information for any other purposes.
- eHealth Ontario ensures, through formal contracts and service level agreements, that any third party it retains to assist in providing services to eHealth Ontario or to health information custodians will comply with the restrictions and conditions necessary for eHealth Ontario to fulfil its legal responsibilities.
- eHealth Ontario personnel and service providers must promptly report any privacy and security breaches to eHealth Ontario for investigation. An enterprise security and privacy incident management program is in place to ensure management of incidents and regular training and awareness for personnel involved in incident management.
- Privacy impact assessments (PIAs) and Security threat and risk assessments (TRAs) are conducted as part of both product/service development and client deployments. Privacy and security risk mitigation

activities are established, assigned to a responsible individual, recorded and tracked as part of each assessment.

- Upon request, eHealth Ontario provides a written copy of the results of privacy impact assessments and security threat and risk assessments to the affected health information custodians. Additionally, eHealth Ontario publishes summaries of physical and delta PIAs, where eHealth Ontario is providing services under PHIPA O. Reg 329/04 sections 6 and 6.2, on the eHealth Ontario website.

2. Technical Safeguards

- Strong passwords, secure tokens, and other authentication solutions are required for administrators to access sensitive systems.
- Administrative access to all IT equipment and applications is provided on a need to know basis controlled via proper authorization and strong, two-factor authentication.
- Access to ONE Mail servers is limited to only those individual who provide technical day to day support for ONE Mail Services;
- All data stored on personnel computers is encrypted.
- Firewalls, anti-virus, anti-spoofing and anti-spam attempt to filter the email messages to eliminate viruses and other harmful content or unsolicited bulk emails.

3. Physical Safeguards

- The eHealth Ontario data centres are purpose-built facilities, with appropriate environmental controls and physically secured against unauthorized access. They are staffed and monitored continuously by trained security personnel.
- Specific physical security zones are implemented to separate and control access to public zone, delivery and loading area, office space, and computer rooms, with increasing physical security controls.
- Data centre physical security controls have been validated by an independent third party in accordance with federal government standards, and through internally conducted threat and risk assessments.
- Access to office areas is controlled with access badges, and traffic in the office areas is recorded by security cameras.
- Visitors and third-party vendors to eHealth Ontario require visitor badges and are escorted at all times by personnel. Access badges expire automatically within 24 hours and cannot be reused.
- Decommissioned equipment that was used to process or store PI or PHI is securely disposed of, according to approved procedures.

4. How is information securely transmitted using the ONE Mail service?

- Information transmitted via the ONE Mail service is only secured when transferred from one ONE Mail user to an email recipient selected from ONE Pages (the ONE Mail directory). The ONE Mail service will enforce encryption when routing emails through the mail system. Information transferred to an email recipient that is not listed in ONE Pages cannot be guaranteed security as it is being transferred outside of the secure ONE Mail system.

- Secure transfer can only be guaranteed to the ONE Mail demarcation point. Users synchronizing messages to a mobile device, laptop or desktop may wish to add additional safeguards such as ensuring they are on a trusted network or connecting over a virtual private network (VPN), as well as adequate password protection for the device.

5. How long does eHealth Ontario store emails?

eHealth Ontario does not store emails transmitted through the ONE Mail Direct service. eHealth Ontario's mail servers are backed up at least once daily and retains a copy of the backups for a minimum of 30 days. A copy of each email sent or received should be stored in accordance with your organization's records management practices.

End User Responsibilities

End users of the ONE Mail system are guided by the eHealth Ontario's Acceptable Use Policy and the ONE Mail guides.

Resources

For more information about security or the ONE Mail service, please see http://www.ehealthontario.on.ca/en/.

For more information about privacy at eHealth Ontario, please see http://www.ehealthontario.on.ca/en/privacy or contact us at privacy@ehealthontario.on.ca You can also mail inquires to the Chief Privacy Officer at:

eHealth Ontario
Privacy Office
777 Bay Street, Suite 701
Toronto, Ontario
M5B 2E7