eHealth Ontario
It's working for you

Privacy and Security Standard of Conduct

Version: 3.3

Document ID: 00990

Document Owner: Chief Privacy Officer and Chief Information Security Officer

Sensitivity Level: Low

Ontario
eHealth Ontario

Contents

Tables

1 Purpose

This *eHealth Ontario Privacy and Security Standard of Conduct* ("Standard") supports eHealth Ontario's ("Agency") commitment to privacy and security by establishing clear behavioural expectations for Personnel and Service Providers who utilize Agency assets or handle the Agency's Sensitive Information, which includes Personal Information ("PI") and Personal Health Information ("PHI"). This Standard articulates:

- An understanding of privacy and security at eHealth Ontario, including a summary of the Agency's legislative and policy requirements related to these areas;
- A practical understanding of the Agency's expectations of Personnel who, in the course of their work at eHealth Ontario, must protect the privacy and security of the Sensitive Information they create, use, access, disclose or otherwise manage; and
- A practical understanding of the Agency's expectations of Service Providers who, in the course of their supply of goods or services to eHealth Ontario must protect the privacy and security of the Sensitive Information they create, use, access, disclose or otherwise manage.

This Standard enables Personnel and Service Providers to understand their privacy and security obligations which they will adhere to during the course of their employment or engagement, as the case may be, and which shall be evidenced through their attestation of the eHealth Ontario Privacy and Security Acknowledgement and Agreement, as described herein.

2 Scope

The responsibilities described in this Standard apply to all eHealth Ontario Personnel and Service Providers.

"Personnel" refers to all Agency employees including Full-Time Regular Employees, Full-Time Temporary Employees, Part-Time Regular Employees, Part-Time Temporary Employees, students and interns.

"Service Providers" means an individual or entity that eHealth Ontario contracts with to provide goods or services that assist in the delivery of eHealth Ontario's mandate. The term includes, but is not limited to, vendors and consultants. The focus of this Policy is on Service Providers whose services require access to eHealth Ontario Sensitive Information, physical sites, Information Assets or Information Systems (including remote access).

This Policy replaces the *Privacy and Security Standard of Conduct for Service Providers*.

3 eHealth Ontario Internal Policies

3.1 Protecting the privacy and security of Sensitive Information in every aspect of our business is one of eHealth Ontario's core values. eHealth Ontario Personnel and Service Providers have a duty to care for and to protect Sensitive Information.

3.2 The minimum policy requirements for handling Sensitive Information are identified in this Standard.

3.3 The responsibilities of Personnel and Service Providers with respect to ensuring compliance with FIPPA, PHIPA and eHealth Ontario policies related thereto are outlined in greater detail in the *eHealth Ontario Privacy and Security Fundamentals Online Training*.

3.4 eHealth Ontario Personnel and Service Providers are required to follow the rules related to privacy and security as described in eHealth Ontario's policies, as updated from time to time. (Please see Appendix "A" for a full listing).

4 Acknowledgement and Agreement

Privacy and Security Acknowledgement and Agreement

4.1 The *eHealth Ontario Privacy and Security Acknowledgement and Agreement* ("Acknowledgement and Agreement") documents the obligations of Personnel and Service Providers to comply with the privacy and security requirements identified in this Standard.

4.2 Acceptance of the Acknowledgement and Agreement, will constitute an acknowledgement that Personnel and Service Providers:

- Have read, understood, and pledge to comply with all the requirements of this Standard;
- Agree to abide by the Agency's legislative requirements (see Section 6) and its internal policies;
- Are aware of the consequences of breaching the requirements set out in this Standard and the policies it supports; and
- Will complete the privacy and security training courses as required by eHealth Ontario.

4.3 All eHealth Ontario Personnel must accept the Acknowledgement and Agreement prior to starting work at eHealth Ontario, and annually thereafter.

4.4 Individuals contracted by eHealth Ontario through Service Providers to support the delivery of its operations and services must acknowledge and agree to abide by the terms of this Standard by signing the Acknowledgement and Agreement prior to providing services to eHealth Ontario. The Agency recognizes that some individuals contracted through Service Providers may not have permission from their employers/agencies to enter into agreements directly with the Agency. In such instances, individuals may sign an agreement with their own employer/agency acknowledging that they have read and understand eHealth Ontario's privacy and security requirements and will abide by them.

4.5 Further, where individuals contracted through Service Providers have entered into a substantially similar agreement with their own employer/agency, and their organization maintains comparable privacy and security policies, standards and practices, eHealth Ontario will accept a copy of that substantially similar agreement in lieu of the Acknowledgement and Agreement. In addition, the Service Provider with whom the individual is affiliated will agree to abide by the Agency's applicable privacy and security requirements on their employees' or affiliates' behalf as part of the terms of their contract with eHealth Ontario. eHealth Ontario may request proof that any Service Provider with whom it contracts maintains substantially similar privacy and security policies, practices and expectations within their own organization.

4.6 Service Providers have the obligation to familiarize themselves with any terms and conditions specified in their contract with eHealth Ontario relating to their management of Sensitive Information.

4.7 Personnel found to be in violation of the Standard may be subject to disciplinary action including termination of employment and legal action.

4.8 Service Providers found to be in violation of the Standard or the terms of their contract with eHealth Ontario may be subject to disciplinary action including termination of their contract with the Agency and legal action.

5 Responsibilities

Personnel and Service Providers

5.1 All Personnel and Service Providers working with access to Sensitive Information related to eHealth Ontario, both on and off eHealth Ontario premises, must be aware of the requirements of this Standard, and agree to comply by accepting the Acknowledgement and Agreement.

Managers

5.2 A "Manager" is a person whose employment responsibilities include supervising and/or directing, human or other resources. At eHealth Ontario, a Manager may be the Chief Executive or other Officers, Senior Vice Presidents, Vice Presidents, Senior Directors, Directors, Managers, Supervisors, program leads, project managers or Personnel who carry out managerial duties.

5.3 eHealth Ontario Managers must ensure that all Personnel under their supervision comply with this Standard and, in consultation with Human Resources, take disciplinary action, as appropriate, when deviations from expected practices and behaviours occur. Managers must take preventive and corrective action in cases of non-compliance with this Standard, even if no privacy or security incident has occurred.

Vice President, Human Resources, Strategic Sourcing and Vendor Management (VP, HR SSVM)

5.4 The VP, HR, SSVM must ensure that all new Personnel receive a copy of this Standard and sign an Acknowledgement and Agreement, prior to, or on the first day of employment. The signed Acknowledgement and Agreement shall be filed in the employee's HR file and must be made available for internal or external audits.

5.5 The VP, HR, SSVM must ensure that all eHealth Ontario Service Providers whose services require access to eHealth Ontario Sensitive Information, physical sites, information assets or information systems (including remote access) receive a copy of this Standard and sign an Acknowledgement and Agreement , prior to, or on the first day of service provision. The signed Acknowledgement and Agreement shall be filed along with the corresponding contract and must be made available for internal or external audits.

5.6 The VP, HR, SSVM shall ensure that any Service Providers who are required to complete the *eHealth Ontario Privacy and Security Fundamentals Online Training* do so as part of their orientation or onboarding process. The VP, HR, SSVM shall consult with the Chief Privacy Officer (CPO) and Chief Information Security Officer (CISO) (or their designates) should specific circumstances warrant consideration or modification of any of the requirements for Service Providers set out in this Standard.

General Counsel and Corporate Secretary

5.7 The General Counsel and Corporate Secretary shall advise the CPO and CISO when specific circumstances warrant consideration of additional modification of the terms of any written contract related to the requirements for Service Providers set out in this Standard.

Chief Privacy Officer and Chief Information Security Officer

5.8 This Standard is issued and approved under the authority of the CPO and CISO, in accordance with the requirements set in the *eHealth Ontario Privacy and Data Protection Policy* and the *eHealth Ontario Information Security Policy*. The CPO and CISO are accountable to ensure that the Standard content is kept up to date, is consistent with the business objectives of the Agency, and remains relevant for the day-to-day working conditions of all Agency Personnel and Service Providers.

Enterprise Service Desk (ESD)

5.9 ESD has the duties as assigned to it under this Policy.

6 Legislative Requirements

This section provides a brief overview of the legislative requirements relating to privacy and security of the Agency's Sensitive Information.

Ontario Regulation 43/02 made under the Ontario *Development Corporations Act* (DCA)

6.1 Regulation 43/02 accords eHealth Ontario the power to provide information management and technology services with the written approval of the Minister of Health and Long-Term Care. eHealth Ontario is permitted to collect, use, and disclose PI, and PHI, if necessary, in the course of providing these services, including in the course of performing maintenance or repairs. eHealth Ontario and its Personnel and Service Providers are prohibited from accessing PI and PHI for any other purpose when providing those services.

6.2 The DCA provides that the Agency may collect PI (as that term is defined in FIPPA) and use or disclose it in order to: (a) register persons to use the Agency's information infrastructure; (b) verify the identity of persons registering or registered to use the Agency's information infrastructure; and (c) maintain and administer the registration of such persons.

Personal Health Information Protection Act and Ontario Regulation 329/04 (PHIPA)

6.3 PHIPA is a provincial health privacy statute that establishes rules for the management of PHI and protection of the confidentiality of that information, while facilitating the effective delivery of healthcare services.

6.4 eHealth Ontario provides services to Ontario's health sector to support responsible and secure management of the PHI collected by health care providers, in accordance with PHIPA. PHIPA establishes rules for the collection, use, and disclosure of PHI.

Freedom of Information and Protection of Privacy Act (FIPPA)

6.5 FIPPA is a provincial statute that provides a right to access information under the control of institutions in accordance with the principles that information should be available to the public; necessary exemptions from the right of access should be limited and specific; and decisions on the disclosure of government information should be reviewed independently of government. FIPPA also protects the privacy of personal information of individuals held by institutions. It provides individuals with a right of access to, and correction of, that information.

6.6 eHealth Ontario is designated as an "Institution" under FIPPA. FIPPA protects the privacy of individuals with respect to their PI controlled or in the custody of eHealth Ontario and provides individuals with a right to access certain information. FIPPA requires that PI be appropriately collected, used and disclosed in accordance with the prescribed requirements.

7 Requirements When Accessing PI and PHI

7.1 When accessing PI and PHI, Personnel and Service Providers are responsible for adhering to the requirements set out in the eHealth Ontario Privacy and Data Protection Policy, and other relevant Privacy Policies as identified in "Appendix A". These requirements include, but are not limited to:

- Protecting PI and PHI
- Participating in Privacy and Security Training and Awareness

- Reporting Privacy and Security Incidents

Protecting PI and PHI

In the following sections 7 through 13, "you" refers to individual Personnel and to individuals contracted through Service Providers to the Agency.

7.2 When PI or PHI is in your care, you are responsible for ensuring it is maintained in a confidential and secure manner and is protected from theft, loss and unauthorized or inappropriate access, collection, use or disclosure, copying, modification, retention or disposal.

7.3 Your responsibilities for protecting PI and PHI include:

7.3.1 You must only use the limited PI or PHI to which you have been granted access and that is considered necessary in fulfilling the requirements of your position with eHealth Ontario. When in doubt about your authority to view PHI or PI, you must consult with your Manager.

7.3.2 You must limit the PI or PHI shared with authorized individuals to that which is strictly necessary.

7.3.3 You must only discuss PI or PHI in confidential and secure places with authorized individuals and only in the context of your job's responsibilities.

7.3.4 You must immediately report suspected privacy incidents, privacy breaches or security incidents to the Enterprise Service Desk (ESD) and your Manager.

8 Information Security Requirements

8.1 Information Security is concerned with managing risks and limiting harm related to potential or actual compromise of the confidentiality, integrity, or availability of information and systems. eHealth Ontario is committed to ensuring the proper security safeguards are in place in order to respect privacy and the protection of PI and PHI of Ontarians, as well as other Sensitive Information.

8.2 eHealth Ontario bases its information security program on the Information Security Policy and supporting Information Security Standards, as set out Appendix "A".

8.2.1 All Personnel and Service Providers must adhere to the requirements set out in the Information Security Policy, and other relevant policies and standards as set out in Appendix "A".

9 Corporate Information and Information Technology Requirements

9.1 All Personnel and Service Providers are responsible for adhering to the requirements set out in the *Corporate Information and Information Technology (I&IT) Resources Acceptable Use Policy*. These requirements include, but are not limited to:

- Handling Sensitive Information
- Protecting your computer
- Handling mobile devices, including your laptop and computer
- Network access
- Wireless access
- Anti-virus and software patches
- Internet and e-mail use

Handling Sensitive Information

9.2 You may e-mail Sensitive Information internally to colleagues if required. You are expected to keep confidential any Sensitive Information acquired in the course of your employment/engagement with eHealth Ontario and shall not directly or indirectly disclose this information to any person, association of persons, corporation or government without the prior written consent of the Agency, both during and after termination of employment/engagement with the Agency.

9.3 In the course of necessary business activities, you must not:

- E-mail Sensitive Information externally, either in the body of the e-mail, or as an attachment, unless it is encrypted to meet or exceed the Agency's cryptography standard, or is password protected. If you require assistance in applying the required security through encryption or password protection, contact ESD;
- Forward Sensitive Information to a non-eHealth Ontario e-mail address;
- Take PHI or PI off-site;
- Take Sensitive Information (other than PHI or PI) off-site unless there is no other less risky method of accessing it and with the permission of your Manager. If you are granted permission to take Sensitive Information (other than PHI or PI) off-site, you must restrict the information to the minimum that is necessary to complete the task. Sensitive information (other than PHI or PI) that is transported off-site, must be locked in a briefcase or in the trunk of your car;
- Disclose or share Sensitive Information with unauthorized individuals.

9.4 When printing documents at home, you must ensure that they are protected in same manner as in the office environment and disposed of using a cross-cut shredder. eHealth Ontario documents should never be placed in garbage or recycling bins.

9.5 When sending information by facsimile, you must always verify that the recipient's number is correct before sending and confirm receipt immediately afterward with the intended recipient by phone or email. eHealth Ontario policy requires that records of disclosures of Sensitive Information be maintained, such as facsimile transmission reports.

Protecting Your Computer

9.6 eHealth Ontario issued computers are configured with software and features that increase the security of the data accessed and stored when using these computers. You are responsible for supporting this commitment to computer security by adopting the following behaviours:

9.6.1 Computers and the information stored on them are important assets that you must protect from loss, damage, theft, or unauthorized access. You are responsible for the security of your computer at all times. Computers must be locked to a desk using a security cable during working hours, and stored in a locked desk drawer during non-working hours. Individuals who occupy 'private' office spaces may leave their laptops locked to their desk if they lock their door.

9.6.2 While working off-site, traveling between sites, or taking work home, you must never leave your laptop unattended. If traveling by car and making stops along the way is anticipated, the laptop should be placed in the trunk before departure, not at the destination. When using laptops in a public place, you must prevent over-the-shoulder access to the information on your screen by unauthorized persons.

9.6.3 Hard drives are encrypted with eHealth Ontario approved encryption software. You should call ESD immediately if you are not certain that the encryption software is actually installed or if it is suspected, for any reason, that the encryption has been compromised. This software requires a complex password that is different from the network password.

9.6.4 Most Personnel do not have administrative privileges to install any unauthorized software or hardware on their laptop. Any attempts to do so will be obstructed with error messages. You must not try to change your administrative privileges. Under special circumstances, some employees or contractors may be given administrative privileges for their laptops, which will allow the installation of additional software other than that originally requested for their computer. However, installing applications, software utilities, productivity tools, or device drivers that are not part of the standard suite still requires approval.

Back-ups and Records Management

9.7 The hard drive on laptop computers is not automatically backed up. Accordingly, all files must be stored on a network drive assigned to you. The network drive is backed up on a regular basis. You are responsible for the protection and backup of any files stored on a local computer drive.

9.8 When working from home, files should be stored on a network drive and connected from home to that drive using a secure access token. This ensures that files are always protected and backed up.

9.9 Files that represent final documents, and could be considered 'records' of the Agency (e.g. policies, procedures, reports, product specifications, brochures, and contracts) must be stored on a secure network folder or on the project, team or division SharePoint site. You should consult with your Manager or project manager to get directions on what documents should be stored on the secure network drive, or a SharePoint site.

Network and Wireless Access

9.10 The ESD will provide you with an initial network password. You must change the initial password immediately, and then change it on a regular basis when prompted.

9.11 Remote network access requires strong authentication using a security token. Where you have been approved to work remotely, you will be provided with a security token. If this security token is lost or damaged, it must be immediately reported to ESD.

9.12 An eHealth Ontario issued laptop may be used at home, with a wireless router or modem, providing that the following conditions are met:

- A secure remote connection to the eHealth Ontario network (Check Point VPN) is established using the eHealth Ontario-issued RSA token;
- The appropriate updates have been made by eHealth Ontario;
- A personal firewall appliance is installed between the laptop and internet access, or you have a wireless router with a built in firewall; and
- The Internet Explorer browser is started only after the VPN connection is successfully established.

Note: ESD or EUC (End User Computing) does not provide any support for technical or security issues resulting from use of wireless communications not provided by eHealth Ontario. Users are personally responsible for the security of their computers while using wireless communication. eHealth Ontario does not promote the use of wireless networks at public Wi-Fi hotspots or at Internet cafes. For greater certainty, notwithstanding the foregoing, you are required to report any security incidents arising out of the use of wireless communications not provided by eHealth Ontario.

9.13 Non-eHealth Ontario-issued laptop or desktop computers, such as personal computers or contractors' computers, must not be connected to the eHealth Ontario secure network, at any location, without requesting approval through Remedy. This ensures that any equipment connected to eHealth Ontario networks meets the minimum security standards needed to protect the confidentiality, integrity, and availability of the networks and of the information used by, or on behalf of, eHealth Ontario.

Software Updates

9.14 eHealth Ontario will install software to computers or laptops as required. All software on these computers is updated regularly and automatically. You must not attempt to bypass, modify or install additional software.

9.15 You will be notified about periodic updates to your software performed by ESD or EUC. You may need to restart your computer after the updates are downloaded and installed. If problems occur during any software applications and you get a pop-up request to report the problem directly to the software manufacturer, decline the offer and select "Do not report" option.

Email Use

9.16 eHealth Ontario owns all e-mail transmissions using eHealth Information assets and reserves the right to monitor, block, access, and review electronic messages. E-mail may be subject to public disclosure in accordance with applicable legislation. You are expected to follow the requirements in the *Corporate I&IT Policy* pertaining to internet and email use.

Handling Mobile Devices

9.17 Mobile Devices include any smartphone, tablet, or cell phone that is running on eHealth Ontario supported platforms including but not limited to Blackberry 10, iOS, Android using a cellular and/or Wi-Fi connection.

9.18 If your job requires regular mobile communications, you will receive a mobile phone from eHealth Ontario. This device can be used securely for communications. You must enable and use the password protection feature at all times. You are responsible for the physical security of this device at all times. If your eHealth Ontario issued mobile phone is lost or damaged, you must immediately report this to ESD at 416-586-4373 or 1-866-250-1554. You should avoid using your personal cell phone for business related communications.

9.19 Cameras of any type must not be used to take pictures of eHealth Ontario sensitive areas, such as data centers or secured floors in downtown facilities, or confidential information on any type of media, unless approved by the Director, Information Security Services.

9.20 You may use USB memory sticks to share information with colleagues or for short term backups, providing that the device is used only among eHealth Ontario computers, and that the USB is an approved and encrypted device issued from ESD. For longer term backups, use the network drive assigned to you on the eHealth Ontario network. Due to the risk of virus infections, the USB memory sticks, including those issued by eHealth Ontario, must not be used (shared) between personal (home) and eHealth Ontario computers.

9.21 You must not transfer Sensitive Information to your Mobile Device without express authorization.

9.22 No person issued an eHealth Ontario laptop is permitted to take it outside of Canada. Should you find it necessary to bring a laptop for eHealth Ontario business purposes on international trips, you must request access to a "clean" laptop that is configured for this purpose from ESD. These laptops will be fitted with eHealth Ontario's standard applications, including appropriate encryption software. You must provide a minimum of two weeks' notice of your intention to travel outside of Canada to EIS to ensure a laptop is available and properly configured for your purposes.

Upon Exiting eHealth Ontario

9.23 When you leave your job at eHealth Ontario, or you end your engagement, you must return the computer and all other IT devices you received. You must not take with you any type of Sensitive Information related to eHealth Ontario in general or the output/products of your work and that of others. All data, records, and information, stored on any media (e.g. paper, CDs, DVDs, tapes, removable hard drives, and USB memory devices) that belong to eHealth Ontario, must be fully accounted for and returned to eHealth Ontario through your responsible Manager.

10 Access Control Requirements

10.1 All eHealth Ontario Personnel and Service Providers are responsible for adhering to the requirements set out in the *Access Control Standard*.

10.2 Use a strong password as the first line of defense against unauthorized access. If you suspect that either your encryption or your network password has been compromised, change it immediately and inform ESD. ESD can also help you reset you network password or recover your data if you forget the encryption password. Follow the requirements for creating a strong password as set out in the *Access Control Standard*.

11 Physical Security Requirements

11.1 All eHealth Ontario Sensitive Information must be secured at all times. eHealth Ontario has adopted a "Clean Desk Policy" in order to guard against unauthorized access to information. This requires that you:

- Not leave materials unattended on your desk or in any other open, unsecured area, such as near printers, copy machines, facsimile machines, or meeting rooms.
- Every time you leave your desk and your laptop is on, use the screen lock functionality.
- Before you leave the office, ensure all confidential materials are secured. Ensure all lockable cabinets and drawers are locked when unattended.
- Place all materials into a locked secure-shred bin or shred them in order to dispose of them. Do not place them in a blue recycling bin or the garbage; and
- After you have finished using a meeting room, remove all materials from the table(s), whiteboard(s), flipchart(s), and ensure that conference calls are terminated.

11.2 eHealth Ontario is committed to implementing physical safeguards which prevent unauthorized access to eHealth Ontario sites. Physical access to eHealth Ontario locations is controlled in the following ways:

11.2.1 In all buildings:

- You must wear your access card visibly on site at all times to identify yourself as an employee (identification badge) or contractor (green window card). You must remove your access card as soon as you leave eHealth Ontario facilities and safeguard it appropriately.
- Do not lend your access card to colleagues or visitors under any circumstances.
- Do not allow others to follow you into eHealth Ontario premises when you open the door for yourself.
- If you lose your access card, immediately contact ESD.

11.2.2 Data Centres

- In addition to the physical security measures listed for all locations, enhanced measures (such as biometric fingerprinting), are in place at data centre locations. All personnel, service providers and visitors must comply with the access requirements to enter either of these locations.
- Once inside, no pictures are allowed with any cameras (regular cameras or cell-phone based cameras).

11.2.3 Visitors

- eHealth Ontario Personnel or Service Providers must ensure that visitors sign in at reception at either the 7th floor of 777 Bay Street, the 2nd floor of 655 Bay Street or the 19th floor of 415 Yonge Street and wear access badges at all times while on eHealth Ontario premises.
- While visitors are on site, eHealth Ontario Personnel must escort them at all times on our premises, including meeting rooms, office space, labs and IT operations areas
- If you see a visitor without a badge, politely approach him or her and redirect them to the Reception Desk. Contact the Operations Security Officer for further assistance if required, and inform the ESD.

12 Training and Awareness

12.1 All eHealth Ontario Personnel are required to complete the mandatory eHealth Ontario Privacy and Security Fundamentals training within 30 days of starting work and annually thereafter. Additional role-based privacy and security training is required for Personnel with access to PI or PHI prior to being granted access.

12.2 eHealth Ontario Service Providers must complete the eHealth Ontario Privacy and Security Fundamentals and role-based privacy and security training, or equivalent, where there is access to PI or PHI prior to being granted access, as directed to do so by eHealth Ontario.

13 Privacy Incidents, Privacy Breaches and Security Incidents

13.1 Incidents and breaches may be accidental or deliberate. Privacy incidents and breaches occur when there is an actual or potential unauthorized or illegal access to, use, collection, disclosure, retention, modification or destruction of PI or PHI. Privacy incidents and breaches can be intentional or inadvertent.

13.2 eHealth Ontario has established the *Privacy Breach Management (PBM) Program* for responding to privacy incidents and breaches and the *Security Incident Response (SIR) Program* for responding to security incidents.

13.3 If you suspect that the privacy, confidentiality, integrity or availability of Sensitive Information has been compromised, you must report the incident to ESD at 416-586-4373 or 1-866-250-1554 at the first reasonable opportunity.

13.4 eHealth Ontario extends "whistleblower" protection to any eHealth Ontario Personnel or Supplier who discloses a "wrongdoing" which may include an actual or potential breach of privacy or security (refer to the *eHealth Ontario Disclosure of Wrongdoing Policy*). As the individual reporting the breach, you may be required to provide details to the investigators and to assist in the investigation and reporting.

Glossary

The following definitions are associated with this Standard:

TERM	DEFINITION
Personal Information (PI)	"Personal Information" means recorded information about an identifiable individual, including, a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual, b) information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved, c) any identifying number, symbol or other particular assigned to the individual, d) the address, telephone number, fingerprints or blood type of the individual, e) the personal opinions or views of the individual except where they relate to another individual, f) correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence, g) the views or opinions of another individual about the individual, and h) the individual's name where it appears with other Personal Information relating to the individual or where the disclosure of the name would reveal other Personal Information about the individual.
Personal Health Information (PHI)	Has the meaning set out in section 4 of the *Personal Health Information Protection Act, 2004* (PHIPA), and generally means identifying information about an individual in oral or recorded form pertaining to that person's health or health services provided to the individual.
Privacy Incident	A privacy incident includes: • A contravention of the privacy policies, procedures or practices implemented by eHealth Ontario, where this contravention does not result in unauthorized collection, use, disclosure and destruction of PI/PHI or does not result in non-compliance with applicable privacy law. • A contravention of agreements which eHealth Ontario enters into with external stakeholders and third party service providers, including but not limited to PHIPA agent agreements, data sharing agreements, confidentiality and non-disclosure agreements and agreements with third party service providers retained by eHealth Ontario, where this contravention does not constitute non-compliance with applicable privacy law.

Privacy Breach	A privacy breach includes: • The collection, use or disclosure of PHI that is not in compliance with the PHIPA and its regulation. • The collection, use or disclosure of PI that is not in compliance with the FIPPA and its regulations. • Circumstances where PI/PHI is stolen lost or subject to unauthorized or inappropriate collection, use or disclosure, copying, modification, retention or disposal.
Security Incident	A security incident includes any activity that could compromise the security of information or systems, including but not limited to, a social engineering attempt such as an unauthorized request for a password, loss of a laptop, computer or mobile device, a computer virus infection, degradation of a system, unauthorized changes to files or file sizes, or the addition of files. • The collection, use or disclosure of PHI that is not in compliance with the PHIPA and its regulation. • The collection, use or disclosure of PI that is not in compliance with the FIPPA and its regulations. • Circumstances where PI/PHI is stolen lost or subject to unauthorized or inappropriate collection, use or disclosure, copying, modification, retention or disposal. In the context of this document and in alignment with IT information library (ITIL) an information security breach is a type of information security incident
Sensitive Information	Information that if released without authorization would cause harm, embarrassment, or unfair economic advantage, such as a breach of confidentiality of PHI or PI, unauthorized modification of financial data, or a release of pre-budget documentation or strategic planning documents.

Table 1: Privacy and Security Standard of Conduct: Glossary

APPENDIX A - Relevant Documents

The following are legislative references and eHealth Ontario policies associated with this Standard of Conduct:

REFERENCE	LOCATION
Freedom of Information and Protection of Privacy Act (FIPPA) and regulations	http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_90f31_e.htm
Personal Health Information Protection Act, 2004 (PHIPA) and regulations	http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_04p03_e.htm
Privacy and Data Protection Policy	www.ehealthontario.on.ca/privacy
Personal Information Privacy Policy	www.ehealthontario.on.ca/privacy
Personal Health Information Privacy Policy	www.ehealthontario.on.ca/privacy
Privacy Incidents and Breach Management Policy	www.ehealthontario.on.ca/privacy
Privacy Policy on the Responsibilities of Third Party Service Providers	www.ehealthontario.on.ca/privacy
Information Security Policy	http://emerge/spaces/security
Access Control Standard	http://emerge/spaces/security
Corporate Information and Information Technology (I&IT) Resources Acceptable Use Policy	http://emerge/spaces/security
Information Classification and Handling Standard	http://emerge/spaces/security
Information Security Cryptography Standard	http://emerge/spaces/security
Information Security Communications and Network Security Standard	http://emerge/spaces/security
Information Security Software and Systems Security Standard	http://emerge/spaces/security
Information Security Screening Policy	http://emerge/spaces/security

Table 2: Privacy and Security Standard of Conduct: References and Associated Documents

APPENDIX B - Privacy and Security Acknowledgement and Agreement

Ontario
eHealth Ontario
cyberSanté Ontario

P.O. Box 148
777 Bay Street, Suite 701
Toronto ON M5G 2C8

Tel: (416) 586 - 6500
Fax: (416) 586 - 4363
Email: info@ehealthontario.on.ca
Website: www.ehealthontario.on.ca

C. P. 148
777, rue Bay, bureau 701
Toronto ON M5G 2C8

Tél: (416) 586 - 6500
Télé: (416) 586 - 4363
Courriel: info@ehealthontario.on.ca
Site Web: www.ehealthontario.on.ca

Privacy and Security Acknowledgement and Agreement

All eHealth Ontario Personnel, including contract employees must sign the eHealth Ontario ("eHealth Ontario" or "Agency") Privacy and Security Acknowledgement and Agreement prior to starting work at the Agency.

In consideration of your working at eHealth Ontario, you:

(i) Acknowledge that eHealth Ontario must comply with *Freedom of Information and Protection of Privacy Act* (FIPPA), *Personal Health Information Protection Act* (PHIPA), and associated regulations, as amended from time to time and with the terms of this *Privacy and Security Acknowledgement and Agreement*;
(ii) Acknowledge receipt of this *Privacy and Security Standard of Conduct* (the "Standard");
(iii) Acknowledge that your work-related conduct is governed by all eHealth Ontario policies and this Standard;
(iv) Acknowledge and agree that eHealth Ontario policies and this Standard form part of your terms of employment or your contract, and that you will comply with its requirements;
(v) Acknowledge that you are prohibited from collecting, using or disclosing personal health information in the course of your employment if de-identified information will serve the purpose and from collecting, using or disclosing more Personal Health Information than is reasonably necessary to meet the purpose.
(vi) Will securely return all property of eHealth Ontario, including all identification cards, access cards and/or keys on or before the date of termination of employment, contractual or other relationship.
(vii) Acknowledge and agree that you will immediately notify the Chief Privacy Officer and Chief Security Officer, representing eHealth Ontario, in the event you become aware of or suspect a violation of FIPPA, PHIPA, eHealth Ontario's *Privacy and Data Protection Policy*, *Information Security Policy* and other eHealth Ontario information management policies, as amended from time to time;
(viii) Acknowledge and agree that you will immediately notify the Chief Privacy Officer and Chief Security Officer, representing eHealth Ontario, in the event that you access, use, disclose or dispose of Personal Information or Personal Health Information, other than in accordance with FIPPA, PHIPA, eHealth Ontario's *Privacy and Data Protection Policy*, *Information Security Policy* and other eHealth Ontario privacy and security policies, as amended from time to time, or if an unauthorized person accesses Personal Information or Personal Health Information;
(ix) Acknowledge and agree that violation of eHealth Ontario policies, this Standard or this Acknowledgement and Agreement may result in disciplinary action, up to and including termination of employment or contract; and
(x) Complete privacy and security online training within the first 30 days of your employment, and to refresh such training at least annually.

For the purposes of this Acknowledgement and Agreement, "Personal Health Information" has the same meaning as Personal Health Information defined in section 4 of the *Personal Health Information Protection Act*, and "Personal Information" has the same meaning as defined in section 2 of the *Freedom of Information and Protection of Privacy Act*. (See the *eHealth Ontario Privacy and Security Employee Standard of Conduct* for a full definition of Personal Information and Personal Health Information.)

_____ _____

Signature Date

_____

Print Name

Please sign and return this page to:
Your manager or their designate

Ontario
eHealth Ontario
cyberSanté Ontario

P.O. Box 148
777 Bay Street, Suite 701
Toronto ON M5G 2C8

Tel: (416) 586 - 6500
Fax: (416) 586 - 4363
Email: info@ehealthontario.on.ca
Website: www.ehealthontario.on.ca

C. P. 148
777, rue Bay, bureau 701
Toronto ON M5G 2C8

Tél: (416) 586 - 6500
Télé: (416) 586 - 4363
Courriel: info@ehealthontario.on.ca
Site Web: www.ehealthontario.on.ca

Privacy and Security Acknowledgement and Agreement

All eHealth Ontario Service Providers must sign the eHealth Ontario ("eHealth Ontario" or "Agency") Privacy and Security Acknowledgement and Agreement prior to starting work at the Agency. An individual may fulfill this requirement by signing this form and returning it to the Agency's Procurement Office, or alternately, the individual may enter into a substantially similar agreement with their employer and provide documentary evidence of same. All service providers agree to abide by the requirements set out in the Standard and related policies as part of the terms of their written agreements with eHealth Ontario. The Agency reserves the right to request copies of substantially similar policies, practices and standards maintained by the service provider's organization.

In consideration of your service provision to eHealth Ontario, you:

(i) Acknowledge that eHealth Ontario must comply with *Freedom of Information and Protection of Privacy Act* (FIPPA), *Personal Health Information Protection Act* (PHIPA), and associated regulations, as amended from time to time and with the terms of this *Privacy and Security Acknowledgement and Agreement*;
(ii) Acknowledge receipt of this *Privacy and Security Standard of Conduct* (the "Standard");
(iii) Acknowledge that your work-related conduct is governed by all eHealth Ontario policies and this Standard;
(iv) Acknowledge and agree that eHealth Ontario policies and this Standard form part of your contract, and that you will comply with its requirements;
(v) You acknowledge that you are prohibited from collecting, using or disclosing Personal Health Information in the course of your contract if de-identified information will serve the purpose and from collecting, using or disclosing more Personal Health Information than is reasonably necessary to meet the purpose.
(vi) You will securely return all property of eHealth Ontario, including all identification cards, access cards and/or keys on or before the date of termination of contract or other relationship.
(vii) Acknowledge and agree that you will immediately notify the Chief Privacy Officer and Chief Security Officer, representing eHealth Ontario, in the event you become aware of or suspect a violation of FIPPA, PHIPA, eHealth Ontario's *Privacy and Data Protection Policy*, *Information Security Policy* and other eHealth Ontario information management policies, as amended from time to time;
(viii) Acknowledge and agree that you will immediately notify the Chief Privacy Officer and Chief Security Officer, representing eHealth Ontario, in the event you access, use, disclose or dispose of Personal Information or Personal Health Information, other than in accordance with PHIPA, FIPPA, eHealth Ontario's *Privacy and Data Protection Policy*, *Information Security Policy* and other eHealth Ontario privacy and security policies, as amended from time to time, or if an unauthorized person accesses Personal Information or Personal Health Information;
(ix) Acknowledge and agree that violation of eHealth Ontario policies, this Standard or this Acknowledgement and Agreement may result in disciplinary action, up to and including termination of contract; and
(x) Complete privacy and security online training when directed to do so by eHealth Ontario.

For the purposes of this Acknowledgement and Agreement, "Personal Health Information" has the same meaning as Personal Health Information defined in section 4 of the *Personal Health Information Protection Act*, and "Personal Information" has the same meaning as defined in section 2 of the *Freedom of Information and Protection of Privacy Act*. (See the *eHealth Ontario Privacy and Security Standard of Conduct* for a full definition of Personal Information and Personal Health Information.)

_____ _____

Signature Date

_____

Print Name

Please sign and return this page to:
Strategic Sourcing and Vendor Management