

eHealth Ontario Privacy and Security Employee Standard of Conduct

Document Identifier: 00990

Version: 2.0

Owner: Chief Privacy and Security Officer

Document Control

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

Document Location:

Review Frequency: This document must be reviewed on an annual basis. Updates may be required more often if significant changes occur in eHealth Ontario business conditions.

Document Prime* Marc Stefaniu
Senior Information Security Consultant
Angelique Hamilton
Senior Privacy Analyst

*Enquiries relating to this document should be referred to the responsible Document Prime.

Approval History

Title	Approved Date
Chief Privacy and Security Officer	2008-10-24

Revision History

Version No.	Version Date	Summary of Change	Changed By
2	2009-02-19	Minor revisions	Angelique Hamilton
2	2008-09-25	Additional revisions	Angelique Hamilton
2.0	2008-07-31	Updates on Privacy related sections and revisions	Angelique Hamilton
2.0	2008-07-29	Updates on Security related sections	Marc Stefaniu
1.1	2008-04-03	New HR contact information for Ack form	Marc Stefaniu
1.0	2007-05-17	Initial Draft	Marc Stefaniu

1 Purpose

The eHealth Ontario Privacy and Security Employee Standard of Conduct (“the Standard”) supports the Agency’s commitment to Privacy and Security by establishing clear behavioural expectations for individuals who utilize eHealth Ontario assets or handle eHealth Ontario information, including Personal Information (“PI”) and Personal Health Information (“PHI”). This Standard helps foster in each individual at eHealth Ontario:

- An understanding of privacy and security at eHealth Ontario, including the Agency’s legislative and policy requirements; and
- A practical understanding of the Agency’s expectations of individuals who, in the course of their work at eHealth Ontario, must protect the privacy and security of the information they create, use, access, disclose or otherwise manage.

2 Scope of Application

The responsibilities described in this Standard apply to all eHealth Ontario personnel, including executives, full time and part-time employees and contract employees who work for the Agency. Third parties who provide services to the Agency, such as vendors and consultants, are subject to the eHealth Ontario Privacy and Security Standard of Conduct for Third Parties, and are not within the scope of application of this standard.

3 Responsibilities

Employees and contract employees. All personnel working with eHealth Ontario information, both on and off eHealth Ontario premises, must be aware of, and comply with the requirements of the Standard, and must sign the Privacy and Security Acknowledgement and Agreement. The signed Acknowledgement and Agreement indicates that employees have read and understood their responsibilities, and agree to comply with the requirements and behaviours described in the Standard. This Agreement must be signed prior to start of work with the Agency, and annually thereafter.

Director, Human Resources. The Director, Human Resources (HR) must ensure that all new full time, part-time and contract employees receive a copy of the Standard and sign an Acknowledgement and Agreement form, prior to, or on the first day of employment. The signed Acknowledgement and Agreement shall be filed in the employees’ HR files and must be made available for internal or external audits.

Executives, directors, and managers. “People Managers” must ensure that all personnel under their supervision have read, signed and comply with the Standard, and take disciplinary action, as appropriate, when deviations from expected practices and behaviours occur. People managers must take preventive and corrective action in cases of non-compliance with the Standard, even if no privacy or security incident has occurred.

Chief Privacy and Security Officer. This Standard is issued and approved under the authority of the Chief Privacy and Security Officer, in accordance with the requirements set in the eHealth Ontario Privacy and Data Protection Policy and the Enterprise Information Security Policy.

Director, Privacy and Director, Information Security. The Directors of Privacy and Security must ensure that the Standard content is maintained and 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 eHealth Ontario personnel.

Anyone found in violation of the Privacy and Security Standard of Conduct may be subject to disciplinary action up to and including termination of employment or contract.

4 Elements of the Standard

Protecting privacy and security of Personal Information (PI) and Personal Health Information (PHI) in every aspect of our business is one of eHealth Ontario's core values. All eHealth Ontario Personnel have a duty to care for and to protect both client and internal information.

This Standard identifies:

- eHealth Ontario's legal and policy requirements relating to privacy and security;
- Your responsibilities to protect the privacy and confidentiality of the information you handle in your daily activities at eHealth Ontario; and
- Ways you must ensure that information in your care is protected.

4.1 Legal Requirements

Ontario Regulation 339/08 made under the Development Corporations Act

This is the Agency's enabling regulation. It 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. In connection with these services, eHealth Ontario is permitted to collect, use, disclose and access Personal Information, including Personal Health Information, if necessary in the course of providing services, including in the course of performing maintenance or repairs. eHealth Ontario and its personnel are prohibited from accessing Personal Information for any other purpose when providing those services.

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

eHealth Ontario provides services to Ontario's health sector to support responsible and secure management of the Personal Health Information collected by health care providers, in accordance with PHIPA. PHIPA establishes rules for the collection, use, and disclosure of Personal Health Information. Section 10(4) of PHIPA and, subsections 6(1), (2), and (3) of the Regulation made under it establish requirements for a person providing goods or services for the purpose of enabling Health Information Custodians (HICs) to use electronic means to collect, use, modify, disclose, retain, or dispose of Personal Health Information.

Freedom of Information and Protection of Privacy Act (FIPPA)

eHealth Ontario is designated as an "Institution" under FIPPA. FIPPA protects the privacy of individuals with respect to their Personal Information controlled or in the custody of provincial government Institutions, including that controlled by eHealth Ontario for its own purposes. It requires that Personal Information be appropriately collected, used and disclosed.

eHealth Ontario Internal Policies

In addition to the statutory obligations, eHealth Ontario staff are required to follow the rules related to privacy and security as described in eHealth Ontario's privacy and security policies, including the eHealth Ontario Privacy and Data Protection Policy and the eHealth Ontario Enterprise Information Security Policy, as updated from time to time.

Your responsibilities with respect to ensuring compliance with FIPPA, PHIPA and eHealth Ontario policies are outlined in greater detail in the Privacy and Security Fundamentals Training.

4.2 What is Privacy?

Privacy is the right of the individual to control the collection, use and or disclosure of his or her Personal Information or Personal Health Information. eHealth Ontario is committed to

respecting privacy and protecting Personal Information and Personal Health Information of Ontarians.

Personal Information. “Personal Information” or “PI” means identifying information about an individual including: name, address, sex, age, education, or employment history, and any other individually identifying information, including IP addresses which may be linked to an individual.

Personal Health Information. “Personal Health Information” or “PHI” generally means identifying information about an individual in oral or recorded form, if the information relates to the physical or mental health of the individual. Examples include: family health history, health card number, any information that identifies an individual and links them to a health care provider.

4.3 What is Information Security?

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 structures are in place in order to respect privacy and the protection of Personal Information and Personal Health Information of Ontarians.

Within the eHealth Ontario environment:

Confidentiality means information is available or disclosed only to authorized individuals, entities, or IT processes. Examples of threats against confidentiality include (but are not limited to): unauthorized access to information, eavesdropping, social engineering, and unsecured disposal of printed documents.

Integrity means information is valid (authentic, consistent, unmodified) and can be relied upon to remain valid over time.

Availability means that the property of assets and services ensures they can be accessed without undue delay and used as required by authorized users. Examples of threats against availability of information include (but are not limited to): stolen computers, system crashes, viruses, and worms.

4.3.1 Security Standards

eHealth Ontario bases its information security program on the Information Security Policy, the Enterprise Security, and Privacy Incident Management Program as well as the following international standards:

- ISO/IEC 27002:2005, Information Technology – Security Techniques – Code of Practice for Information Security Management
- ISO/IEC 27001:2005, Information Technology – Security Techniques – Information Security Management Systems – Requirements.

4.4 Privacy and Security Responsibilities

4.4.1 Acknowledgement and Agreement

All eHealth Ontario Personnel and contract employees must sign the eHealth Ontario “Privacy and Security Acknowledgement and Agreement” prior to starting work at eHealth Ontario, and annually thereafter. In signing this form, you acknowledge that you:

- Have read, understood, and pledge to comply with all the requirements of this Standard;
- Agree to abide by the legal requirements and internal policies that govern eHealth Ontario;
- Are aware of the consequences of breaching the requirements set in this Standard and the policies it supports; and
- Will complete the Privacy and Security online training courses within 30 days of starting work at eHealth Ontario, and annually thereafter.

4.4.2 Protecting Personal Information and Personal Health Information

When Personal Information or Personal Health Information is in your care, you are responsible for ensuring it is maintained in a confidential and secure manner and is protected from unauthorized use or disclosure.

You **must**:

- Collect, use and disclose Personal Information and Personal Health Information only as directed by eHealth Ontario.
- Only use the limited Personal Health Information and Personal Information to which you have access as necessary in fulfilling the requirements of your position with eHealth Ontario.
- Immediately report any suspected privacy or security incident to Enterprise Service Desk (ESD) and your manager.

You **must not**:

- Access Personal Health Information unless you are expressly authorized to do so.
- Disclose Personal Health Information to which you have access.
- Discuss Personal Information or Personal Health Information in public places.
- When in doubt about your authority to handle Personal Health Information or Personal Information, speak with your manager; ask questions.

4.4.3 Clean Desk Policy

All eHealth Ontario 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:

- Do 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: press ‘Ctrl – Alt – Delete’ and click ‘Lock Computer’.
- 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 Eco-Shred bin or shred them in order to dispose of them. Do not place them in a blue recycling bin or the garbage.
- 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.

4.4.4 Handling Confidential Materials

eHealth Ontario Personnel are expected to keep confidential any data or information acquired in the course of employment 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 with the Agency.

- You may e-mail confidential information internally to colleagues if required to do so in the course of necessary business activities.

However, you **must not**:

- E-mail confidential information externally, neither in the body of the e-mail, nor as an attachment, unless it is encrypted or password protected. Should you require assistance in applying the required security through encryption or password protection, contact ESD.
- Forward confidential materials to a non-eHealth Ontario personal e-mail address;
- Take confidential eHealth Ontario materials off-site unless there is no other less risky method of accessing it available to you and you have the permission of your manager. If you are permitted to take confidential or Personal Information off-site, you must restrict the information to the minimum necessary to complete the task; When transporting eHealth Ontario information off-site, ensure it is locked in a briefcase or in the trunk of your car;
- Take any Personal Health Information off-site; or
- Disclose or share confidential materials or Personal Information, including Personal Health Information, with unauthorized individuals.

Further, 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 shredder. Never place eHealth Ontario documents in garbage or recycling bins.

In addition, when sending information by facsimile, you must always verify 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 you maintain records of disclosures of Personal Information, including Personal Health Information, such as facsimile transmission reports.

4.4.5 Access to eHealth Ontario Buildings

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:

All Buildings

- You must wear your access card visibly on site at all times to identify yourself as an employee (blue color card) or contractor (green color 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 the Operations Security Officer at 416-586-4215 and inform the ESD.

Markham Computer Center (MCC) and /Streetsville Computer Center (SCC)

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

Visitors

- eHealth Ontario personnel must ensure that visitors sign in at reception at either the 7th floor of 777 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 staff 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 at 416-586-4215 for further assistance if required, and inform the ESD.

4.4.6 Protecting Your Computer

Your eHealth Ontario issued computer has been configured with software and features which increase the security of the data accessed and stored using the Agency's computers. You are responsible for supporting that commitment to computer security by adopting the following behaviours:

Hardware

Your laptop computer and the information stored on it are important assets that you must protect from loss, damage, theft, or unauthorized access.

During working hours, your laptop must be locked to a desk using a security cable. If you store your laptop within eHealth Ontario facilities during non-working hours, you must secure your laptop in a locked desk drawer. Employees or contractors who occupy 'private' office spaces may leave their laptops locked to their desk if they lock their door.

You are responsible for the security of your laptop at all times. While working off-site, traveling between sites, or taking work home, you must never leave your laptop unattended. If you anticipate traveling by car and making stops along the way, place your laptop in the trunk before you leave, not at destination. If you use your laptop in a public place, you must prevent over-the-shoulder access to the information on your screen by unauthorized people.

Software

In order to enhance the protection of privacy and security of information on your laptop, your hard drive is encrypted with eHealth Ontario approved encryption software. Call ESD immediately if you are not sure if the encryption software is actually installed or if you suspect for any reason that the encryption has been compromised.

The encryption software requires a password that is different from the network password. You will be prompted to enter the encryption password as soon as you power up the laptop. You must choose a very strong password for the encryption software.

For the majority of employees the laptop is 'locked down'. This means that you do not have the administrative privileges to install any unauthorized software or hardware on your laptop. Any attempts you may make 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 your laptop. However, installing applications, software utilities, productivity tools, or device drivers that are not part of the standard suite still requires approval from your manager and from the Enterprise Information Systems (EIS). To request approval, start by calling the ESD. They will instruct you on the approval process.

Back-ups and Records Management

The hard drive on your laptop computer is not automatically backed up. Accordingly, store all files on a network drive assigned to you. The network drive is backed up on a regular basis. If you store files on your local computer drive, you are responsible to create backups at least once a week.

When working from home, you can copy any working files (or 'documents') to your local laptop drive (also known as the "C:" drive). When you return to the office, upload your latest versions of the files onto the network drives (check with ESD for the right name of the network drive for you). A preferred alternative is to always store the files on a network drive and connect from home to that drive using your secure access token. This ensures that your files are always protected and backed up.

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 network server called the 'I:' drive or on the documents on your project, team, or division SharePoint site. Talk to your manager or project manager to get directions on what documents should be stored on the "I:" drive, or a SharePoint site.

Upon Exit

When you leave your job at eHealth Ontario, you must return the laptop and all other IT devices you received. You must not take with you any type of confidential 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) belong to eHealth Ontario, and must be fully accounted for and returned to eHealth Ontario through your manager.

Taking eHealth Ontario Laptops Across International Borders

When crossing international borders, you must cooperate and comply with security requirements, including the potential request to turn on your laptop, or to provide your password to a border security officer. Therefore the following precautions must be taken to minimize the risk to eHealth Ontario data privacy and security:

Laptops. 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 EIS. These laptops will be

fitted with eHealth Ontario's standard applications, including Computrace and 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.

4.4.7 Network Access

An initial network password will be provided by the Enterprise Service Desk. You must change the initial password immediately, and then change it on a regular basis. You will get a reminder on your log-on screen seven days before you need to change the password.

Your manager may approve your working from home or from a remote office. Remote network access requires strong authentication using a security token. If you have been approved to work remotely, you will be provided with a security token. If your security token is lost or damaged, immediately report this to the Enterprise Service Desk (ESD) at 416-586-4ESD.

Non-eHealth Ontario-issued laptop or desktop computers, such as personal computers or contractors' computers, must not be connected to the eHealth Ontario network, at any location, without approval from the Director of Enterprise Information Services or the Director of Information Security. This is required in order to ensure 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.

Wireless Access

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

- The McAfee anti-virus software is at the most recently updated level issued by eHealth Ontario;
- All security patches are up-to-date;
- The Microsoft Windows Firewall is enabled;
- A personal firewall appliance is installed between the laptop and internet access, or you have a wireless router with a built in firewall;
- A secure remote connection to the eHealth Ontario network (Check Point VPN-1 SecureClient) is established using the eHealth Ontario-issued RSA token; and
- Internet Explorer browser is started only after the VPN connection is successfully established.

ESD does not provide any support for technical or security issues resulting from use of wireless communications. 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.

4.4.8 Passwords

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 forgot the encryption password.

Passwords must be at least eight characters in length, and contain characters from three of the following four categories: uppercase characters (A-Z); lowercase characters (a-z); numeric (0-9); or special characters (e.g. !, \$, #, _, ~, %, ^).

Passwords must be changed when prompted by the system. You must not reuse any of your previous six passwords.

Do not share your password with others and do not write it down. ESD personnel do not require and will not request that you disclose your password. Therefore, report to ESD any case when someone is asking to disclose your password.

In the event that you are away from the office for an extended period of time, an administrator can enable your manager to access your files.

Your telephone is equipped with a voice mailbox that is protected with a password. You must protect that password and change it when prompted by the system. Do not write it down.

4.4.9 Anti-Virus and Software Patches

Your computer comes with Agency approved anti-virus, anti-spyware and Computrace software. All software on your computer is updated periodically and automatically. You must not attempt to install additional anti-virus software or to request periodic updates of that software. The Enterprise Service Desk group will apply other application or security patches that affect privacy and security measures on a periodic basis. You will be notified by e-mail about these updates beforehand. You must leave your computer on at the indicated time. 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.

4.4.10 Internet and E-mail Use

eHealth Ontario owns all e-mail transmissions 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. The following are eHealth Ontario’s expectations of its personnel as it pertains to Internet and E-mail use:

- Do not forward work related documents to your personal e-mail, such as Hotmail, Yahoo mail, Gmail, or other accounts from your Internet Service Provider (ISP).
- Do not access or attempt to access someone else’s e-mail without proper authorization.
- Do not open e-mails and attachments from senders you don’t recognize. Some attached files may contain viruses. Report suspicious e-mail to the ESD and request instructions for blocking repeated SPAM senders.
- Do not visit web sites intended for adult only audiences, gambling or games, illegal activities or disrespect, hatred, and intolerance of others.
- Do not forward chain letters, solicitation for charities, “feel-good” letters, alleged virus alerts, or any other such SPAM. They disrupt colleagues from their work, clog the networks, and use up storage space. With respect to alleged virus alerts, be assured that our EIS and ESD departments are also receiving these messages and applying the proper review procedures.

- Do not provide details of your identity or work place, including e-mail address, to any site for the purpose of receiving newsletters, product offerings or other benefits, unless directly related to your job and role at eHealth Ontario.
- Do not create, modify, execute or transmit any computer program or instructions intended to obscure the true identity of an e-mail sender.
- Do not forge, or attempt to forge any part of any e-mail transmission.
- Do not reply to SPAM messages, even if they offer to remove you from their mailing list. By responding, you confirm your e-mail address is active and you will receive more SPAM. Simply delete any SPAM message you receive.
- Use the eHealth Ontario approved format for an electronic signature and standard disclaimer for your eHealth Ontario e-mail account.
- Limited personal use of e-mail and Internet is acceptable at work providing it does not interfere with work responsibilities.
- Respect copyright and licensing requirements from the distributor when downloading material.

4.4.11 Other Mobile Devices

Cell Phones

If your job requires regular mobile communications you will receive a BlackBerry mobile phone from eHealth Ontario, or another authorized and supported cell phone. This device can be used securely for both voice and e-mail communications. It is recommended that you 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 416-586-4ESD.

You should avoid using your personal cell phone for business related communications. If circumstances require the use of your personal cell phone for business, do not use it for any text transmissions, and limit the voice use to non-confidential information. Under no circumstances can you direct eHealth Ontario e-mail to your personal cell phone.

Cameras

Cameras of any type (digital, cell phone, BlackBerry, etc) 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 Chief Privacy & Security Officer.

The standard eHealth Ontario-issued BlackBerry devices are distributed to users with the built-in camera disabled. You must not try to re-enable the camera. If special circumstances exist where eHealth Ontario business requirements necessitate the enabling of the camera function, contact ESD to initiate the established approval process.

USB Memory Devices

USB memory devices, also known as USB memory sticks, have replaced diskettes as a media for making backups and transporting digital information between computers. The main risks in using these devices are potential virus infections and data loss in case the device is lost or stolen.

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. For

longer term backups do not rely on USB memory sticks. Use the network drive assigned to you on eHealth Ontario network.

Do not use USB memory sticks received from unknown sources, such as free promotional materials from vendors and exhibitors. A number of cases were reported where these devices were infected with viruses or spyware.

eHealth Ontario has a preferred product for USB memory sticks which supports encryption, thus protecting the data in case the device is lost. Call ESD to request a device. Management approval may be required.

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.

4.5 Privacy and Security Incidents

4.5.1 What is an Incident?

Incidents may be accidental, deliberate, or suspected. Privacy incidents occur when there is an actual or potential unauthorized or illegal access to, use, collection, disclosure, retention, modification or destruction of Personal Information (PI) or Personal Health Information (PHI). Security incidents are adverse events or situations that result in a potential compromise of information confidentiality, integrity, or availability.

eHealth Ontario has established the Enterprise Security and Privacy Incident Management program (ESPIM) for responding to incidents. You must report any incident regardless of its nature (privacy and/or security), or perceived level of potential harm, by immediately contacting the ESD.

Examples of privacy or security incidents include:

- The unauthorized use, disclosure, transfer, or exchange of Personal Information or Personal Health Information. Examples include: misdirected facsimile transmissions, misplaced employee personnel files, tickets containing PHI.
- The compromise of information systems containing Personal Information or Personal Health Information.
- Unauthorized access to information, or unauthorized use, collection, disclosure, retention, modification, or destruction of information.
- Waste, fraud, abuse, loss or theft of, or damage to physical assets (e.g., computers, networks, servers, etc), or informational assets (e.g., applications, databases, reports, etc.).
- Discovery of a vulnerability or weakness in hardware or software that could lead to loss of confidentiality, integrity, or availability of information.
- Virus infections or detection of spy-ware and other mal-ware.
- Lost or compromised passwords, office access cards, or remote access tokens.
- Discovery of software applications installed on computers without management approval and without proper change control processes.

4.5.2 What to do in the event of a Privacy or Security Incident

- eHealth Ontario has a regulatory obligation to report security and privacy incidents at the first reasonable opportunity. If you suspect that the privacy, confidentiality, integrity or availability of information in any business or

office application has been compromised, you must report the incident to ESD at 416-586-4373 (local) or call 866-464-4373 (toll free). Trained investigators will respond to your inquiries and guide you in dealing with privacy or security incidents.

Anyone reporting an incident may be required to assist the Director(s) Privacy and/or Security by providing details to the investigators to assist with the preparation of a Privacy and/or Security Investigation report.

4.5.3 Whistleblower Protection

eHealth Ontario extends “whistleblower” protection to any eHealth Ontario employee or contractor who reports an actual or potential breach of privacy or security.

4.6 Privacy and Security Training and Awareness

Training and awareness are vital to creating a culture of privacy and security at eHealth Ontario. All eHealth Ontario Personnel are required to complete the mandatory Privacy and Security Fundamentals training modules. Additional role-based privacy and security training may be required.

4.7 Getting Help for Privacy and Security Questions

4.7.1 Your Privacy and Security Related Questions

If you have any sensitive questions or concerns about your responsibilities related to privacy or confidentiality, we encourage you to contact the Director of Privacy or Security, in person, by phone or by email.

4.7.2 Other Supporting Resources

For assistance with any computer related questions or concerns regarding the privacy and security issues and standards outlined in this document, contact:

Enterprise Service Desk (ESD)

Phone: 416-586-4373 (local) or 866-364-4373 (toll free)

E-mail: esd@ehealthontario.on.ca

For more information on how to maximize the use of your office equipment, visit:

http://teamsites/sites/EIS_Portal/default.aspx

For Hardware and Software Request Form fill in the information required in this form:

http://teamsites/sites/EIS_Portal/pages/Service%20Requests.aspx

To learn more about information security, visit:

http://teamsites/sites/Security_Team/default.aspx or contact us at: information.security@ehealthontario.on.ca

Appendix A - Privacy and Security Acknowledgement and Agreement Form

THIS PAGE LEFT INTENTIONALLY BLANK



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

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

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

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

eHealth Ontario

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 FIPPA, PHIPA, and associated regulations, as amended from time to time;
- (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 and agree that you will immediately notify the Chief Privacy and Security Officer, representing eHealth Ontario, in the event of your awareness of any violation of eHealth Ontario’s Privacy and Data Protection Policy, Information Security Policy and other eHealth Ontario information management policies, as amended from time to time;
- (vi) Acknowledge and agree that you will immediately notify the Chief Privacy and Security Officer, representing eHealth Ontario, in the event of your access, use, disclosure or disposal of Personal Information or Personal Health Information, other than in accordance with eHealth Ontario’s Privacy and Data Protection Policy, Enterprise 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;
- (vii) 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
- (viii) 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

