

# University Health Network Policy & Procedure Manual Administrative: Appropriate Use of Information & Information Technology

## 1. Policy

University Health Network (UHN) will make all reasonable efforts to protect information and information technology (IT) resources owned or under the custody of UHN (“**UHN information and IT resources**”) against disclosure, disruption, inappropriate or unauthorized access, loss or theft, and tampering.

All **UHN agents** (including all UHN employees, physicians/clinicians, learners, researchers, volunteers, observers, consultants, contractors, or other service provider/vendor (“third party”), etc.) who have access to UHN information and IT resources are required to use these resources in a manner that does not jeopardize the safety of patients and the UHN community, open UHN to any negative ethical, reputational, legal, regulatory or technical consequences, or reflect poorly on UHN.

This policy contains requirements for the appropriate use of UHN information and IT resources with respect to:

- [general computing](#)
- [protecting personal health information \(PHI\), personal information \(PI\), and corporate confidential information \(CCI\)](#)
- [using email](#)
- [faxing, photocopying, and printing](#)
- [using the intranet, internet, and social media](#)
- [telephone, web or video conferencing, paging, instant messaging, and texting](#)
- [telecommunication for commercial purposes](#)
- [working remotely](#)
- [reporting privacy breaches and security incidents](#)

This policy pertains to **all** UHN information and [IT resources](#) and technologies, whether or not they are explicitly identified or named in this policy.

This policy applies to **all** UHN agents.

This material has been prepared solely for use at University Health Network (UHN). UHN accepts no responsibility for use of this material by any person or organization not associated with UHN. No part of this document may be reproduced in any form for publication without permission of UHN. A printed copy of this document may not reflect the current, electronic version on the UHN Intranet.

|               |   |                |  |
|---------------|---|----------------|--|
| Policy Number | <b>1.40.012</b>                                       | Original Date  | <b>01/03</b>   |
| Section       | <b>Privacy &amp; Information Security</b>             | Revision Dates | <b>06/07; 11/08; 09/10; 01/11; 04/19; 05/19; 03/22; 08/24; 06/25</b> |
| Issued By     | <b>UHN IT Executive Committee</b>                     | Review Dates   |  |
| Approved By   | <b>Vice-president &amp; Chief Information Officer</b> | Page           | <b>1 of 20</b>   |

## 1.1 Exceptions

Any exceptions to this policy must be approved in advance and in writing by the Chief Information Security Officer, Chief Technology Officer, Chief Information Officer, or, where appropriate, the Privacy Office.

**Note:** Contact the UHN Digital Security team to initiate the request.

## 1.2 Enforcement

Failure to adhere to this policy may result in the suspension or loss of access privileges, as well as other disciplinary measures, up to and including cessation of employment or affiliation with UHN.

In the event of a privacy breach, disciplinary action may also include notification to applicable professional college(s), the [Information and Privacy Commissioner of Ontario \(IPC\)](#), or other legally required or permitted organizations or individuals. Individuals found to have willfully contravened Ontario's [Personal Health Information Protection Act \(PHIPA\)](#) may also face fines up to \$200,000 by the IPC and organizations may face fines up to \$1 million. The IPC is also able to levy administrative penalties against organizations.

## 1.3 Roles & Responsibilities

### 1.3.1 All UHN Agents

- Read and comply with this policy.
- Comply with all end user agreements signed as a prerequisite to being provisioned access to any electronic system.
- Read, sign, and comply with the requirements of the UHN Confidentiality Agreement annually.
- Complete mandatory Privacy and Cybersecurity e-learning annually.
- Fulfil all privacy and security responsibilities as defined in this policy, other relevant security policies and supporting documents, and employment or contractual agreements.
- Use UHN information and IT resources only for the purpose of their UHN-authorized work.
- Maintain the confidentiality, integrity, and availability of information accessed consistent with UHN's approved safeguards.

This material has been prepared solely for use at University Health Network (UHN). UHN accepts no responsibility for use of this material by any person or organization not associated with UHN. No part of this document may be reproduced in any form for publication without permission of UHN. A printed copy of this document may not reflect the current, electronic version on the UHN Intranet.

|               |   |                |  |
|---------------|---|----------------|--|
| Policy Number | <b>1.40.012</b>                                       | Original Date  | <b>01/03</b>   |
| Section       | <b>Privacy &amp; Information Security</b>             | Revision Dates | <b>06/07; 11/08; 09/10; 01/11; 04/19; 05/19; 03/22; 08/24; 06/25</b> |
| Issued By     | <b>UHN IT Executive Committee</b>                     | Review Dates   |  |
| Approved By   | <b>Vice-president &amp; Chief Information Officer</b> | Page           | <b>2 of 20</b>   |

- Ask questions when unsure of a privacy or security control, requirement, policy, process, procedure, or practice. Contact your manager or UHN Privacy or Digital Security (see [Appendix: Contact Information](#)).

### 1.3.2 Managers & Supervisors

- Understand this policy and any supporting documents.
- Ensure that departmental operating processes, procedures, and practices do not undermine the privacy or security of UHN's information or IT resources.
- Ensure that UHN agents reporting to them complete mandatory annual privacy and security training.
- Ensure that reports and third parties are aware of and understand their privacy and security responsibilities.
- Hold reports and third parties accountable for privacy and security violations.

### 1.3.3 Digital Security

- Maintain this policy by reviewing and updating it (at least) annually.
- Identify the need to develop, publish, or maintain any security-related guidance documents to support this policy.
- Act as the point of contact for all questions related to security.

### 1.3.4 Privacy

- Review and approve this policy.
- Identify the need to develop, publish, or maintain any privacy-related guidance documents to support this policy.
- Act as the point of contact for all questions related to privacy.

This material has been prepared solely for use at University Health Network (UHN). UHN accepts no responsibility for use of this material by any person or organization not associated with UHN. No part of this document may be reproduced in any form for publication without permission of UHN. A printed copy of this document may not reflect the current, electronic version on the UHN Intranet.

|               |   |                |  |
|---------------|---|----------------|--|
| Policy Number | <b>1.40.012</b>                                       | Original Date  | <b>01/03</b>   |
| Section       | <b>Privacy &amp; Information Security</b>             | Revision Dates | <b>06/07; 11/08; 09/10; 01/11; 04/19; 05/19; 03/22; 08/24; 06/25</b> |
| Issued By     | <b>UHN IT Executive Committee</b>                     | Review Dates   |  |
| Approved By   | <b>Vice-president &amp; Chief Information Officer</b> | Page           | <b>3 of 20</b>   |

## 1.4 General Computing

UHN has the right to monitor, log, and audit all access to UHN information and IT resources, including the use of its name, logo, or identity where the activity is performed using a UHN device.

UHN monitors, logs, and audits the network activity of personal devices when they are connected to the UHN corporate or guest networks, or when there is user activity within a mobile device management solution. No UHN agent should have an expectation of privacy if they use UHN information or IT resources for personal purposes. All agents will be held accountable for any misuse of UHN information and IT resources.

### UHN agents must always:

- ✓ Use only their assigned user ID and passphrase/password (“credentials”) to access UHN information and IT resources, with the exception of authorized shared/group credentials.
- ✓ Use **only** UHN-approved IT resources to conduct UHN business, with the limited exceptions outlined below.

**Note:** Personal IT resources should only be used if UHN has provided the agent with a means of accessing UHN information or IT resources via a personal IT resource in a secure way (e.g. through the use of Office 365 or mobile device management solution).

- ✓ Comply with all UHN policies when using UHN information and IT resources, whether or not those resources are accessed on-site or remotely.
- ✓ Use **only** UHN-approved IT resources (including artificial intelligence (AI) tools, automated software/bots, and other IT resources) when [PHI/PI/CCI](#) is being entered, handled, or discussed.

**Note:** Entering PHI/PI/CCI in unapproved tools is a privacy breach and a violation of PHIPA and professional college guidelines and policies, as vendors may use UHN PHI/PI/CCI to train vendor algorithms and for other non-UHN purposes.

**Note:** Data where direct identifiers (such as name and MRN) are removed may still be PHI. Refer to [UHN's De-Identification and Anonymized Data Standard](#) to confirm whether data is PHI.


**Note:** The signed version of Microsoft CoPilot has been approved for use at UHN.

- ✓ Before using Microsoft CoPilot, review UHN's [Acceptable Use Guidelines for Microsoft \(MS\) CoPilot, MS Teams Recording and Transcription, and Teams Premium](#) and ensure all use is compliant with the guidelines.

This material has been prepared solely for use at University Health Network (UHN). UHN accepts no responsibility for use of this material by any person or organization not associated with UHN. No part of this document may be reproduced in any form for publication without permission of UHN. A printed copy of this document may not reflect the current, electronic version on the UHN Intranet.

|               |  |                |   |
|---------------|--|----------------|---|
| Policy Number | 1.40.012                                   | Original Date  | 01/03   |
| Section       | Privacy & Information Security             | Revision Dates | 06/07; 11/08; 09/10; 01/11; 04/19; 05/19; 03/22; 08/24; 06/25 |
| Issued By     | UHN IT Executive Committee                 | Review Dates   |   |
| Approved By   | Vice-president & Chief Information Officer | Page           | 4 of 20   |

- ✓ When using Microsoft CoPilot, ensure they are signed into UHN's Microsoft CoPilot with their UHN credentials.

**Note:** The approved use of Microsoft Copilot will be indicated by an icon within the tool. As of the current date stamp of this policy, the icon is a green shield with checkmark (i.e.  ). Using Microsoft CoPilot without signing into UHN's Microsoft CoPilot will result in a privacy breach.

- ✓ Make it a practice to review meeting participant lists for any inclusion of unapproved AI tools or automated agents, and remove them from meetings before proceeding or before discussing any PHI/PI/CCI.

**UHN agents must never:**

- ✗ Allow another person to use their credentials for any purpose. (e.g. logging into a system, software, or technologies).

**Note:** The agent is accountable for all actions performed with their credentials.

- ✗ Allow their personal use of UHN IT resources to interfere with its normal performance or with their job-related duties and responsibilities.
- ✗ Use unauthorized digital tools (including AI products such as ChatGPT) for UHN work purposes.
- ✗ Use UHN IT resources to:
  - contravene [UHN's Purpose, Principle, and Values, Fostering Respect in the Workplace](#) policy 2.50.005, or any other UHN policy;
  - engage in online gaming or gambling;
  - solicit or promote commercial interests that have not been sanctioned by UHN (e.g. using the [email](#) system for a personal business); **or**
  - violate provincial or federal laws, professional codes of ethics or standards of professional conduct.
- ✗ Disable, override, or willfully bypass any security control or attempt to exploit any suspected security weakness on any UHN IT resource, unless it is part of their assigned responsibilities and they are explicitly authorized to do so.
- ✗ Knowingly perform an act that will interfere with the normal operations of a UHN IT resource or try to disrupt that resource either by making it unavailable, or by affecting the integrity of the data being stored in or processed by the IT resource.

This material has been prepared solely for use at University Health Network (UHN). UHN accepts no responsibility for use of this material by any person or organization not associated with UHN. No part of this document may be reproduced in any form for publication without permission of UHN. A printed copy of this document may not reflect the current, electronic version on the UHN Intranet.

|               |   |                |  |
|---------------|---|----------------|--|
| Policy Number | <b>1.40.012</b>                                       | Original Date  | <b>01/03</b>   |
| Section       | <b>Privacy &amp; Information Security</b>             | Revision Dates | <b>06/07; 11/08; 09/10; 01/11; 04/19; 05/19; 03/22; 08/24; 06/25</b> |
| Issued By     | <b>UHN IT Executive Committee</b>                     | Review Dates   |  |
| Approved By   | <b>Vice-president &amp; Chief Information Officer</b> | Page           | <b>5 of 20</b>   |

## 1.5 Protecting Personal Health Information, Personal Information & Corporate Confidential Information

UHN and all UHN agents have a legal obligation to maintain the privacy and security of [PHI/PI/CCI](#). To meet these obligations, only UHN-approved IT resources may be used to collect, use, or store PHI/PI/CCI. In the event of a [privacy breach](#) with respect to PHI/PI, UHN agents may be subject to [disciplinary action](#), including notification to applicable professional colleges and the [IPC](#). Individuals found to have willfully contravened [PHIPA](#) may also face fines up to \$200,000 by the IPC and organizations may face fines up to \$1 million. The IPC is also able to levy administrative penalties against organizations.

**Note:** See [Privacy & Access](#) policy 1.40.007 for more information on how UHN protects patient privacy and ensures the proper collection, use, and disclosure of personal health information. See [Information Security](#) policy 1.40.028 for more information on how UHN secures its information and IT resources.

**Note:** To confirm whether an IT resource is approved for handling PHI/PI/CCI, contact the local help desk.

### UHN agents must always:


- ✓ Ensure any changes to existing IT resources or implementation of new IT resources that store or process [PHI/PI/CCI](#) are assessed by UHN Digital Security and assessed and approved by UHN Privacy prior to implementation.
- ✓ Abide by the terms and condition of shared systems, especially those that provide access to PHI (e.g. RM&R and ConnectingOntario).
- ✓ Use encrypted and UHN-approved devices (e.g. laptops, servers, pagers, etc.) for storage and transfer of PHI/PI/CCI.
- ✓ Ensure that any access, collection, retention, deletion, transmission/transfer, or any other interaction with PHI/PI/CCI is only done to fulfill UHN-assigned duties, and not for any other purpose.
- ✓ Ensure that when PHI/PI/CCI needs to be stored, it is stored on UHN-approved devices and storage networks (e.g. a UHN-provided OneDrive, SharePoint, or network drive). PHI should not be used or stored outside of the health information system (HIS) unless necessary and where necessary. The least amount of PHI for the purpose should be stored, and only for as long as necessary for the defined purpose.

**Note:** UHN-provided storage networks should be the primary storage location for important files instead of local hard drives (e.g. 'C' drive or My Documents) even if it is encrypted, as local hard drives are not backed

This material has been prepared solely for use at University Health Network (UHN). UHN accepts no responsibility for use of this material by any person or organization not associated with UHN. No part of this document may be reproduced in any form for publication without permission of UHN. A printed copy of this document may not reflect the current, electronic version on the UHN Intranet.

|               |   |                |  |
|---------------|---|----------------|--|
| Policy Number | <b>1.40.012</b>                                       | Original Date  | <b>01/03</b>   |
| Section       | <b>Privacy &amp; Information Security</b>             | Revision Dates | <b>06/07; 11/08; 09/10; 01/11; 04/19; 05/19; 03/22; 08/24; 06/25</b> |
| Issued By     | <b>UHN IT Executive Committee</b>                     | Review Dates   |  |
| Approved By   | <b>Vice-president &amp; Chief Information Officer</b> | Page           | <b>6 of 20</b>   |

up and information may be unrecoverable in the event of the device experiencing a hardware failure or malicious attack (e.g. ransomware).

- ✓ Where possible, share files containing PHI/PI/CCI with their team using a UHN-provided storage network.
- ✓ Edit documents online (e.g. when using Office365) without saving them to a local computer drive if accessing files on an [unmanaged device](#) or a UHN-shared device.
- ✓ Lock their screen (e.g. by pressing ctrl + alt + delete and selecting “Lock this computer” or  +L on a Windows workstation) or log out of all applications on a scratch PC when leaving it unattended.
- ✓ Lock their mobile device (e.g. by using screen lock or storing the mobile device in a locked area) when leaving it unattended.
- ✓ Ensure that any pictures or visual and audio recordings taken on UHN premises do not contain or reveal any CCI or PHI/PI (except where taken for the purpose of providing direct patient care, or unless documented consent has been obtained from the individual about whom the information relates and for the purposes for which the picture was taken).

**Note:** Identifiers can include voice recordings (both the content of the recording and/or the sound of a voice), pictures of a patient’s face or body part that can uniquely identify them (e.g. a tattoo, unusual tumour, etc.), or any other data element that could lead another person or technology (e.g. AI) to identify the individual about whom the information relates. Pictures or recordings that capture displays of an application or system may also include PHI/PI/CCI. Always capture the least amount of information necessary to achieve the purpose.

**Note:** See [Consent for Audio/Visual Taping](#) policy 3.20.004.

**Note:** For research purposes, documented consent for all approved uses of PHI (including audio and visual recordings) is requested at the outset of the research study and periodically thereafter as required by the Research Ethics Board (REB).

- ✓ Verify a patient’s identity prior to disclosing PHI, as per [Positive Patient Identification](#) policy 3.30.016.

This material has been prepared solely for use at University Health Network (UHN). UHN accepts no responsibility for use of this material by any person or organization not associated with UHN. No part of this document may be reproduced in any form for publication without permission of UHN. A printed copy of this document may not reflect the current, electronic version on the UHN Intranet.

|               |   |                |  |
|---------------|---|----------------|--|
| Policy Number | <b>1.40.012</b>                                       | Original Date  | <b>01/03</b>   |
| Section       | <b>Privacy &amp; Information Security</b>             | Revision Dates | <b>06/07; 11/08; 09/10; 01/11; 04/19; 05/19; 03/22; 08/24; 06/25</b> |
| Issued By     | <b>UHN IT Executive Committee</b>                     | Review Dates   |  |
| Approved By   | <b>Vice-president &amp; Chief Information Officer</b> | Page           | <b>7 of 20</b>   |

- ✓ Transmit or transport PHI/PI/CCI securely.

**Note:** When electronically transmitting PHI/PI/CCI, the order of the preferred methods is:

1. [secure email](#) (i.e. both the sender and recipient of the email is accessible through the UHN Global Address List (GAL))
2. [File Share](#), using the Patient Info option for all PHI/PI/CCI, along with a strong password

**Note:** The password must be sent through a means other than [email](#), e.g. tell the user the password in person or over the phone.

**Note:** For files too large for File Share, contact UHN Digital.

3. [unsecure email](#), with PHI/PI/CCI **sent in an encrypted file attachment using a strong password**

**Note:** The password must be sent through a means other than [email](#), e.g. tell the user the password in person or over the phone. See [Guide to Encrypting Files Using 7-zip](#).

4. [fax](#)

- ✓ Securely dispose of PHI/PI/CCI and any IT resources that may contain this information by following their department's processes and procedures for destruction (e.g. by placing paper in a secure shredding receptacle).

**Note:** See [Management, Retention & Destruction of UHN Records](#) policy 1.30.007, [Privacy & Access](#) policy 1.40.007, and related policies.

**UHN agents must never:**

- ✗ Download or save [PHI/PI/CCI](#) onto any unencrypted device or [unmanaged device](#).

**Note:** The only exception is the rare circumstance when unsecure methods of recording or sharing of PHI is urgently required for patient care purposes.

**Note:** Where PHI/PI/CCI is downloaded or saved onto unencrypted or unmanaged devices to address an urgent patient care matter, the PHI/PI/CCI must be deleted or removed from the unencrypted or unmanaged device as soon as possible following the event. Where appropriate, ensure to clear the browser's temporary files after accessing a UHN IT resource (e.g. Office 365) from a non-UHN device.

**Note:** Opening or viewing file attachments may cause them to download onto the device.

- ✗ Include PHI in any unencrypted message sent by pager, text, email, or other non-UHN-approved communication method, except when urgently required for patient care purposes.

This material has been prepared solely for use at University Health Network (UHN). UHN accepts no responsibility for use of this material by any person or organization not associated with UHN. No part of this document may be reproduced in any form for publication without permission of UHN. A printed copy of this document may not reflect the current, electronic version on the UHN Intranet.

|               |   |                |  |
|---------------|---|----------------|--|
| Policy Number | <b>1.40.012</b>                                       | Original Date  | <b>01/03</b>   |
| Section       | <b>Privacy &amp; Information Security</b>             | Revision Dates | <b>06/07; 11/08; 09/10; 01/11; 04/19; 05/19; 03/22; 08/24; 06/25</b> |
| Issued By     | <b>UHN IT Executive Committee</b>                     | Review Dates   |  |
| Approved By   | <b>Vice-president &amp; Chief Information Officer</b> | Page           | <b>8 of 20</b>   |

- ✗ Paste, save, upload, share, send, or receive PHI/PI/CCI to or using non-UHN-approved applications, email, file-hosting systems, websites or services (e.g. Google Drive, Dropbox, Slack, etc.).

**Note:** For example, never copy & paste PHI/PI/CCI from Office365 to a personal Gmail account.

**Note:** Contact the Digital Service Desk to confirm whether a particular tool is approved for use at UHN.

- ✗ Synchronize files containing PHI/PI/CCI to an [unmanaged device](#), e.g. synchronizing files containing PHI from a UHN-approved solution (e.g. OneDrive) to a personal, unmanaged computer.

**Note:** UHN agents are accountable for ensuring PHI/PI/CCI is saved onto UHN-approved devices/applications.

- ✗ Discuss or disclose (through any medium, e.g. email, social media, verbal, etc.) PHI/PI/CCI to anyone, unless that individual has a UHN-defined [need-to-know](#) and, in the cases of PHI, only for the purposes for which it has been collected or with patient consent.

- ✗ Discuss PHI/PI/CCI in public areas, including elevators, as it may be easily overheard.

**Note:** Be mindful of eavesdropping in offices, wards, or units.

## 1.6 Using Email

**Note:** A confidentiality disclaimer is automatically attached to all emails sent from UHN accounts to external recipients.

**Note:** UHN strictly limits the sending of communications to all users. Messages deemed unsuitable for all-user distribution may be disseminated through alternative methods of communication. See [Ways to Get Your Message Out at UHN](#).

### UHN agents must always:

- ✓ Ensure that they have documented consent from patients for the specific purposes under which the patient can be emailed.
- ✓ Delete emails when no longer needed.
- ✓ Send emails containing [PHI/PI/CCI](#) using only [secure email](#).

**Note:** For other methods of transmission, see section [1.5 Protecting PHI/PI/CCI](#).

This material has been prepared solely for use at University Health Network (UHN). UHN accepts no responsibility for use of this material by any person or organization not associated with UHN. No part of this document may be reproduced in any form for publication without permission of UHN. A printed copy of this document may not reflect the current, electronic version on the UHN Intranet.

|               |   |                |  |
|---------------|---|----------------|--|
| Policy Number | <b>1.40.012</b>                                       | Original Date  | <b>01/03</b>   |
| Section       | <b>Privacy &amp; Information Security</b>             | Revision Dates | <b>06/07; 11/08; 09/10; 01/11; 04/19; 05/19; 03/22; 08/24; 06/25</b> |
| Issued By     | <b>UHN IT Executive Committee</b>                     | Review Dates   |  |
| Approved By   | <b>Vice-president &amp; Chief Information Officer</b> | Page           | <b>9 of 20</b>   |

- ✓ Double check the “To,” “CC,” and “BCC” fields prior to sending messages containing PHI/PI/CCI.
- ✓ Use a UHN-approved tool for mass distribution when routinely distributing emails (such as newsletters) to multiple patients.
- ✓ Identify themselves when sending an email from a shared account, or an account that has been delegated to them (e.g. by using the “Sent on Behalf of” function).
- ✓ Where possible, retain messages containing PHI in their inbox or in an archive that is saved to a network drive rather than in an archive on a local hard drive (e.g. ‘C’ drive, My Documents, desktop), as only network drives are automatically backed up.

**Note:** Messages relevant to an individual's care must be stored in the patient's health record.

- ✓ Keep personal messages in a separate folder marked as “Personal” to distinguish work-related email from personal email in the event of a [Freedom of Information and Protection of Privacy Act \(FIPPA\)](#) request.
- ✓ Only use the email account provided to them by UHN when conducting UHN business.

**Note:** External email accounts that are secure (e.g. ONE Mail) may be used to conduct UHN business only if a UHN email account has not been provided. Never use email accounts not authorized for use at UHN (e.g. Hotmail, Gmail, etc.) to conduct UHN business.

**UHN agents must never:**

- ✗ Click on links or open attachments received from unknown senders, as these may contain malware.

**Note:** When in doubt, contact the local help desk or forward the email to [spam@uhn.ca](mailto:spam@uhn.ca).

- ✗ Send emails containing [PHI](#) to an unsecured email account, unless:
  - a. The patient has provided documented, express consent to communicate by email for the specific purposes that they are emailing the patient. (See the Sending & Receiving Email from Patients section of [Email Usage](#) policy 1.40.014 for how to obtain consent); **or**
  - b. The email is required for a one-time emergency, urgent, or other exceptional circumstance for the provision of care or to prevent harm between care providers or patients.

This material has been prepared solely for use at University Health Network (UHN). UHN accepts no responsibility for use of this material by any person or organization not associated with UHN. No part of this document may be reproduced in any form for publication without permission of UHN. A printed copy of this document may not reflect the current, electronic version on the UHN Intranet.

|               |   |                |  |
|---------------|---|----------------|--|
| Policy Number | <b>1.40.012</b>                                       | Original Date  | <b>01/03</b>   |
| Section       | <b>Privacy &amp; Information Security</b>             | Revision Dates | <b>06/07; 11/08; 09/10; 01/11; 04/19; 05/19; 03/22; 08/24; 06/25</b> |
| Issued By     | <b>UHN IT Executive Committee</b>                     | Review Dates   |  |
| Approved By   | <b>Vice-president &amp; Chief Information Officer</b> | Page           | <b>10 of 20</b>  |

- ✘ Provide someone who is not privileged to see the same information as they are with delegate access to their email account.
- ✘ Auto-forward email to either:
  - a. Any external email account; **or**
  - b. An internal email account, unless it is to support UHN business (e.g. to provide adequate coverage in the case of short leaves) and they can reasonably expect that the recipient will not receive any PHI/PI to which the recipient would not have a [need-to-know](#).
- ✘ Send PHI in a mass communication, with the exception of a one-time emergency, urgent, or other exceptional circumstance for the provision of care or to prevent harm to a patient (e.g. sending out a Code Yellow email).
- ✘ Recall emails sent externally if they think they may have breached [PHI/PI/CCI](#), as this could result in an additional breach.

**Note:** If the UHN agent believes this has occurred, this must be reported as a privacy incident. See section [1.12 Reporting Privacy & Security Incidents](#).

- ✘ Open attachments that they reasonably believe to contain PHI/PI/CCI on any [unmanaged devices](#) or any shared devices (where other users are not authorized to view the information), as attachments may be downloaded automatically.
- ✘ Alter the original content of messages without the author's approval.

## 1.7 Faxing, Photocopying & Printing

**Note:** For information on the secure set up of printers, faxes, and photocopying machines, contact [UHN Digital Security](#).

### UHN agents must always:

- ✓ Retrieve faxes/papers that contain [PHI/PI/CCI](#) from fax inboxes/faxes and printers immediately.
- ✓ Ensure that they do not leave original materials in/on photocopiers or fax machines.

**Note:** Delete/place in shredding boxes faxes once they have been reviewed and redirected.

This material has been prepared solely for use at University Health Network (UHN). UHN accepts no responsibility for use of this material by any person or organization not associated with UHN. No part of this document may be reproduced in any form for publication without permission of UHN. A printed copy of this document may not reflect the current, electronic version on the UHN Intranet.

|               |   |                |  |
|---------------|---|----------------|--|
| Policy Number | <b>1.40.012</b>                                       | Original Date  | <b>01/03</b>   |
| Section       | <b>Privacy &amp; Information Security</b>             | Revision Dates | <b>06/07; 11/08; 09/10; 01/11; 04/19; 05/19; 03/22; 08/24; 06/25</b> |
| Issued By     | <b>UHN IT Executive Committee</b>                     | Review Dates   |  |
| Approved By   | <b>Vice-president &amp; Chief Information Officer</b> | Page           | <b>11 of 20</b>  |

- ✓ To minimize the risk of inadvertent disclosure when faxing, only fax PHI/PI/CCI when it is necessary for the provision of care or other UHN business.
- ✓ Report faxes containing PHI/PI/CCI that are sent to the wrong or unauthorized recipient as a privacy incident. (See section [1.12 Reporting Privacy & Security Incidents.](#))
- ✓ Double-check the fax number entered on the screen.
- ✓ Whenever possible, enter frequently used numbers into the speed/auto dial of the fax machine/e-fax to minimize input errors.
- ✓ Ensure an accurate source of contact information is used to avoid misdirected faxes.
- ✓ Use a fax cover sheet that clearly indicates the sender's name, recipient's name, and the sender's relevant contact information, as well as the following confidentiality statement:

ATTENTION: THIS FAX INCLUDES CONFIDENTIAL INFORMATION

This facsimile is intended only for use by the addressee named above. If you are not the intended recipient, or the employee or agent responsible for delivering it to the intended recipient, you are hereby notified that any dissemination, copying or disclosure of the contents of this facsimile is strictly prohibited.

If you received this facsimile in error, notify us by telephone immediately at **[insert phone number]**.

\*\*\*\*\*

For any change to your name/location/provider information, you must contact the following organizations: **[insert organization/department names & phone numbers]**.

## 1.8 Using the Intranet, Internet & Social Media

UHN reserves the right to restrict access to material on social media and external web sites where such content or use of such tools is deemed inappropriate or not secure. However, an absence of restrictions does not imply that accessible tools or information are authorized.

### UHN agents must always:

- ✓ Remember that their personal and off-hours use of the internet and social media could lead to disciplinary action, up to and including cessation of employment or affiliation with UHN if it violates provincial or federal laws,

This material has been prepared solely for use at University Health Network (UHN). UHN accepts no responsibility for use of this material by any person or organization not associated with UHN. No part of this document may be reproduced in any form for publication without permission of UHN. A printed copy of this document may not reflect the current, electronic version on the UHN Intranet.

|               |   |                |  |
|---------------|---|----------------|--|
| Policy Number | <b>1.40.012</b>                                       | Original Date  | <b>01/03</b>   |
| Section       | <b>Privacy &amp; Information Security</b>             | Revision Dates | <b>06/07; 11/08; 09/10; 01/11; 04/19; 05/19; 03/22; 08/24; 06/25</b> |
| Issued By     | <b>UHN IT Executive Committee</b>                     | Review Dates   |  |
| Approved By   | <b>Vice-president &amp; Chief Information Officer</b> | Page           | <b>12 of 20</b>  |

professional codes of ethics, standards of professional conduct, or UHN's [Fostering Respect in the Workplace](#) policy 2.50.005.

- ✓ Abide by [UHN's Social Media Guidelines](#) when posting or commenting.
- ✓ Ensure that their use or interaction with UHN social media accounts relates to the organization's vision, mission, and values.
- ✓ Obtain approval from [Communications and Brand Strategy \(CaBS\)](#) prior to:
  - a. creating a UHN-related account on a social media platform or an internet website
  - b. posting official UHN-related content to the internet
  - c. using the UHN logo on social media or the internet
- ✓ Verify that [PHI/PI/CCI](#) is not contained in pictures, audio or visual recordings, comments, or documents that they are going to post, even if they believe personal identifiers (e.g. patient names) have been removed, unless they have documented consent.

**Note:** For research purposes, documented consent for all approved uses of PHI (including audio and visual recordings) is obtained at the outset of the research study. No additional layer of consent is required. Also see [Consent for Audio/Visual Taping](#) policy 3.20.004 and [UHN's Social Media Guidelines](#).

**UHN agents must never:**

- ✗ Expressly or implicitly attribute personal statements, opinions or beliefs to UHN, unless they have been authorized to do so by CaBS.

**1.9 Telephone, Web or Video Conferencing, Paging, Instant Messaging, SMS & Texting**

**UHN agents must always:**

- ✓ Use conferencing solutions that have been assessed by UHN Digital Security and assessed and approved by UHN Privacy for handling [PHI/PI/CCI](#) whenever such information needs to be discussed (e.g. TeleHealth).
- ✓ Inform all participants of the risks associated with using conferencing solutions if their PHI/PI will be discussed.
- ✓ Obtain patient consent for the use of any patient-requested unapproved communication solutions.

This material has been prepared solely for use at University Health Network (UHN). UHN accepts no responsibility for use of this material by any person or organization not associated with UHN. No part of this document may be reproduced in any form for publication without permission of UHN. A printed copy of this document may not reflect the current, electronic version on the UHN Intranet.

|               |   |                |  |
|---------------|---|----------------|--|
| Policy Number | <b>1.40.012</b>                                       | Original Date  | <b>01/03</b>   |
| Section       | <b>Privacy &amp; Information Security</b>             | Revision Dates | <b>06/07; 11/08; 09/10; 01/11; 04/19; 05/19; 03/22; 08/24; 06/25</b> |
| Issued By     | <b>UHN IT Executive Committee</b>                     | Review Dates   |  |
| Approved By   | <b>Vice-president &amp; Chief Information Officer</b> | Page           | <b>13 of 20</b>  |

- ✓ Obtain consent prior to recording any calls with a patient or any calls that will involve PHI/PI.
- ✓ Inform all participants if an audio/video call is being recorded.
- ✓ Ensure that positive patient identification occurs prior to using conferencing solutions to interact with a patient, as per [Positive Patient Identification](#) policy 3.30.016.
- ✓ Inform all participants if any activity will be live-streamed (e.g. a surgical procedure being streamed for educational purposes either within UHN or to individuals outside of UHN), and receive documented express consent prior to the procedure, as per [Live Broadcasting of Operative Procedures](#) policy 37.30.001.
- ✓ Discuss PHI/PI/CCI in a private setting (e.g. a private office or meeting room).

**Note:** Conduct an environmental scan before videoconferencing to ensure that no unintended PHI/PI/CCI is visible to the other party. Close blinds or drapes when using web or video-conferencing, and be mindful of others being able to overhear the call.

- ✓ Limit the information left in a voicemail where there is no documented consent from the patient.

**Note:** See [Leaving Voicemail for Patients](#) for details.

**UHN agents must never:**

- ✗ Share [PHI/PI/CCI](#) using any unapproved communications solutions.

**1.10 Telecommunication for Commercial Purposes**

**UHN agents must always:**

- ✓ Ensure that [electronic messages](#) sent for commercial purposes on behalf of UHN or from any UHN IT resources is done in a manner that complies with the Canadian Anti-Spam Legislation (CASL) and its regulations (see '[CASL](#)' [The New Canadian Anti-Spam Law](#) intranet page), and with UHN's [Telecommunications for Commercial Purposes](#) policy 1.40.027.

This material has been prepared solely for use at University Health Network (UHN). UHN accepts no responsibility for use of this material by any person or organization not associated with UHN. No part of this document may be reproduced in any form for publication without permission of UHN. A printed copy of this document may not reflect the current, electronic version on the UHN Intranet.

|               |   |                |  |
|---------------|---|----------------|--|
| Policy Number | <b>1.40.012</b>                                       | Original Date  | <b>01/03</b>   |
| Section       | <b>Privacy &amp; Information Security</b>             | Revision Dates | <b>06/07; 11/08; 09/10; 01/11; 04/19; 05/19; 03/22; 08/24; 06/25</b> |
| Issued By     | <b>UHN IT Executive Committee</b>                     | Review Dates   |  |
| Approved By   | <b>Vice-president &amp; Chief Information Officer</b> | Page           | <b>14 of 20</b>  |

## 1.11 Working Remotely

[Remote access](#) hardware (e.g. remote access tokens) must be returned to UHN, or UHN may remove remote access software, under the following conditions:

- cessation of employment or affiliation with UHN
- at the request of UHN
- deactivation of a remote access account
- violation of any provision of this or any other policy or agreement

### UHN agents must always:

- ✓ Use [managed devices](#) or UHN-approved solutions (e.g. Office365) to work remotely with [PHI/PI/CCI](#).
- ✓ Be aware of “shoulder surfing” (i.e. people looking over their shoulder), as this could lead to a breach of PHI/PI/CCI.
- ✓ Clear the browser's temporary files after accessing a UHN IT resource (e.g. Office 365) from a non-UHN device.
- ✓ Change their UHN passphrase/password as soon as they return to UHN after using a public device (e.g. public library computer).

**Note:** Do not access an internal UHN IT resources from a public device unless absolutely necessary.

- ✓ Lock IT resources that contain PHI/PI/CCI in the trunk or place it out of view before getting to their destination when required to leave their mobile device in a vehicle.

**Note:** If they get to the destination before securing the device, UHN agents should take it with them instead.

- ✓ Follow the proper procedures to disconnect from any IT resource (including shared systems) that provides access to PHI/PI/CCI remotely (i.e. use the disconnect or logout option rather than simply closing the application).

### UHN agents must never:

- ✗ Print [PHI/PI/CCI](#) at a remote location or make copies (e.g. by copying files, taking screen shots, taking pictures etc.) of such information at a remote location unless they are authorized by their manager or supervisor to do so.
- ✗ Access PHI/PI/CCI in an area where unauthorized individuals can view the information (e.g. cafés, public transit, and other non-private settings).

This material has been prepared solely for use at University Health Network (UHN). UHN accepts no responsibility for use of this material by any person or organization not associated with UHN. No part of this document may be reproduced in any form for publication without permission of UHN. A printed copy of this document may not reflect the current, electronic version on the UHN Intranet.

|               |  |                |   |
|---------------|--|----------------|---|
| Policy Number | 1.40.012                                   | Original Date  | 01/03   |
| Section       | Privacy & Information Security             | Revision Dates | 06/07; 11/08; 09/10; 01/11; 04/19; 05/19; 03/22; 08/24; 06/25 |
| Issued By     | UHN IT Executive Committee                 | Review Dates   |   |
| Approved By   | Vice-president & Chief Information Officer | Page           | 15 of 20  |

- ✗ Leave a device remotely connected to a UHN internal resource unattended in a public place or in any private area in which unauthorized individuals could gain access to the device.

## 1.12 Reporting Privacy & Security Incidents

**Note:** Examples of privacy and security incidents include, but are not limited to:

- unauthorized or accidental disclosure, or inappropriate or unauthorized access of [PHI/PI/CCI](#)
- attempts (either failed or successful) to gain unauthorized access to any form (paper or electronic) of PHI/PI/CCI
- theft or loss of an IT resource that contains PHI/PI/CCI, even if it is encrypted
- malware infection on an IT resource
- compromised passphrase/password

**UHN agents must always:**

- ✓ Immediately report suspected or confirmed:
  - a. privacy incidents to their manager/supervisor and the Privacy Office by using the [Incident eForm](#), and
  - b. security incidents to their manager/supervisor or local help desk.
- ✓ Provide their full cooperation with any privacy or security incident investigation.

## 1.13 Additional UHN Resources

- [‘CASL’ The New Canadian Anti-Spam Law](#)
- [Consent for Audio/Visual Taping](#) policy 3.20.004
- [Guide to Encrypting Files Using 7-zip](#)
- [Incident eForm](#)
- [Leaving Voicemail for Patients](#)
- [Positive Patient Identification](#) policy 3.30.016
- [UHN's Social Media Guidelines](#)
- [Telecommunications for Commercial Purposes](#) policy 1.40.027

This material has been prepared solely for use at University Health Network (UHN). UHN accepts no responsibility for use of this material by any person or organization not associated with UHN. No part of this document may be reproduced in any form for publication without permission of UHN. A printed copy of this document may not reflect the current, electronic version on the UHN Intranet.

|               |   |                |  |
|---------------|---|----------------|--|
| Policy Number | <b>1.40.012</b>                                       | Original Date  | <b>01/03</b>   |
| Section       | <b>Privacy &amp; Information Security</b>             | Revision Dates | <b>06/07; 11/08; 09/10; 01/11; 04/19; 05/19; 03/22; 08/24; 06/25</b> |
| Issued By     | <b>UHN IT Executive Committee</b>                     | Review Dates   |  |
| Approved By   | <b>Vice-president &amp; Chief Information Officer</b> | Page           | <b>16 of 20</b>  |

## 2. Definitions

**Corporate confidential information (CCI):** Information used for UHN management, business, or financial purposes, including, but not limited to:

- information on salaries and benefits
- information on Hospital payments such as OHIP numbers
- information on Hospital budgets, expenses or planning
- patient health information or other data used by administration/management for logging, registering, scheduling, tracking, or billing patients
- sensitive or privileged legal information
- employee status information/communications regarding any employee
- information that could expose the organization's reputation to damage
- information regarding use of animals at UHN for research
- information regarding use of compounds or devices that could expose internal UHN operation to malicious acts by external parties (e.g. use of a compound or device that would signal to an activist group that certain types of experimentation are being carried out at UHN)

**Electronic message:** A message sent by any means of telecommunication, including a text, sound, voice, or image message, unless the message is a “two-way interactive voice call” or a facsimile or voice recording sent to a telephone account.

**Email:** The transmission of [electronic messages](#) between an addresser and one or more addressees using dedicated software (e.g. Microsoft Outlook). It does not refer to instant messaging or short-message/multimedia messaging (SMS/MMS) services.

**External email:** All non-UHN email accounts, whether or not the email is considered secure or unsecure (e.g. email addresses at another organization, ONE Mail, Hotmail, Gmail, etc.).

**Information technology (IT) resource:** All technology hardware and software assets used for the creation, use, transmission, transport, and destruction of information. A UHN IT resource includes, but is not limited to:

- infrastructure technology owned or leased by UHN (e.g. servers, database, applications, wireless access points, etc.)
- end-points and end user devices owned or leased by UHN (e.g. workstations, laptops, tablets, cellphones, pagers, fax machines, printers, photocopiers, etc.), whether or not they are attached to the UHN network.
- applications and software owned or leased by UHN (e.g. EPR, Patient Portal, Office 365, etc.)
- UHN-branded social media accounts (e.g. Twitter accounts, Instagram accounts, etc.)

This material has been prepared solely for use at University Health Network (UHN). UHN accepts no responsibility for use of this material by any person or organization not associated with UHN. No part of this document may be reproduced in any form for publication without permission of UHN. A printed copy of this document may not reflect the current, electronic version on the UHN Intranet.

|               |   |                |  |
|---------------|---|----------------|--|
| Policy Number | <b>1.40.012</b>                                       | Original Date  | <b>01/03</b>   |
| Section       | <b>Privacy &amp; Information Security</b>             | Revision Dates | <b>06/07; 11/08; 09/10; 01/11; 04/19; 05/19; 03/22; 08/24; 06/25</b> |
| Issued By     | <b>UHN IT Executive Committee</b>                     | Review Dates   |  |
| Approved By   | <b>Vice-president &amp; Chief Information Officer</b> | Page           | <b>17 of 20</b>  |

**Managed device:** For the purposes of this policy, a managed device refers to any end user device that is centrally managed by UHN, including Mobile Device Management (MDM) devices. All end user devices not centrally managed by UHN are considered to be unmanaged devices.

MDM devices refer to personal devices that UHN has the ability to secure and manage with centralized security configurations, and that also allows for the remote wipe of a system in cases of loss or theft. See [Mobile Device Management](#) policy 1.40.026.

**Need-to-know:** A principle which stipulates that authorized access to information must only be granted to individuals if it is necessary for them to perform their assigned duties.

**Personal health information (PHI):** Information about an individual, whether living or deceased, and whether in oral or recorded form. It is information that can identify an individual and that relates to matters such as the individual's physical or mental health, the provision of health care to the individual, payments or eligibility for health care in respect of the individual, the donation by the individual of a body part or bodily substance, and the individual's health number ([PHIPA 2004](#)). PHI can be information about a physician or other care provider, a hospital staff person, a patient, or a patient's family member. Examples of PHI include a name, medical record number (MRN), health insurance number, address, telephone number, and PHI related to a patient's care, such as blood type, x-rays, consultation notes, etc. **Note:** Data where direct identifiers (such as name and MRN) are removed may still be PHI. Refer to [UHN's De-Identification and Anonymized Data Standard](#) to confirm whether data is PHI.

**Personal information (PI):** Any information about an identifiable individual, whether living or deceased, and whether in oral or recorded form, that is sensitive in nature. This refers to information collected or accessed by UHN for the purposes of employment or affiliation with UHN, with the exception of business contact information (e.g. information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email, or business fax number of the individual). Examples of PI include, but is not limited to, ethnic origin, race, religion, age, sex, gender, sexual orientation, marital status, information regarding education, financial, employment, criminal history, social insurance number, home address, personal telephone number, etc.

**Remote access:** Remote access refers to specific situations in which an agent accessing UHN internal resources over an unsecured network (e.g. the internet). An example of remote access includes accessing UHN email or network drive from home.

**Secure email:** Refers to either (1) internal email, i.e. email sent or received between any UHN email account; or (2) email sent externally to an organization with which UHN has a secure channel. All email addresses that appear in the [Global Address List \(GAL\)](#) are considered secure.

This material has been prepared solely for use at University Health Network (UHN). UHN accepts no responsibility for use of this material by any person or organization not associated with UHN. No part of this document may be reproduced in any form for publication without permission of UHN. A printed copy of this document may not reflect the current, electronic version on the UHN Intranet.

|               |   |                |  |
|---------------|---|----------------|--|
| Policy Number | <b>1.40.012</b>                                       | Original Date  | <b>01/03</b>   |
| Section       | <b>Privacy &amp; Information Security</b>             | Revision Dates | <b>06/07; 11/08; 09/10; 01/11; 04/19; 05/19; 03/22; 08/24; 06/25</b> |
| Issued By     | <b>UHN IT Executive Committee</b>                     | Review Dates   |  |
| Approved By   | <b>Vice-president &amp; Chief Information Officer</b> | Page           | <b>18 of 20</b>  |

**Social media:** A type of online media that expedites conversation, as opposed to traditional media, which delivers content but doesn't allow readers/viewers/listeners to participate in the creation or development of the content. Social media is interactive and allows users to comment and participate in the discussion on whichever social media medium they are using, whether it's a social networking site, blog, micro-blog or video-sharing site.

**Unmanaged device:** All end user devices not centrally managed by UHN. Any end user device that is centrally managed by UHN is considered to be a managed device. See definition for [managed device](#).

**Unsecure email:** Refers to any email sent or received between a UHN email account and external organization's email account with which UHN does not have a secure channel. Only email addresses that are part of the [ONE Mail or ONE Pages](#) infrastructure are considered secure.

**Working remotely:** Any situation in which a UHN agent conducts UHN business off-site, including situations in which a UHN agent does not connect to a UHN internal resource, but is using a UHN information or IT resource classified as "internal" or higher to conduct business (e.g. working off-line on a UHN business proposal). See definition for [remote access](#).

This material has been prepared solely for use at University Health Network (UHN). UHN accepts no responsibility for use of this material by any person or organization not associated with UHN. No part of this document may be reproduced in any form for publication without permission of UHN. A printed copy of this document may not reflect the current, electronic version on the UHN Intranet.

|               |   |                |  |
|---------------|---|----------------|--|
| Policy Number | <b>1.40.012</b>                                       | Original Date  | <b>01/03</b>   |
| Section       | <b>Privacy &amp; Information Security</b>             | Revision Dates | <b>06/07; 11/08; 09/10; 01/11; 04/19; 05/19; 03/22; 08/24; 06/25</b> |
| Issued By     | <b>UHN IT Executive Committee</b>                     | Review Dates   |  |
| Approved By   | <b>Vice-president &amp; Chief Information Officer</b> | Page           | <b>19 of 20</b>  |

## Appendix: Contact Information

| For questions related to:  | Contact:   |
|--|--|
| Access, use, disclosure, or destruction of PHI/PI                                | The Privacy Office: 416-340-4800 ext. 6937 (14-6937) or <a href="mailto:Privacy@uhn.ca">Privacy@uhn.ca</a> |
| Retention of medical records   | Health Record Services: <a href="mailto:healthrecordservices@uhn.ca">healthrecordservices@uhn.ca</a>       |
| Use of intranet, internet, and social media for UHN purposes and all user emails | Communications and Brand Strategy: 416-340-4636 (14-4636)  |
| General IT issues and requests   | Your local help desk   |
| This policy in general or the digital security of UHN information and IT assets  | Digital Security: <a href="mailto:digitalsecurity@uhn.ca">digitalsecurity@uhn.ca</a>                       |

This material has been prepared solely for use at University Health Network (UHN). UHN accepts no responsibility for use of this material by any person or organization not associated with UHN. No part of this document may be reproduced in any form for publication without permission of UHN. A printed copy of this document may not reflect the current, electronic version on the UHN Intranet.

|               |   |                |  |
|---------------|---|----------------|--|
| Policy Number | <b>1.40.012</b>                                       | Original Date  | <b>01/03</b>   |
| Section       | <b>Privacy &amp; Information Security</b>             | Revision Dates | <b>06/07; 11/08; 09/10; 01/11; 04/19; 05/19; 03/22; 08/24; 06/25</b> |
| Issued By     | <b>UHN IT Executive Committee</b>                     | Review Dates   |  |
| Approved By   | <b>Vice-president &amp; Chief Information Officer</b> | Page           | <b>20 of 20</b>  |