

Appendix B: Privacy and Security Checklist for Working Remotely

Version 1, published May 2020

The privacy of our patients' and residents' **personal health information (PHI)** must be maintained as much as possible when working remotely, outside of Unity Health's physical environments. In addition, you must take steps to ensure that other **corporate confidential information (CCI)** remains private and in Unity's control. Wherever it says PHI below, the same steps can be taken with CCI to protect it.


To ensure that you are compliant with Unity Health policies when working remotely, you must:

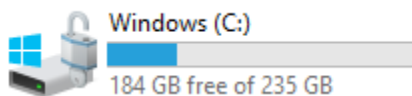
1. Recognize which of your devices are encrypted
2. Choose the right device, or the right tool, for the work that you are doing
3. Remember everyday security practices
4. Limit your use of paper and remember to secure it
5. Mind your physical and auditory surroundings
6. Report security incidents and privacy breaches

1. Recognize which of your devices are encrypted

Encryption protects the data stored on a device or passing through a device. Encryption is required on any device that stores PHI. Encryption converts information into unreadable content to hide the information's true meaning from unauthorized users. Users who are authorized to access the information, and have the encryption codes, will be able to see and to work with the information.

- To verify if your Unity Health-issued laptop is encrypted:

Open the "This PC"  icon, or open your Explorer icon, and ensure the C: drive has a lock on it like below:



- iPads and iPhones get encrypted when a passcode has been generated to login or "unlock" the device.
- MaaS360 is an encryption program that creates a secure 'container' on a user's device to allow users to read and write emails, and view attachments, without the email being saved to the device itself.
- To verify that encryption is in place on most smartphones go to Settings --> Touch ID & Passcode --> Enter the device passcode --> Scroll to the bottom and it should read "Data Protection Enabled".
- To tell if your device issued by another hospital is encrypted, contact the hospital that issued the device.

2. Choose the right device, or the right tool, for the work that you are doing

- Choose encrypted devices (phone, computer or tablet) and locations (e.g. network folders, approved systems) to view, create or store PHI:
 - Always use an **encrypted device** for Unity Health-related work.
 - An encrypted, Unity Health-issued device is preferred.
 - If you do not have an encrypted, Unity Health-issued device, you may temporarily use a device issued by another hospital that you know is encrypted.
 - Email and network folders can be accessed by logging onto the network remotely from your site's website or by using a secure VPN token.
 - Always store PHI in a clinical system (e.g. Meditech, Soarian), a designated administrative system (e.g. Safety First), or a personal or shared network folder that you commonly use for your work.
 - If neither saving in a clinical system, an administrative system, or to a network drive is possible, files containing PHI may be stored, temporarily, on encrypted devices. Only the minimum amount of information that is needed may be stored on a device.
 - If no encrypted device is available, you may not store PHI to the device.
 - Remember: Any and all temporary or permanent documents, in any format (e.g. Excel files, Word documents, Notepad files, EMR reports, Safety First reports), that identify a patient count as PHI.

- Accessing email:
 - Use your Unity Health email account for all work-related activity.
 - If you are using a Unity Health-issued or other hospital-issued encrypted device, you can use webmail (i.e. signing in through OWA directly) or access your email by signing into the network directly (angel at St. Michael's) or with a security token for all three sites.
 - If you are using an unencrypted personal device, that does not have MaaS360, you should log into the network to access email, if you need to view, save, change, or upload any attachments.
 - Remember: Simply opening (viewing) an email attachment means that the attachment is downloaded and saved on the device. Attachments containing PHI must not be opened or saved on unencrypted personal devices. If an attachment is inadvertently opened on an unencrypted device, delete the downloaded file and empty the trash.

- Making telephone calls:
 - Submit a [ShopIT request](#) to have your onsite phone extension converted to a mobile number, which can be accessed through a tool called Jabber. This means that you can send and receive calls on your device, through Jabber, as if you were using your office phone.
 - If you are using a phone with a number that you do not want displayed to the person you are calling, you may be able to block the display of your personal number when making outbound calls, by disabling "show my caller ID" on some smartphones or checking with your phone provider for instructions on how to block your number.
 - Unencrypted personal phones can be used to make phone calls, as long as phone numbers for patients are deleted from the call log immediately after the call.

- Messaging and texting:
 - Only approved messaging apps (i.e. SPOK) may be used to transmit PHI.
 - SMS, WhatsApp, Facebook messenger, Jabber instant messaging, Slack, and other free/online tools may not be used to transmit PHI, whether encrypted or non-encrypted devices are used.

- Phone/video conferencing:
 - Conference calls (using your phone’s tools or using Jabber) are secure and can be used to discuss PHI, as long as all callers are permitted to hear the PHI (i.e. in the “circle of care”).
 - Video/web conferencing (Cisco, Zoom) may be used to discuss PHI or for other confidential conversations.
 - Please to go <http://remote.unityhealth.to/howto/> for more information.

3. Remember everyday security practices

- Limit the use of hospital-issued devices for personal use.
- Be diligent when using email, as there is an increase in cyberattacks and phishing emails circulating - contact Help Desk to report a suspected phishing email.
- Use a private internet or Wi-Fi connection (i.e. your home’s password protected internet connection or personal Hotspot). Never use public Wi-Fi or another unsecured internet connection to access Unity Health Toronto resources, including remote access to clinical systems and network folders, as well as webmail.
- Always use your own credentials (username and password) when logging in and don’t share your credentials with others. Don’t write passwords in places where others in the home could see them.
- Log out of, or lock, devices when not in use to ensure that another person can’t use it.

4. Limit your use of paper and remember to secure it

- Do not remove original paper documents, containing PHI, from Unity Health premises unless absolutely necessary to continue your work.
- Only print documents that contain PHI or other confidential information, if necessary.
- Lock up all papers with PHI (printed or hand-written) when not in use or when leaving them unattended, and do not lock papers or devices in a vehicle.
- When papers are no longer needed, cross-cut paper (to a size of 3/8” x 1/2” maximum), return papers for shredding, or mail paper documents with clinically-relevant PHI for entry into the patient’s chart:

Send documentation via interoffice mail or drop off at St. Joseph’s Health Records, Ground Floor, Morrow Wing	Send documentation via interoffice mail or drop off at St. Michael’s Health Records, 1 st floor, Donnelly Wing	Send documentation via interoffice mail or drop off at Providence Health Information Management, A127
St. Joseph’s Health Centre Health Records Department 30 The Queensway Toronto, ON M6R 1B5	St. Michael’s Hospital Health Records Department 30 Bond St. Toronto ON M5B 1W8	Providence Healthcare Health Information Management 3276 St. Clair Avenue East Toronto, ON M1L 1W1

5. Mind your physical and auditory surroundings

- Position yourself so that others cannot overhear your conversations.
- Position yourself so that others cannot read over your shoulder.
- If using a monitor or smart TV to project or extend your laptop screen, ensure that PHI will not be displayed to others in the area.

6. Report security incidents and privacy breaches

- Notify your supervisor immediately if there is potential that PHI may be compromised by reporting lost or stolen passwords, devices or papers.
- Contact the Help Desk to report lost or stolen devices.
- Report all privacy breaches to the privacy office at privacy@unityhealth.to

Questions?

Check the privacy and security policies on your site intranet.

To ask a privacy question or report a privacy breach, contact the Privacy Office at 416-864-6088 or privacy@unityhealth.to

If you suspect a phishing email, contact the Help Desk.

If your device is lost or stolen, contact the Help Desk, who can help wipe files from Unity Health-issued devices.

What is personal health information (PHI)?

Personal health information (PHI) includes any information that identifies a person and relates to their health or to the provision of care, treatment or assessment for that individual.

PHI can exist in any form (oral, written, or electronic). Any information that is not explicitly related to health is also PHI, if it is contained in a record of PHI. Examples of PHI and records of PHI include: a paper record of treatment in a physician's office, an electronic record of all diagnostic tests performed on a patient, a faxed referral for a patient, an email discussing the Power of Attorney for a named client.

PHI includes, but is not limited to:

- information relating to the physical or mental health of the individual, including the individual's medical history and the individual's family medical history;
- information relating to the providing of health care to the individual, including the identification of a person as a provider of health care to the individual;
- information relating to the payment or eligibility for health care;
- information relating to the donation by the individual of any body part or bodily substance of the individual or is derived from the testing or examination of any such body part or bodily substance;
- the individual's health care number; or
- information that identifies an individual's substitute decision-maker.

What is corporate confidential information (CCI)?

Corporate confidential information is any information related to Unity that is not publicly available. This includes, draft documents (i.e., a policy), human resource information, billing and financial information, etc.

I, the employee, have reviewed this Privacy and Security Checklist. I understand and agree to abide by the requirements in this document.

Employee's Signature		Manager's Signature	
Employee's Name (Please print)		Manager's Name (Please print)	
Date		Date	