How to Protect your Health Information Online

UHN

Information for patients using myUHN Patient Portal

It's important to do all you can to keep your personal health information safe online. This will help prevent other people from using or seeing your information without your permission.

Read this information to learn about:

- how to protect your personal health information
- websites where you can learn more about online safety

Patient Education
Improving health through education

Author: Greg Yhan, Manager of Information and Security and the myUHN Patient Portal Team
Revised: 07/2017
Form: D-8540

UHN
Toronto General
Toronto Western
Princess Margaret
Toronto Rehab

Use these simple tips to make sure your information is safe:

☑ Keep your personal information private.

Don't give out personal information on the phone, by email or online unless you know who the person is and why they need to know the information.

☑ Keep your password private.

- Never save your password on a public computer, such as a computer at an Internet café or public library.
- Change your password after using a public computer.
- Don't share your password with others.

☑ Choose passwords that are hard for others to guess but easy for you to remember.

- Use passwords that have a mix of letters and numbers. Use both small and capital letters.
- Don't use your first or last name in your password to make it harder to guess.

☑ Protect your information in public.

- Make sure no one is looking over your shoulder. Do this when you use any device (including your phone or tablet) in a public place.
- Avoid using public computers to access private information. If you do need to use one, then:
    - Always 'Sign out' of your account before closing the browser. Do this even if you have to step away from the computer for a minute.
    - Delete your browser history before you leave the computer. This erases any records of websites you visited. It also erases your passwords or other information you entered. Click here to learn how.
    - Keep your password private by changing it after using a public computer.

☑ Install security updates.

Most personal computers use Microsoft Windows and Apple MacOS operating systems. The makers of these systems regularly send security updates. These updates help keep your computer safe from threats to your privacy.

Set up your operating system to automatically check for new updates. Or, download and install security updates often. To learn how, go to:

Microsoft:
💻Website: http://windows.microsoft.com/en-us/windows/is-computer-up-to-date#1TC=windows-7

Apple:
💻Website: https://support.apple.com/en-ca/HT201541

☑ Use anti-virus software.

Anti-virus software helps prevent viruses from infecting your computer. A virus can affect how your computer works and cause you to lose information. Anti-virus software can find and remove viruses on your computer.

Viruses can come from email attachments and websites, or CD-ROMs, DVDs, or USB drives you connect to your computer.

To protect your computer from viruses:

- Use up-to-date anti-virus software from a company that is reliable and has good customer reviews. Some examples of reliable anti-virus software companies include:
  - AVG®
  - Free Charity Antivirus®
  - My Free Antivirus®
  - McAfee®
  - Norton®
  - Prevention®
- Register new anti-virus software right away. Sign up for automatic notices about software updates, if available.

- Use anti-virus software that can download profiles of new viruses, so it can check for them as soon as they are found.

☑ Prevent spyware downloads.

Spyware is software that spies on you. It tracks what you do on your computer without your permission. It can track the websites you visit. It can also track what you type in your computer, such as your card numbers, account numbers and passwords. In serious cases, people called **identity thieves** can use this information to illegally look at or use your private accounts.

Spyware can be downloaded onto your computer without you knowing it. Be careful before installing software that offers free email virus protection or faster Internet service. These are common ways that spyware is downloaded. Make sure you run basic checks on software before downloading or installing it:

1. Download software from the company who made it. They will have the latest and safest version of the software.
2. Your anti-virus software will check any software you download as it is downloading. But before you open the software, have your anti-virus scan it one more time.

To prevent a spyware download:

- Read customer reviews of software before downloading it.
- Never install a program unless you are sure it is from a website or publisher you can trust.
- Always run a virus scan on your download.

To remove spyware from your computer:

- Your anti-virus software can help you find spyware, stop it from being installed or remove it. Uninstall it as soon as you find out it has been downloaded.

☑ Don’t be fooled by phishing.

Phishing is when people use fake emails, web pages, text messages and pop-up windows to steal information. This can include passwords, social insurance numbers, credit card and bank account numbers. Often, these emails, web pages and text messages seem to come from well-known organizations. So, it’s easy to be tricked into providing personal information.

Change your passwords right away if you think you are a victim of a phishing attack. If you are using the same password for more than one account, change all of your passwords.

University Health Network (UHN) does not send email or text messages:

- asking patients to provide, confirm or update personal records
- from an address that is not from UHN or that have links to websites not made by UHN
- with no information about why a patient is receiving the email
- asking patients to respond quickly

☑ Be careful when sharing access to your myUHN account.

A shared access user is someone you invite to see your personal health information on myUHN. Before inviting someone to see your personal health information, think about:

- Will this person have my best interests in mind?
- What type of information do I want to share?
- Does this person need to see all of my personal health information?

Look at your list of shared access users often to decide if you still need to share information with them.

Where can I find more information?

If you would like more information about how to protect your personal information online, go to:

Government of Canada – Get cyber safe: Cyber security risks
💻Website: www.getcybersafe.gc.ca/cnt/rsks/Cmmn-thrts-eng.aspx#s05

Province of Ontario – How to avoid and recover from identity theft
💻Website: www.ontario.ca/law-and-safety/how-avoid-or-recover-identity-theft

United States Computer Emergency Readiness Team (US-Cert)
💻Website: www.us-cert.gov/ncas/tips