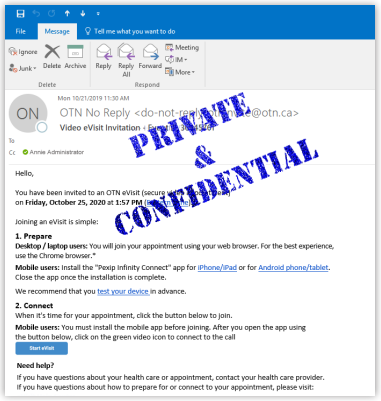
Video Visit Privacy and Security

Understand the Risks of Using Email

Today, most emails you send are not encrypted and their security can never be 100% guaranteed. For example, if you leverage a popular web based email client, such as Gmail, those emails are not encrypted once sent. As a result, communicating with patients over email poses several risks.



These risks include the following:

- Email can be forwarded, intercepted, circulated, stored or even changed without the knowledge or permission of the Physician or the patient.
- Email senders can easily incorrectly address an email, resulting in it being sent to unintended and unknown recipients.
- Email is indelible. Even after the sender and recipient have deleted their copies of the email, back-up copies may exist on a computer or in cyberspace.
- Emails may be subject to review by Third Parties (*e.g.*, law enforcement), or in the context of an access request, litigation, or Privacy Commissioner or College investigation.
- The email address that patients provide to their physicians (personal or business) carries with it certain risks as outlined below:
  - **Personal** - The content of personal emails sent to web mail addresses (*e.g.*, Gmail, Yahoo, MSN Live Outlook) are routinely scanned by the web mail providers to enable targeted advertising to email users.
  - **Business** - Use of business email address is considered the "Property" of an Organization/Employer, and subject to review by them. When using an Employer's or a Third Party's email system (e.g., Hospitals and Clinics), these Parties may have the right to access the email communications.

eVisit (Videoconference) OTNinvite

The OTNinvite feature is designed to mitigate the risks of communicating via email. The invitation email content has been carefully reviewed to ensure the privacy and security of the communications. Some of the email safeguards include:

1. Emails generated from the OTNhub do not contain any identifiable information (such as the physician's or the clinic's name or email), which may be considered PHI in the context of a clinical event.
2. Users are asked to confirm the name and email address when emails are generated from the OTNhub.
3. PIN information is never included in the email notification for clinical events. (This means that an intercepted email will not include enough information for a third party to join an event protected by a PIN.) The videoconference organizer can provide the PIN to an invitee during their initial consultation or over the phone.

Follow Best Practices...

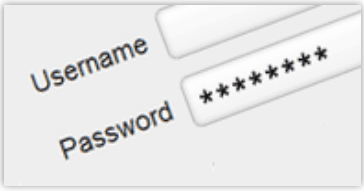
When receiving your invitation email

- Do not share the invitation email, invitation link URL or PIN with anyone.
- Enter a name when you log in so that other participants know that you have joined the videoconference and they will see a meaningful label with your video image.
- When receiving an email invite, make sure that it originates from the following address: do-not-reply-otninvite@otn.ca
- Do not open any attachments. A videoconference email invitation from OTN will never contain any attachments. If an attachment is present in the email, it is most likely spoofed and did not come from OTN.
- Do not reply to the invitation email. The email will never ask you to disclose any personal or sensitive information.
- Before clicking on the provided videoconference link, make sure to read the target address by hovering your mouse pointer over the link. If it is not pointing to an otn.ca website, do not click on the link.

When using your computer, videoconferencing, and emailing

- Before sending an email, check the recipient's address for accuracy and any spelling mistakes. This will ensure that the email is sent to the intended recipient.
- Be aware of your surroundings. Never use eVisit or virtual care technology in a public or unsecure environment (e.g., an airport, internet café or open area).

- Be mindful of the prevalence of malware and malicious applications. Ensure your computer is secure with anti-spyware, anti-virus protection and an auto-lock screen saver.
- Do not use the "Remember Me" function on a login page. (Clear your user name and password when you sign out.)
- Ensure your computer (desktop, laptop, tablet or phone) is password protected and follow these best practices around password use:
  - Change passwords with access to confidential information regularly (*e.g.*, every six months).
  - Do not share your credentials (*i.e.*, User ID and password) with anyone, including trusted colleagues, family members, and support technicians.
  - Do not write down your password and then store it where it is easy to find.
  - Do not use the same password for all applications. Passwords used to access confidential information require stronger protection and hence should not be used on potentially insecure sites where it can be stolen.



Need Help?

Contact OTN Technical Support: **1-855-654-0888**