



# ELECTRONIC COMMUNICATION

## PRIVACY & SECURITY BEST PRACTICES

OCT 27, 2020

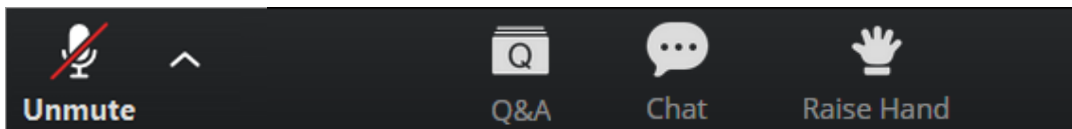
Doctors Technology Office

# Housekeeping:

## Control Panel:

By default the control panel is set to auto-hide.

By moving your cursor to the bottom of the screen the control panel will appear. The control panel includes the mute, chat, raise hand and Q&A functions.



**Mute:** By default, you will be put on Mute when you join the Webinar.



## Hand raising:

The hand raising feature is found on the middle of the Zoom control panel.

By default, your hand will not be raised.

When your hand is down, the button look like this:



Click on the button to raise your hand if you have a question or a comment.

When your hand is raised the button looks like this:



Click on the button to lower your hand if your question or comment has been addressed.

# INTRODUCTIONS

## FACILITATOR

- Kaitlyn Shaw, Manager, Doctors Technology Office, Doctors of BC

## PANELISTS

- Mauree Aki Matsusaka, Health Technology Advisor Doctors Technology Office, Doctors of BC
- Dr. Liisa Honey, MD, FRCSC, Physician Advisor, Practice Improvement, CMPA
- Derek Puddester, MD, MEd, FRCPC, Deputy Registrar, College of Physicians and Surgeons of BC

# CONFLICT OF INTEREST DECLARATION

- Each organization is vendor-neutral and does not endorse any specific tools.
- No conflicts of interest to declare from any of the panelists

# OUTLINE

- Privacy & Security in the time of COVID-19
- Best Practices for Electronic Communication
- Selecting the Right eCommunication Tools
- Additional Resources
- Questions

# LEARNING OBJECTIVES

At the end of this one-hour webinar and interactive panel discussion, participants will be able to:

- Define minimum provincial requirements for engaging in electronic communication with patients
- Define common guidelines around obtaining and documenting informed consent for electronic communication with patients
- Apply best practices for how and when to communicate electronically with patients using commonly used tools (i.e. virtual care, text, email, other)

# PRIVACY & SECURITY IN THE TIME OF COVID-19

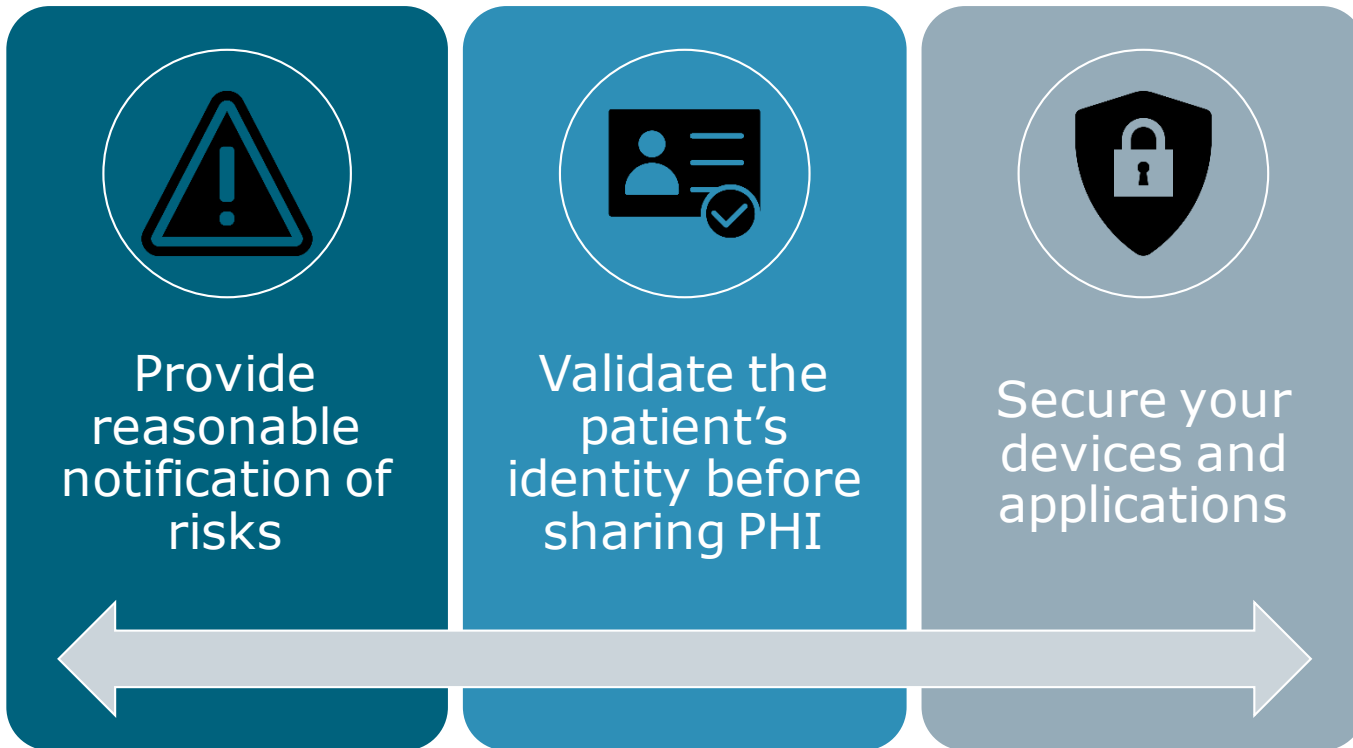
- Clinics have rapidly adopted virtual care/eCommunication to continue delivery of care
- Focus on healthcare delivery – meeting patient where they are at
- Professional obligation to implement security safeguards and protect patient confidentiality remains



It is important to recognize that security relies on **small, everyday acts** and awareness from each team member.

# PROVINCIAL DIGITAL COMMUNICATION POLICY REQUIREMENTS

Under the *Provincial Digital Communications Policy*, verbal or digital consent from the patient is acceptable before use of all Virtual Health solutions; however, the key requirements are:





# WHAT IS INFORMED CONSENT?

Informed consent may involve the following components:

- explain the risks and privacy issues related to electronic communication
- explain steps patients can take to protect their information
- explain how their information will be used in the delivery of care
- ensure that patients fully understand the risks and can ask questions/express concerns before consenting

Informed consent is a process that takes place between provider and patient. A signature on a form is secondary.

# DOCUMENTING PATIENT CONSENT

Refer to [DTO Virtual Care Toolkit](#):

- **Consent can be documented various ways:**
  - Physically and/or electronically signed form
  - Document that you have had a verbal conversation with the patient in your EMR
  
- **Consent** only needs to be documented once, unless info will be used for a new purpose. No need to ask every time.
  
- The patient should be able to **retract consent at any time** or share questions or concerns with their provider OR the clinic Privacy Officer as needed

# PROTECTING PATIENT INFORMATION



When using devices to communicate with patients, providers must make reasonable security arrangements to protect patient confidentiality.

- Providers are to restrict disclosure of personal information to what is relevant and necessary for the purpose of the communication on **“need to know” basis.**
- If the info you are communicating is of a sensitive nature, **seek a more secure method of communication.**
- **Delete emails, images and documents when purpose is fulfilled**

# TIPS FOR SECURING MOBILE DEVICES

- **Keep software, OS, apps and anti-virus/malware protection up-to-date**
- **Avoid sending personal information while using public Wi-Fi.** If unavoidable, consider using a VPN (virtual private network) or tools with end-to-end encryption.
- **Enable auto-lock and 'find my phone' app**
- Use your device settings to **control what data your Apps have permission to access**
- **Download apps from trusted sources**



# **SELECTING THE RIGHT eCOMMUNICATION TOOLS**

# SELECTING SECURE TOOLS

Tools with end-to-end encryption should be used whenever you are sharing private health information electronically.

## Best Practices for Selecting Secure Solutions

- Avoid using consumer products (i.e. Gmail, Telus) for sending PHI as many are **not encrypted by default**
- Consider working closely with your vendor to **ensure that your app security settings and configuration is customized for healthcare use**
- Ideally, select tools that host or **route data solely via Canadian servers**
- Check with your health authority to see **what tools are appropriate to use**

# EMAIL



## BEST USED FOR

- Content that should be saved for future reference/record
- Appointment reminders, follow ups, check-ins, brief status updates
- Providing directions or timely information i.e. educational material, links or lab requisitions etc.

## RISKS/LIMITATIONS

- Unsecured emails could be sent to wrong patient or intercepted
- No analytics
- No control over how long patient retains email or documents

**Privacy Tip:** Send an initial email to validate the patient's contact before sharing private info or documents.

# TEXT MESSAGING



## BEST USED FOR

- Quick check-ins or follow up
- Appointment reminders
- Educational information exchange

**Privacy Tip:** Most secure text messaging tools require both sender and receiver to use same application for end-to-end encryption

## RISKS/LIMITATIONS

- Patients would have your phone # to call you directly
- No guarantee correct patient will receive/respond to messages
- Most tools not encrypted
- Difficult to document messages in EMR
- No control on when/if texts are deleted



# OTHER eCOMMUNICATION OPTIONS

- **Websites:** Your clinic website can be used to share clinic location & hours, appointment scheduling, clinic notices etc.
- **Secure Patient Portal:** Contact your EMR to determine whether they offer secure patient portals or integrated messaging services.
- **Managed File Transfer (MFT):** This option allows you to use existing tools such as Outlook or secure portals to facilitate file transfer with patients/health professionals.

Please contact [DTOinfo@doctorsofbc.ca](mailto:DTOinfo@doctorsofbc.ca) for assistance with navigating your health technology options.



# VIRTUAL CARE/VIDEOCONFERENCING

## BEST USED FOR

- One-on-one or group virtual care visits, either scheduled or on-demand
- Providing webinars or group education sessions i.e. diabetes
- Providing video consultations, virtual exams, directions or timely information
- Collaborating with other care providers

## RISKS/LIMITATIONS

- Potential of sharing meeting invite with wrong contact
- Inability to control whether patient joins from a secure device or confidential location
- Bandwidth: poor network connection can impair audio/visual quality

# SCENARIO

16 year old female schedules a follow up call for renewal of oral contraceptive and acne medication. She appears sullen, not quite her usual self. There appears to be circular and dark discolouration on her right cheek. She keeps looking off-screen quickly, then down.

You ask if she is alone and she says yes, quickly and forcefully. You pause, ask if there is anything else she would like to discuss. She says no, asks you to fax the renewals to her pharmacy and hangs up.

# SCENARIO

78 yo male with multiple health issues (COPD, cardiomyopathy, recurrent depression) and prescribed 5+ medications is due for regular follow-up. His 12 year-old granddaughter helps with the telehealth connection. He is increasingly irritated with the experience - he can't hear the physician well, has concerns increasing dizziness and the granddaughter says he fell this morning.

After a few questions, he states he isn't understanding the questions and doesn't understand why he can't be seen in person. After all, his daughter can get her nails done in a salon and his son sees his physiotherapist weekly. He slams the laptop shut in frustration.

# ADDITIONAL RESOURCES

- [PHSA Office of Virtual Health COVID-19 Accessible Solution Toolkit](#)
- [Provincial Patient and Care Team Digital Communications Policy](#)

## Doctors Technology Office

- [Physician Office IT Security Guide](#)
  - [Virtual Care Quick Start Guide & Toolkit](#);
  - [Getting Patients Back to Practice Guide](#)
  - [DTO YouTube page- Virtual Care Learning Series](#)
  - [Virtual care FAQ for physicians and MOAs](#)
- 1-on-1 support/coaching via Physician/MOA peer mentors or Health Technology Advisors – email [DTOinfo@doctorsofbc.ca](mailto:DTOinfo@doctorsofbc.ca)

# ADDITIONAL RESOURCES

## College of Physicians And Surgeons of BC

- Telemedicine
- Medical Records, Data Stewardship and Confidentiality of Personal Health Information
- Photographic, Video and Audio Recording of Patients
- Social Media

## Canadian Medical Protective Association

- Using electronic communications, protecting privacy
- Telehealth and virtual care

## Office of Information and Privacy Commissioner of BC

- Contemplating a Bring your Own Device (BYOD) Program? Consider these tips
- Protecting Personal Information Away from the Office

# QUESTIONS & FEEDBACK

For more information on resources and workshops, contact us:

**Doctors Technology Office**

[dtinfo@doctorsofbc.ca](mailto:dtinfo@doctorsofbc.ca) or call us at 604-638-5841