PRIVACY & SECURITY TRAINING

OntarioMD

8 Essential Steps for Cybersecurity Success

1. Establish your practice and determine technology needs

- Select and implement a certified electronic medical record (EMR) if you don't already have one
- Consider your and colleagues' record-keeping and technology needs: EMRs, email, verified virtual visit solutions, mobile applications, etc.
- If sharing an EMR, establish a written agreement that sets out custodianship and accountabilities for medical records (per CPSO) (e.g., data sharing agreement)
- Do not use personal email or public computers to communicate with patients

2. Develop privacy and security policies and procedures

- Appoint a practice Privacy Officer (solo practitioners are their own Privacy Officers)
- Establish a Privacy Policy, which includes:
  - collection, use, and disclosure of personal health information through virtual care (including communications by email);
  - the identity and contact details for your Privacy Officer; and
  - instructions for reporting complaints/breaches to the Ontario Information and Privacy Commissioner

3. Use complex passwords and multi-factor authentication

Effective password controls

- Create different, complex passwords for each account
  - alphanumeric phrases (e.g., 1Lik3p1zz4!" = I like Pizza!)
  - combination of numbers, special characters, and capital letters; longer is better
- If necessary, use a secure password manager (or "keychain")
- Store written passwords in a secure location
- Change passwords regularly and do not re-use old passwords

Multi-factor authentication methods

- Security questions, PIN, texted codes, authentication apps, fingerprint, biometrics, voice recognition

4. Regularly update software and hardware

Effective password controls

- Apply security patches for software and hardware
- Enable automatic updates whenever possible
- Replace out-dated systems or applications that are no longer supported

5. Implement security software

Preventive action

- Install anti-virus or anti-malware software to help detect, prevent, and remove malware (malicious software)
- Enable automatic updates for security software to ensure your devices are safe from exploitation through holes in your security
- Install a DNS (Domain Name System) Firewall Network Protection to monitor and filter incoming and outgoing network traffic and protect you from attackers
- Use a virtual private network (VPN) to encrypt your data and make it impossible for cybercriminals to read

6. Consistently back up data

Methods to prevent data loss

- Identify software and information essential to your organization
- Regularly back up systems with essential information
- Test your back up and recovery process to ensure it works
- Store back-ups in a secure location

7. Establish an incident and breach response plan

- Create an **Incident Response Policy** that outlines:
    - how often you will back up information and systems
    - how your organization will respond to different levels of incidents
    - who is responsible for handling incidents (i.e., internal teams or service providers)
    - contact information for people who are part of your incident response team and are accessible
    - a privacy breach protocol

8. Participate in cybersecurity training and education

Cybersecurity for health care

- Training and education are the best ways to combat cybersecurity attacks
- OntarioMD offers a privacy and security training module to educate you and your staff on the best cybersecurity practices for the health care space

If you have any questions about protecting your practice from cybersecurity attacks, OntarioMD can help. **Contact support@ontariomd.com for advice and tips.**

OntarioMD.ca

OntarioMD OntarioMD @OntarioEMRs OntarioMD OntarioMD ontariomd.blog

The views expressed in this publication are the views of OntarioMD and do not necessarily reflect those of the Province.