Protecting patient data in a virtual world:

how to help safeguard health data from cybercriminals

by Ariane Siegel
General Counsel & Chief Privacy Officer, OntarioMD

Cybercriminals are targeting hospitals and health care providers with malicious ransomware attacks that are resulting in data theft and disrupted patient services, which is particularly alarming as cases of COVID-19 are spiking.

Health care providers are also increasingly reliant on digital information systems, and where virtual care is the new normal for physicians, they should exercise caution and follow best practices to protect personal health information (PHI). Implementing the latest privacy and security measures also help to protect providers against liability.

In Ontario, help is available through OntarioMD, a subsidiary of the OMA. OntarioMD has developed tools and resources to help you assess threats, actively safeguard information and respond to cyberattacks.

That's important, because sensitive health care information is being increasingly targeted.

In December 2019, LifeLabs, Canada's largest medical testing company, revealed that hackers had accessed the personal health information of 15 million patients in Ontario and B.C. and that it had paid a ransom to recover the data.

Around the same time, hackers effectively shut down the computer systems of three Ontario hospitals, forcing employees to transcribe patient information onto paper by hand as email systems were taken offline, health care records became harder to access, and patient care was slowed down.

In this situation, malware struck a laptop, and was able to spread to the entire network. Although the hackers boasted they had easily penetrated the hospital grid after finding a significant hole in the security system, CEO Sarah Downey of Toronto's Michael Garron Hospital said a firewall picked up the malware before the data could leave the hospital.

While these examples are specific to large companies and hospitals, smaller physician practices are confronting the threat of malware such as ransomware.

Physicians in Ontario are encouraged to use electronic medical record (EMR) systems certified by OntarioMD. Certified EMRs are designed based on requirements and standards for privacy and security of patient data. To complement certified EMRs, OntarioMD staff are available to help evaluate and advise on firewalls, software and services that can be put in place to provide additional safeguards.

Ontario's Privacy Commissioner has said that physicians in this province have a duty to be trained in privacy and security issues, and that training should be extended to their support staff. OntarioMD has addressed this need by offering an education tool to help health care providers and support staff learn how to keep patient and practice information confidential.

The OntarioMD online Privacy & Security Training Module is available 24/7 at OntarioMD.ca. The module is accredited by the College of Family Physicians of Canada's Ontario Chapter for two Mainpro+® credits and goes a long way to educate you and your staff on your legal obligations under the Personal Health Information Protection Act, and provides sound advice for protecting the physical assets in your office as well as your electronic data.

> Physicians in Ontario are encouraged to use electronic medical record (EMR) systems certified by OntarioMD.

To date, approximately 4,000 users have benefited from the online training that covers a range of topics from best practices for safeguarding a patient's personal health information, establishing practice policies and protocols for use of digital health tools, patient consent, and responding to privacy breaches and incidents such as ransomware attacks. A range of bulletins and information on steps to help keep data secure is also available in the "Resource Library" on OntarioMD.ca.

Since the adoption of virtual care tools by many physician practices, OntarioMD, together with the Ontario Medical Association, has also developed consent language that can be copied and used in communications with patients before a virtual encounter.

If you believe a breach has occurred, OntarioMD IT staff can help assess the threat and can recommend steps to keep your information safe, by suspending feeds from external digital health assets to your practice if the threat originated from an outside source such as a hospital.

OntarioMD recommends that you and your staff who access provincial digital health assets such as ConnectingOntario ClinicalViewer, Health Report Manager (HRM®), eNotifications, eConsult, and Ontario Laboratories Information System (OLIS) complete the Privacy & Security Training Module once a year to refresh your understanding of the best practices and to learn about new developments.

Digital health care is always evolving, and to help protect you as you navigate the world of virtual care, OntarioMD updates its training to address a broader set of potential issues as more and more physicians go online as part of their practice.

Some practical tips for data protection include:

- Delete emails and any images with PHI from inboxes and device trash bins.
- Ensure software and hardware applications have been updated with the latest security patches (i.e., operating system, firewalls, etc.).
- Encrypt critical data at rest when stored internally, and in transit when communicated externally.
- Transmit personal health information through secure messaging to ensure messages are encrypted.
- Use two-factor authentication and change passwords regularly.
- Maintain audit logs.
- Work with your EMR vendor to ensure data is backed up, and conduct tests to ensure that backup systems are working.

OMA Cyber Liability Insurance is also available through OMAInsurance.com as added protection, and the OMA Legal & Governance teams can provide timely assistance and information to members regarding patient data-related queries.

Health care providers are a target because they have large amounts of confidential and valuable information. OntarioMD invites you to connect with us about our many resources, products and knowledge at support@ontariomd.com. OMA Legal support is also available at info@oma.org. ■

Virtual Care and Cybersecurity Resources for Physicians

Best Practices Around Virtual Care

- The OMA continues to receive questions about best practices around virtual care. We have developed resources and information about expanded access to virtual care in the context of COVID-19, including information about billing codes. View the OMA virtual care web page at **www.oma.org/virtualcare**.
- OntarioMD has also compiled a list of vendors with virtual care products, including your EMR vendor, as well as other resources to help you understand how your colleagues are using virtual tools in their practices. View the OntarioMD virtual care web page at **ontariomd.vc**.

Cybersecurity Information and Privacy & Security Training

- Cybercrime is evolving quickly and affects many areas of our daily interactions. Cyberattacks continue to grow and put everyone at higher risk, which requires us to become more vigilant and familiar with IT security. Given the increased use of technology during COVID-19, the OMA has provided cybersecurity information for all members on our website at **content.oma.org/cybersecurity**. This page will be updated regularly with information on cybersecurity issues that may affect you.
- OntarioMD offers a comprehensive Privacy & Security Training Module to help support the use of digital health tools in the medical practice. The module can be completed any time, and is available free of charge to physicians and their staff. OntarioMD also offers a range of bulletins and information on keeping patient data secure. The need for this training and information is more important than ever, so visit **ontariomd.ca** today! ■