Ransomware and Cyber Threats Continue to Target the Healthcare Sector

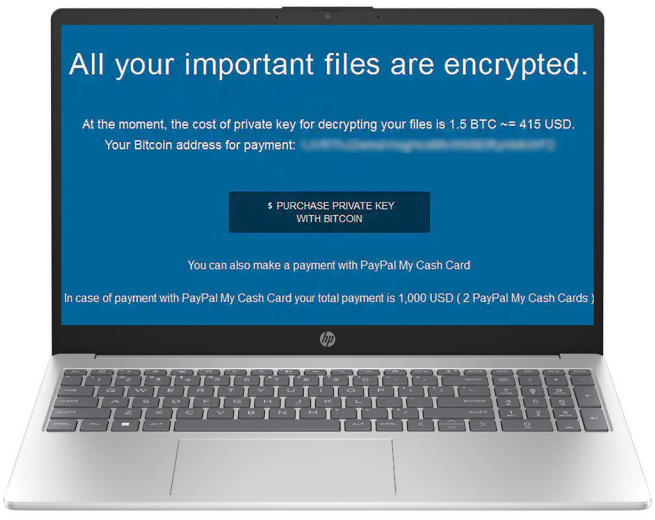
Ransomware has become more sophisticated and organized

Cybercriminals continue to target healthcare professionals and organizations on a regular and increasing basis. This trend is not surprising when one considers that electronic medical records (EMRs) contain valuable personal health information (PHI) and personal information (PI), making them attractive targets for cybercriminals. Ontario's digital health ecosystem now supports billions of medical records and enables clinicians to access patient information across the province, making cybersecurity essential to protecting patient care and maintaining trust in digital health services.

Cybercriminals seek to steal information for identity theft, financial fraud, extortion, or to gain unauthorized access to healthcare systems through phishing or other social engineering attacks. Modern ransomware attacks often involve both the theft of sensitive information and the encryption of systems, allowing attackers to demand payment, not only for restoring access, but also to prevent the public release of stolen information. Increasingly, attackers use artificial intelligence (AI) to create convincing phishing emails, text messages, and voice calls that are difficult to distinguish from legitimate communications.

What is ransomware?

Ransomware is a form of malware or malicious software distinct from other malware. Ransomware is most often triggered by a phishing email attachment, compromised password, malicious links, exploitation of unpatched software, vulnerable remote access services, or compromised third-party vendors. Once inside a network, attackers may steal sensitive information before encrypting systems and demanding payment. This is known as 'double extortion', which is becoming increasingly the norm. Attackers steal the data before encrypting it, then threaten to publish or sell it even if you restore the data from back-up and never pay. This means restoring data from back-up no longer fully resolves an incident; you must also investigate whether data was copied out.



Indicators of a ransomware attack could include:

- A user's realization that a link that was clicked on, a file attachment opened, or a website visited, may have been malicious;
- An increase in activity in the central processing unit (CPU) of a computer and disk activity for no apparent reason (due to the ransomware searching for, encrypting and removing data files);
- An inability to access certain files as the ransomware encrypts, deletes and renames and/or relocates data;
- Detection of suspicious network communications between the ransomware and the attackers' command and control server(s). IT personnel would most likely detect it via an intrusion detection or similar solution;
- Unexpected multi-factor authentication (MFA) prompts that you did not initiate;
- Reports of unusual activity or logins from unfamiliar locations;
- Files that appear to have been copied or transferred before systems become encrypted.

How can you protect your patient data?

- Limit direct server access to system administrators. Users should only access workstations for daily use of their EMR.
- All workstations and mobile devices should have endpoint protection, anti-malware software, security monitoring, and operating system updates applied promptly.
- Minimize the number of people with system administrative privileges. It is particularly damaging if administrator account information is stolen.
- Use strong unique passwords for every account and enable MFA wherever available. Consider using a password manager to securely generate and store passwords.
- Ensure your information technology provider has back-ups scheduled for your data with appropriate frequency, and that the back-ups are tested regularly for consistency.

.

What to do if you have been hit with ransomware?

If ransomware is suspected, immediately disconnect affected computers or devices from the network (without powering them off unless directed by IT), notify your organization's IT support, Privacy Officer, or designated cybersecurity contact, and contact your EMR vendor and your OntarioMD Practice Advisor, if applicable. Prompt reporting may help limit the spread of the attack and preserve evidence for investigation.

Once your IT provider is engaged, they will help determine the extent of the impact. Generally, the most complete way to remedy the situation is to restore data from back-ups prior to the ransomware attack. The appropriate local administrator should also convene an investigation team encompassing health IT professionals and clinicians to identify the root cause and establish processes for preventing and mitigating future incidents. Organizations should also assess whether there is any effect on patient care, activate business continuity plans where necessary, and determine whether the incident triggers obligations under the *Personal Health Information Protection Act* (PHIPA), including privacy breach notification requirements.

Is this a privacy breach? Can attackers actually access your personal health information?

A ransomware attack may constitute a privacy breach. While some ransomware attacks involve only the encryption of data, many modern attacks also involve the unauthorized access to, or theft of, personal information before systems are encrypted. In either case, the Information and Privacy Commissioner of Ontario (IPC) deems this encryption a “use” of personal information under PHIPA and it must be reported as a breach. Furthermore, organizations should assume that sensitive information may have been compromised until an investigation determines otherwise. If the investigation identifies unauthorized access to, disclosure of, or loss of personal health information, fulfill your notification obligations under PHIPA and follow applicable organizational policies.

Recommended actions to reduce ransomware risk:

1. Elevate awareness in your practice of potential threats.

- Consider cybersecurity as a patient safety issue as well as an information security issue. Disruptions to digital health systems can affect the delivery of patient care.
- Enhance employee awareness about malware threats and educate them about information security principles and techniques.

2. Assess your cyber risks regularly.

- Work with your IT provider to identify technical and administrative vulnerabilities before attackers do. Regular cybersecurity risk assessments can help identify opportunities to strengthen your security posture.

3. Make sure EMR back-ups are regular, secure and separate.

- Ensure back-ups are performed regularly, tested periodically, stored separately from production systems, and protected from unauthorized modification or deletion.
- Maintain multiple versions of back-ups and verify that restoration procedures work before they are needed.

4. Have up-to-date anti-virus and malware detection software installed on all computers and servers.

- Update all devices, operating systems, application, firmware, browsers, and endpoint protection software with the latest security patches. Promptly address vulnerabilities and remove unsupported software from service whenever possible.
- Develop and maintain a whitelist of software programs that users are allowed to run and another list of those programs that are at risk of bearing malicious code. Only allow systems to execute programs known and permitted by security policy.

5. Implement user-focused strategies to make defence systems more reliable.

- Healthcare providers and staff must operate applications and devices securely, and practices must teach staff how to spot email messages likely carrying malicious code. You should also train staff to recognize AI-generated phishing emails, text messages, voice impersonation ("vishing"), QR code ("quishing"), and other forms of social engineering.
- Consider conducting periodic phishing simulations and cybersecurity awareness training to help staff recognize evolving cyber threats and understand how to report suspicious activity promptly.

6. Review and test your recovery plans.

- Ask your internal or external IT support provider to review your disaster recovery, business continuity, and cyber incident response plans regularly.
- Test back-up restoration processes to ensure patient data can be recovered when needed.
- Confirm there is a plan to maintain patient care if access to your EMR or other clinical systems is disrupted.

7. Limit use of privileged accounts.

- Minimize the number of staff with administrative privileges. This information is very vulnerable.

8. Be cautious with email attachments and embedded content.

- Do not enable macros or active content in documents received from unknown or unexpected sources.
- Be cautious when opening attachments or clicking links, even if they appear to come from trusted organizations.

9. Treat unsolicited messages, attachments, and links cautiously.

- Do not open unexpected attachments, click unknown links, or scan QR codes from unverified sources.
- Be cautious of urgent messages requesting passwords, MFA codes, payments, or access to sensitive information.
- Verify unusual requests through a trusted communication channel before taking action.

10. Prepare for a ransomware attack TODAY.

- Assume cybercriminals will target and attack your practice with ransomware and prepare now. This includes developing specific plans on how you will continue to operate without access to your EMR, or other information systems, for an extended period of time.
- Assume your organization will experience a cyber incident and ensure plans are in place to continue delivering safe patient care if access to your EMR or other clinical systems is disrupted.

11. Review your EMR vendor's insurance and cybersecurity practices.

- Check if your EMR vendor's insurance covers cyber extortion demands, costs to restore compromised data, or loss of revenue from network downtime. Work with your vendor to address these gaps and others, such as breaches of protected healthcare information.
- Ask vendors how they protect patient information, manage cybersecurity incidents, maintain back-ups, and notify clients of security events.

12. Respond, recover, investigate and continuously improve.

- Following any cyber incident, review what happened, identify lessons learned, implement corrective actions, and update policies, procedures, training, and technical safeguards to reduce the likelihood and impact of future incidents.

For more information:

If you have questions or comments not addressed in this bulletin, please contact your OntarioMD Practice Advisor or support@ontariomd.com. The Information and Privacy Commissioner of Ontario also has guidance on ransomware: How to Protect Against Ransomware | Information and Privacy Commissioner of Ontario.

OMD is a wholly owned subsidiary of the Ontario Medical Association and is funded by the Province of Ontario. The views expressed in this publication are the views of OntarioMD and do not necessarily reflect those of the Province.