WHAT SHOULD YOU DO IF YOU ARE UNDER CYBERATTACK?

Don't panic! Ensure you know how to reach your local IT support in case of an emergency and inform your clinic's Privacy Officer immediately.

1 Contain

Immediately take steps to contain the privacy/security breach.

- Stop user activity and try to recover any lost records.
- Contact your Privacy Officer.
- Ensure evidence for a future investigation is not compromised.

2 Evaluate

Determine the extent of the breach and potential harm.

- What kind of information was involved and how sensitive is it?
- Could the information be misused?
- What caused the breach?
- How will the breach affect others?

3 Notify

Determine whether or not to notify about the breach based on:

- Legal obligations.
- Sensitivity of the information.
- Number of people affected.
- If information was recovered.
- If it could be used for fraud.

4 Prevent

Develop long-term safeguards to prevent further breaches within two months.

- Update policies.
- Perform a security audit.
- Re-train employees on company privacy obligations.

Visit the Office of Information and Privacy Commissioner's *Privacy Breach Checklist* for full details.

Contact us for more information, guidance, or support.

DOCTORS TECHNOLOGY OFFICE
604 638-5841
DTOinfo@doctorsofbc.ca

DTO Doctors Technology Office
A GPSC initiative

CYBERSECURITY AWARENESS

A GUIDE TO ENSURE DATA SECURITY

GPSC General Practice Services Committee

WHY SHOULD WE CARE?

Cybersecurity is not an IT issue. It is a patient safety issue. Physicians are legal custodians of the patient's personal health information under the Personal Information Protection Act (PIPA).

Understanding and awareness is the best way to:

- defend against cyberattacks
- achieve effective security
- mitigate a risk of privacy breaches

Two Common Threats

Phishing

Email fraud – also known as "phishing" or "brand proofing" are fraudulent attempts by cyber criminals to obtain your patients' personal information or install malicious software (malware) on your computer.

In addition to email, they can be in the form of Internet or text messaging. Regardless, the message may look like it comes from a legitimate company or a person you know.

Phishing is targeted at specific individuals or groups seeking unique information known by someone familiar to the clinic or organization.

Ransomware

Ransomware is a form of malware that infects a computer or network and spreads rapidly to lock the computer's information.

Ransomware encryption makes the data inaccessible to the user. The criminals responsible will demand payment in order to remove encryption and return the files or unlock the infected computer.

Ransomware frequently infects organizations through phishing messages containing malicious links or attachments. It can also be introduced through malicious advertising on legitimate websites that have been previously compromised.

Stay Informed and Be Vigilant

DO

- Review messages carefully.
- Look for unusual language, grammar, or spelling errors.
- When in doubt, contact the sender by another method to confirm whether the message came from them.
- Hover over the link – don't click – to see if the address is identical to what is written.

DO NOT

- Open emails from spammers or unknown sources.
- Click on email attachments from an unknown source.
- Accept software updates that appear from a pop-up window or suspicious email (ex. Java or Adobe Flash updates).

BE WARY OF

- An email from someone you know, asking you to do something out of the ordinary.
- Unsolicited emails that appear to have a sense of urgency, contain warnings, or generate curiosity.
- Clicking on unfamiliar ads on websites and links from emails.

WHEN IN DOUBT, DELETE THE EMAIL