Doctors Nova Scotia

Protecting personal health information in electronic form

Personal health information (PHI) within electronic health records is subject to the Nova Scotia's *Personal Health Information Act (PHIA)*.

Other personal information, such as **a patient's income, ethnic origin or banking information, is protected under the Personal Information Protection and Electronic Documents Act (PIPEDA), a federal law.** Applying the rules for PHIA to all personal information held by your medical practice should generally ensure you are complying with both.

Physicians must implement electronic information system safeguards within their practice to protect their network's infrastructure, hardware and software, to ensure the system functions consistently and only authorized persons have access.

Physicians must create and maintain policies that support the enforcement and implementation of the above safeguards. Physicians must also **maintain a record of every security breach of their electronic medical record (EMR) system** and the corrective measures taken to prevent future privacy and security breaches.

What is cybersecurity?

Cybersecurity refers to the processes and techniques involved in protecting sensitive data, computer systems, networks and software applications from cyberattacks.

A cyberattack is any malicious activity that attempts to collect, disrupt, deny, degrade or destroy information system resources or the information contained therein.

Types of attacks

The first step to being cybersecure is understanding the types of threats and attacks.

- **Phishing** occurs when a cybercriminal sends spam emails to trick victims into revealing login credentials, credit card numbers, bank account information and other sensitive information.
- **Social engineering** is an attack where hackers use fake advertisements, prize offers or similar lures to trick victims into providing personal and bank account information.
- **Ransomware** is a software program that uses a unique, robust encryption algorithm to block access or lock files on the targeted system and demand a ransom for returning the data.
- **Botnets attacks** attempt to access the network and plant malicious code or malware to stop the network from working.

Protecting personal health information in electronic form

Key considerations

Cybersecurity is based on three fundamental concepts: confidentiality, integrity and availability.

- **Confidentiality** refers to methods used to protect private information. This concept requires defining and enforcing access levels for information.
- **Integrity** is means protecting data from deletion or modification by unauthorized parties and ensuring the ability to reverse any unauthorized changes.
- **Availability** refers to the availability of your data. Components like hardware, software, networks, devices and security equipment should be maintained regularly.

Risks

Cyberattacks may have the following consequences on you and your practice:

- **Identity fraud** and theft
- **Data and/or financial loss** and reputational damage
- **Legal consequences**

MORE INFO

This guide is excerpted from the Doctors Nova Scotia *E-health Privacy and Security Guide*. For comprehensive information, please refer to the guide.

Protect yourself

There are several steps you can take to safeguard your systems and data.

Secure and robust passwords: Passwords must be strong and complex, with at least eight characters that meet the following criteria:

- Uppercase (A to Z) and lowercase (a to z) letters
- Numerals (0 to 9)
- Non-alphanumeric keyboard symbols (!, $, #, %)

If you have access to multiple web-based accounts, it is recommended that you use a commercial password manager.

Secure usernames: All clinic staff should have their own username. Do not share usernames and passwords.

Multi-factor authentication: Use multi-factor authentication to supplement the username and password with another factor that only the individual can access (for example, a fingerprint, an access code sent by text message or email).

Keep software and hardware current: Apply software updates to fix security risks. Replace software that is no longer updated by the manufacturer. Replace aging devices before they become a security risk.

Use anti-virus and anti-malware software: Use anti-virus software to detect and disarm viruses, and anti-malware software to target other malicious software. Be sure to run regular updates.

Use a firewall: Ensure the computer's operating system firewall program is turned on and purchase a commercial firewall software. Set both to a high security threshold.

Protect and segregate devices and equipment: Protect the PHI stored on the devices in the clinic by storing portable equipment in different places; enabling PINs, passwords and encryption on all devices; backing up devices regularly; and only using apps from trusted sources.

Protect data: Protect against data breaches when sharing or transferring PHI.

- **Enable email encryption** to disguise the content to prevent unintended recipients from accessing sensitive information.
- **Use secure file sharing,** which allows files to be shared confidentially, using encryption and a passcode.
- **Consider "sneakernet,"** which refers to the transfer of data between computers by removable, physical devices (for example, USBs, hard drives) rather than less secure methods. Ensure they are password protected and/or encrypted.
- **Set file permissions** carefully when sharing sensitive data.
- **Enable disaster recovery** to protect the practice from cyberattacks or device failures.
- **Monitor access** – track who, how and when the practice's system was accessed to detect unauthorized internal or external activity.

Get help when you need it

Contact product vendors with questions or email Doctors Nova Scotia's e-health advisor, Brent Andrews, at brent.andrews@doctorsns.com

Note: This guide is not intended as legal or professional advice or opinion. It is recommended that physicians and staff members seek legal or professional advice should concerns arise.