Cybersecurity for Dental Professionals

Protecting Information in the Digital Age

ODA ASM April 2024 | Seminar Learning Resources

Together We Can Make Dentistry Safer Online

Dentistry is a leader in digital transformation amongst healthcare practices. Dentists like yourself have invested heavily in technology to create a better patient experience, enable better case outcomes, and create better case acceptance. The use of data has allowed many of you to become more much more profitable.

At the same time, cybercrime is constantly increasing, and technology is blanketing every corner of our lives. Understanding and implementing basic cybersecurity is one of the most important life skills of the 21st century.

The following pages will help you navigate how to stay safe online, personally and professionally.

Anne Genge

Disclaimer: This compilation is intended for general information purposes only and does not replace an independent professional assessment.

While every effort has been made to provide accurate information, the nature of cybersecurity is that it is constantly evolving. Links to other resources have been included, but we cannot guarantee their accuracy.

Every practice is unique and requires custom and continuous evaluation to determine what solutions will fit your specific situation.

Permitted use: Limited to registered attendees of ODA Annual Spring Meeting Seminar April 18, 2024

Why Does Cybersecurity Matter?

"Unauthorized access to personal health information can have significant consequences for all involved. Individuals whose personal health information is the subject of unauthorized access may suffer discrimination, stigmatization and emotional or psychological harm."

Unauthorized access to personal health information may cause irreparable damage to the reputation of custodians and their agents, as well as to the relationships they have with individuals who have entrusted them with their personal health information.

Ontario Office of The Privacy Commissioner PHIPA - Detect_Deter.pdf (ipc.on.ca)

"Patient data is your business data and you can't operate without it. The same goes for if it's leaked. Reputational damage and costs from a breach can ruin your business."

Terminology

"With technology blanketing every corner of our lives, cyber skills are now critical life skills as we all strive to keep our personal information safe from cyber criminals"

PHI Personal Health Information

ePHI Personal Health Information in the electronic form

Breach A breach is a theft, loss, unauthorized use, or disclosure of personal information or personal health information.

Security Incident A security incident is an event that may indicate that an organization's systems or data have been compromised or that measures put in place to protect them have failed. A security incident is not always a breach.

Privacy breach management protocol sets out the requirements related to the identification, reporting, containment, notification, investigation, and remediation of actual and suspected privacy breaches.

Encryption is the scrambling of data to make it inaccessible to anyone unless they have a 'key' (password) to decrypt and open it. This is commonly used for email between dental practitioners to protect personal health information and sensitive practice data.

Virus Malicious software that is loaded onto a computer and then run without the user's knowledge or knowledge of its full effects.

Malware Malicious software intended to infiltrate and damage or disable computers.

Spyware Malware that passes information about a computer user's activities to an external party.

Social Engineering The name of the tactics used by cybercriminals to trick you into gaining access to your systems, phone, or personal data. Usually appeal to your emotions using urgency, fear tactics, or emotions.

Phishing A popular method used by cyber-criminals to try to obtain financial or other confidential information (including user names and passwords) from internet users, usually by sending an email that looks as though it has been sent by a legitimate organization (Bank, Apple, PayPal, CRA). The email usually contains a link to a fake website that looks authentic. This is a big threat to healthcare data.

Ransomware A type of virus that once downloaded can encrypt your files or entire system(s) and demand payment to release the key to unlock them. New variants also steal data and hold it ransom.

What is Personal Health Information?

There's much more in your health records than you think. Exposure most certainly puts you at greater risk for identity theft, but your records can also contain some of the most sensitive and potentially embarrassing details about you. Unlike a credit card, once the information is out there, it can't be changed.

Personal health information (PHI) is a category of information that **refers to an individual's medical records and history.**

Here are some examples:

Health information is considered PHI when any of the following 18 identifiers are included:

- Names
- Bithdates
- Phone numbers
- Email addresses
- Geographic information
- FAX numbers
- Social insurance numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers such as license plates
- Medical record numbers
- Account numbers
- Health plan beneficiary numbers
- Internet protocol addresses
- Website URLs
- Device identifiers and serial numbers
- Full face pictures, x-ray's and other identifying images
- Biometric identifiers (such as retinal scans and fingerprints)
- Any unique identifying code or number

What is a Data Breach?

With millions of health records already breached, it's never been more important to acquire the knowledge you need to defend your practice, also learn how to respond when something bad happens

There are many types of breaches. You're hearing about them every day. A breach can be as simple as sending a treatment receipt to the wrong address, but **data breaches** have far more grave outcomes.

The Ontario Information Privacy Commissioner's definition of a health information breach can be found here: Responding to a privacy breach - IPC

Data breaches include the following and more:

- Ransomware
- Data theft
- Data exposure
- Unauthorized access/snooping
- Lost USB - unencrypted
- Lost hard drive - unencrypted
- Email hacked - unencrypted

For example, in Ontario an individual found guilty of committing an offence under PHIPA can be liable for a fine of up to $200,000 or up to one year in prison, or both. An organization or institution can be liable for a fine of up to $1,000,000

Potential consequences of a breach under PHIPA - IPC

health-privacy-breach-guidelines.pdf (ipc.on.ca)

Privacy breach protocol - IPC

Detecting and Deterring Unauthorized Access to Personal Health Information - IPC

Dental Office Security Risk Quiz

10 questions to help you identify cybersecurity risks and blind spots

1. My entire team knows what to do if our systems become infected with ransomware (the current biggest threat to health data)

2. Everyone on my team gets annual training on safe email practices, i.e. phishing, virus threats through email, dangers of using free email accounts, dangers of accessing webmail via practice systems.

3. My practice has a formal system and plan in place to maintain constant availability of patient data and ensure data is protected from loss.

4. My IT company provides proof, i.e. regular reports that my data is protected and that systems are up to date.

5. We run quarterly fire drills to test backups to ensure the data is recoverable.

6. We ensure that no patient information is ever exchanged over unencrypted or free email accounts. Examples: Gmail, Hotmail, Yahoo.

7. Everyone on my team receives regular training regarding privacy compliance requirements and responsibilities.

8. We have a system for ensuring that only those authorized have access to patient and practice data. (blind spots include remote workers, software providers, IT providers, consultants)

9. We have a formal data security plan that includes annual risk assessments, monitored cybersecurity, ransomware protection, and computer safeguards to prevent human error.

10. We obtain periodic professional cybersecurity risk assessments and follow management plans to ensure gaps are fixed.

Dental Office Privacy & Security Resources

This compilation is helpful for practice owners, managers, and privacy officers in understanding compliance requirements, how to prepare, prevent, and respond to breaches.

Quick references for PHIPA Ontario - PHIPA FAQ
phipa-faq.pdf (ipc.on.ca)

What laws apply to me?
https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/

Office of the Privacy Commissioner – Canada has guidance, templates, and training
https://www.priv.gc.ca/en/

What is a breach and how to report it. https://www.priv.gc.ca/en/privacy-topics/business-privacy/safeguards-and-breaches/privacy-breaches/respond-to-a-privacy-breach-at-your-business/gd_pb_201810/#_Part_1

Responding to a Privacy Breach in Ontario
health-privacy-breach-guidelines.pdf (ipc.on.ca)

Telehealth Security
virtual-health-care-visits.pdf (ipc.on.ca)

HIMMS has excellent cybersecurity for healthcare resources
https://www.himss.org/resources/cybersecurity-healthcare

HealthIT News follows digital health and privacy & security breach cases, interesting articles
https://www.healthcareitnews.com/

HHS Wall of Shame is a running list of breaches in USA. Is helpful in understanding different real-world scenarios of incidents related to your specific sector of healthcare.
https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Ontario Privacy Commissioner – Privacy Impact Assessment Guidelines
https://www.ipc.on.ca/wp-content/uploads/resources/phipa_pia-e.pdf

Anne Genge

Information Privacy & Security Professional

Specialization: Dental Practices

anne@myla.training