intiveo.

GUIDE

Digital Security Basics for Dental Practices

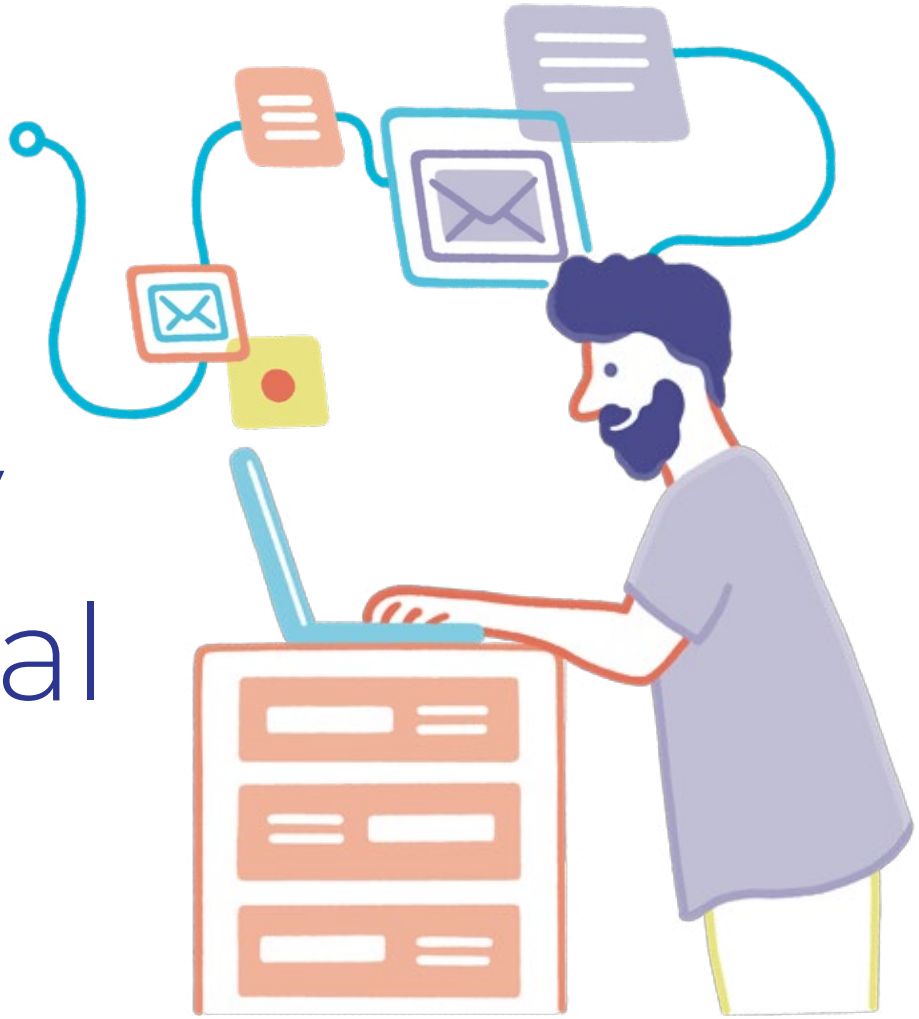


Table of Contents

Digital Security: A Top Priority

Digital Security: A Top Priority

Making digital security a top priority is important for every dental and oral surgery practice. Keeping your patients' information safe is not just ethical, it is also an important part of maintaining healthcare standards and abiding by the law.

Digital security can feel like a daunting undertaking for dental practices, but this guide can help. Let's walk through some of the most common threats, as well as text and email best practices that will help keep your data secure. Then, for Canadian dental practitioners, we've added a bonus section on how Law 25 in Québec affects your practice.

Personal information and personal health information are protected by HIPAA in the US and PIPEDA in Canada.

Data Breaches

How HIPAA/PIPEDA Compliance Factors In

The Health Insurance Portability and Accountability Act (HIPAA)[1] in the United States and the Personal Information Protection and Electronics Document Act (PIPEPA)[2] in Canada are pieces of legislation that, if complied with, help prevent against data breaches. Two of their key provisions include:

- Requiring entities to protect personal health information (PHI) or personal information (PI)
- Placing restrictions on the disclosure of PHI and PI for unauthorized purposes

Often, dental and oral surgery clinics will employ a third-party service provider to help them manage their compliance to HIPAA and PIPEDA. This has advantages and disadvantages. Having a dedicated, expert team to look after your digital security takes the pressure off the team at the dental office itself. However, more than half of data leaks occur with a third-party vendor.[3]

When it comes to keeping your data secure, the single most important action you can take as a practice is to monitor and audit your security consistently. This includes asking or ensuring any third-party service providers include such monitoring and auditing in their own practices. This can result in positive outcomes for security management, because issues, including data breaches, are detected much sooner.

[1] The Security Rule | HHS.gov
[2] PIPEDA compliance help - Office of the Privacy Commissioner of Canada
[3] How to Prevent Data Breaches in 2024 (Highly Effective Strategy) | UpGuard

Phishing and Ransomware Attacks

Phishing

Phishing is an incredibly common type of data breach. Hackers will successfully deceive staff into clicking on suspicious links in a text or email, or on a website.

One of the most common types of phishing is email phishing. This might be an email that appears to be from a trusted international organization and, in the healthcare industry, will often reference a well-known medical crisis or event of some kind.[4]

For example, an email referencing a sudden medical crisis, like Covid-19, might offer a link to download a document or report about it, sending the unsuspecting staff member to a website where they then enter their credentials. In fact, according to a recent report, 68%[5] of data breaches involved some kind of deception, where an apparently innocent link or message allows a hacker to collect useful information.

Phishing occurs when hackers manipulate someone into clicking on a suspicious link.

[4] What are the Biggest Cyber Threats in Healthcare? | UpGuard
[5] 2024 Data Breach Investigations Report | Verizon

Ransomware

Ransomware is a type of malware (malicious software designed to disrupt or corrupt a computer or network).

Ransomware relies, partly, on the desire for healthcare clinics or organizations to minimize disturbances in their operations. When malware gets into a network — often through phishing — the cybercriminals then get in touch with the clinic or organization and demand money in order to end the ransomware attack. In the U.S., the FBI has issued a directive to never pay this ransom and instead report the attack. However, to minimize damage and maintain their reputation, many pay the ransom. As you may imagine, this does not always result in an end to the ransomware attack.

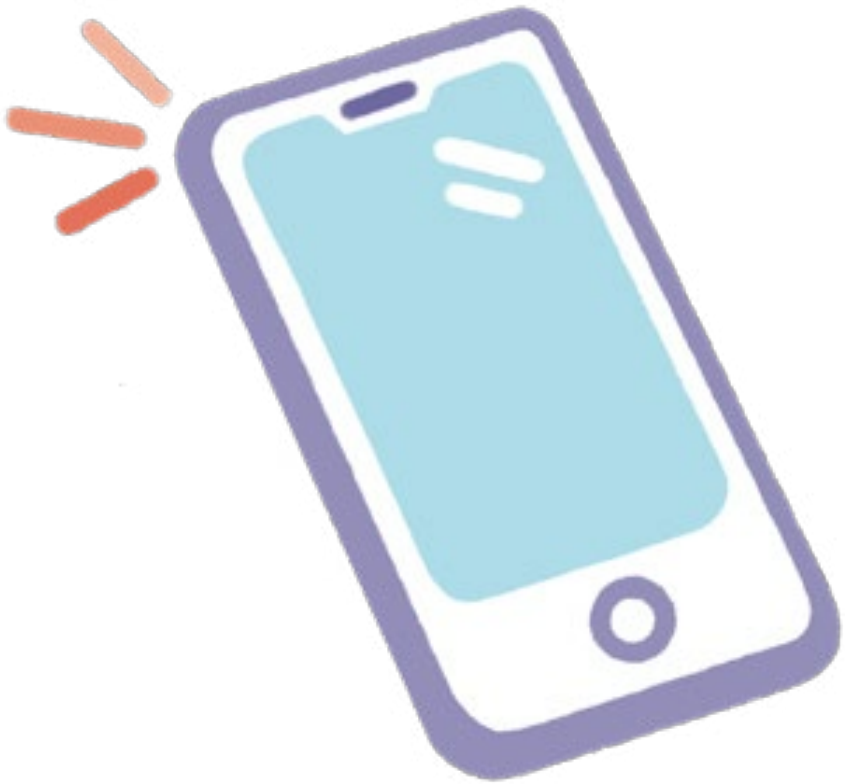
One of the troubling developments in ransomware attacks is that the people who use it have been paying attention to how other companies use software as a ready-to-go service. Ransomware-as-a-Service is now readily accessible to cybercriminals, meaning they can just sign in and launch an attack without a lot of technical know-how.

Ransomware is a type of malware that involves paying a ransom.

Malware is a type of malicious software designed to disrupt or corrupt a computer or network.

Text and Email: Best Practices

Text and Email: Best Practices



Let's talk about best practices for text and email, two of the key ways that cyber criminals can gain access to your staff — and eventually your data.

8 Best Practices

1. **Use encrypted communication channels.** Always! Encrypted messaging and email platforms safeguard patient data from unauthorized access when you're sending and receiving text messages.
2. **Limit the amount of sensitive information getting sent.** Avoid sharing detailed personal and medical information through these channels as much as possible. If your practice has a secure portal, direct them there!
3. **Authenticate recipients and senders.** Before sending or receiving any sensitive information, make sure you know the identity of the people you're communicating with. Verifying email addresses and phone numbers can definitely help.
4. **Set up access controls.** Using access controls with your practice's messaging and email systems is important. Restrict access to only the people who need it. Use strong, unique passwords and multi-factor authentication when you can.

Text and Email: Best Practices

5. **Educate, educate, educate.** Regular training sessions are the best tool for getting team members to recognize phishing attempts and understand proper handling techniques for sensitive information.
6. **Monitor and audit communications.** Keeping records of all communications and regularly monitoring for unauthorized access or breaches goes a long way.
7. **Provide patients with a disclaimer.** Remind patients not to share personal information through unencrypted channels and encourage them to verify the authenticity of messages they receive from your staff.
8. **Update security protocols regularly.** Continuously review and enhance your communication security policies to adapt to evolving threats and regulations. Staying proactive ensures that your practice stays compliant with regulations as well.

La Loi 25: What Canadian Dental Practices Need to Know

La Loi 25: What Canadian Dental Practices Need to Know

Recently, Québec introduced Law 25/Loi 25[6], which will affect not only dental and oral surgery practices in Québec, but also any practice interacting with a practice there. Québec's Law 25 introduces stricter regulations to enhance data privacy and protection, particularly impacting dental practices. This law mandates that practices implement advanced security measures, obtain explicit patient consent for data use beyond direct care, and ensure compliance when transferring patient information outside Québec.

To comply with Law 25, practices should audit their current data security measures, update consent forms, train staff on new requirements, and review protocols for cross-border data transfers. These steps will help ensure compliance with the law's stringent standards.

Adhering to Law 25 offers dental practices an opportunity to strengthen their commitment to patient privacy and trust. By understanding and implementing the necessary changes, practices can not only achieve compliance but also reinforce their reputation in the digital age, where protecting patient information is crucial to maintaining integrity.

Québec's Loi 25/Law 25 has introduced even stricter regulations to enhance data privacy and protection, which will likely impact other provinces as well.

[6] Everything you need to know about Quebec's Law 25 (cfib-fcei.ca)

Stay Compliant With Intiveo

Adhering to different security acts can be a bit overwhelming, but at Intiveo, we try to make it easy. We have a lot of experience with digital security because our own measures are so rigorous. We are proud to have continuously maintained high HIPAA and PIPEDA compliance standards, including SOC 2 compliance through a SOC 2 Type 1 audit. This helps ensure that anyone using our platform adheres to HIPAA and PIPEDA regulations. With Intiveo, rest easy knowing your practice is fully compliant!

Would you like more insights for your dental practice? We offer several resources including guides, self-assessments, templates packages, and more! Check them out here!