Alberta Doctors' Digest

Cybersecurity and cyber insurance for Alberta medical clinics

Why cyber risk is a medical risk

In Alberta, medical clinics are trusted custodians of some of the most sensitive personal information in the province. Every day, physicians, administrators, and staff handle health records, diagnostic reports and billing data, all of which hold immense value to cyber criminals.

Health care is now one of the most targeted sectors for cyber attacks in Canada. Ransomware incidents, phishing schemes and vendor system compromises have disrupted hospitals, clinics, and pharmacies across the country. For medical practices, the consequences of a cyber breach can go far beyond temporary inconvenience – they can halt patient care, erode trust, and trigger costly legal and regulatory obligations.

In a sector defined by compassion and confidentiality, cybersecurity isn't just an IT function – it's a patient safety and professional reputation issue.

The cyber threat landscape in health care

Attackers increasingly view health care as low-hanging fruit. Clinics often rely on legacy systems, shared passwords or outdated IT infrastructure that wasn't designed for today's threat environment. Meanwhile, electronic medical record (EMR) systems, online booking tools and telehealth platforms create new points of vulnerability.

Common cyber threats facing Alberta clinics include:

- **Ransomware attacks:** Encrypting patient data and demand payment to unlock systems.
- **Phishing emails:** Impersonating labs, payers or software vendors to trick staff into revealing credentials.
- **Vendor compromises:** Attackers targeting IT providers or EMR vendors to gain broader access.
- **Insider mishandling of data:** Includes lost devices or unauthorized record access.

These attacks aren't theoretical. In recent years, Canadian health care organizations from Newfoundland to Saskatchewan have suffered ransomware incidents that took systems offline for weeks, forcing a return to paper charts and manual patient tracking. Alberta clinics aren't immune. In fact, smaller practices may be more vulnerable because they often lack dedicated IT security resources.

The real cost of a breach

When a cyberattack hits a medical practice, the costs escalate quickly.

- **Operational downtime:** Clinics may be unable to access EMRs, lab portals or scheduling systems for days or even weeks.
- **Patient notification and regulatory compliance:** Under Alberta's *Health Information Act (HIA)* and *Personal Information Protection Act (PIPA)*, breaches involving health information must be reported to both the Office of the Information and Privacy Commissioner (OIPC) and affected patients.
- **Incident response and legal costs:** Forensics, legal counsel and privacy breach reporting can easily exceed $100,000 for even a modest clinic.
- **Ransom demands:** Average ransomware demands in health care now range from $200,000 to $800,000.
- **Reputation damage:** Patients expect their personal health data to be protected. Once trust is lost, it's difficult to rebuild.

In short: one email click or missed software update can paralyze an entire practice.

Cybersecurity best practices for medical clinics

While the threat landscape continues to evolve, the fundamentals of good cyber hygiene remain consistent. Clinics that implement the following controls significantly reduce both their exposure and their insurance costs:

- **Multi-factor authentication (MFA):** Require MFA on all email and remote access accounts, this blocks over 90% of credential-based attacks.
- **Regular patching:** Keep operating systems and EMR software up to date with security patches.
- **Secure backups:** Maintain encrypted, offline backups of all critical data and test them regularly.
- **Endpoint protection:** Use next-generation antivirus or endpoint detection and response (EDR) tools on all workstations and servers.
- **Email filtering and staff training:** Train staff to identify phishing attempts and verify any unusual requests.
- **Vendor vetting:** Ensure third-party IT vendors and EMR providers have written security commitments and incident response protocols.
- **Incident response plan:** Establish a clear process and contact list (IT, insurer, legal counsel, privacy officer) for breach events.

Tip: Ask your EMR provider whether they are responsible for patching and breach notification under your service agreement. The answer varies and can determine who's liable after an incident.

The role of cyber insurance

Cyber insurance has become as essential to modern practice management as malpractice insurance is to patient care. A well-structured policy isn't simply a financial safety net — it's an access point to immediate expert help during a crisis.

A comprehensive cyber policy typically includes:

- **Incident response services:** Immediate 24/7 access to forensics, IT containment and legal guidance.
- **Breach notification and credit monitoring:** Coverage for notifying affected patients and monitoring identity theft.
- **System restoration and data recovery:** Costs to rebuild and restore EMR systems and data.
- **Business interruption coverage:** Compensation for income lost while systems are down.
- **Ransomware and cyber extortion:** Negotiation and payment facilitation (where legally permissible).
- **Regulatory defence:** Legal representation and fines/penalties where insurable by law.

Example:
A mid-sized Alberta clinic with 12 physicians and 25 staff was hit with a ransomware attack that encrypted its EMR. The insurer's incident response team restored access within four days, coordinated patient notifications and covered approximately $380,000 in response and downtime costs. The clinic resumed operations without losing patient records or facing major reputational harm.

Key questions to ask your insurance broker

When reviewing or purchasing cyber coverage, clinic leaders should ask:

- Does the policy cover business interruption from EMR downtime?
- Are cloud-hosted EMR and vendor breaches included?
- Is there coverage for social engineering or funds transfer fraud?
- Are we meeting the security requirements our insurer expects?
- Can our cyber policy coordinate with our existing D&O or malpractice coverage?

Cyber insurance isn't a one-size-fits-all product. A broker experienced in health care and privacy risks can help tailor coverage to the specific needs of a medical practice.

Creating a culture of cyber resilience

Technology alone won't protect your clinic – people and processes are equally important.
Clinic leaders can foster a cyber-aware culture by:

- Scheduling quarterly phishing simulations or security refreshers.
- Holding vendors accountable for their own security practices.
- Designating a privacy officer and ensuring that incident procedures are well-documented.
- Staying informed on evolving threats through resources like The Canadian Centre for Cyber Security, CIRA's free cybersecurity awareness training, Alberta Medical Association and Westland Insurance educational materials.

Cyber incidents are now a predictable business risk, not a rare event. For Alberta's medical community, cybersecurity is inseparable from patient safety and professional reputation.

By combining proactive security measures with robust cyber insurance coverage, clinics can ensure that when – not if – an attack occurs, they have the tools, resources, and resilience to recover quickly and continue delivering exceptional patient care.

Secure your coverage today.

Banner image credit: Cliff Hang, Pixabay.com