OMD Educates: Cybersecurity, Patient Privacy & Protecting Your Practice – Presented by OMA Insurance

Questions and Answers

Q1: Who has the main responsibility for cybersecurity? EMR, clinic owner and or each doctor?

A1: Cybersecurity is a shared responsibility, but accountability for safeguarding personal health information remains with the health information custodian, which is often the physician or clinic operating the practice. EMR vendors play an important role in securing their platforms and infrastructure, and many certified EMR products are subject to significant privacy and security requirements. Cybersecurity incidents do not arise only from the EMR but may be introduced at the user level. They frequently originate through email, compromised devices, weak passwords, phishing attempts, third-party applications, or internal processes within a clinic. For that reason, physicians, staff, technology vendors, and service providers all have a role to play. The most effective approach is to view cybersecurity as a clinic-wide risk management responsibility rather than solely an IT responsibility. Physicians and clinic owners should ensure they have appropriate safeguards, training, vendor oversight, and incident response in place.

Q2: Do EMR vendors not have any liability?

A2: Liability for a privacy/security incident may be shared. Assignment of liability is always dependent on the particular situation, the cause of an incident and what steps were taken to mitigate. EMR vendors may have liability in certain circumstances. If a breach results from a failure of the vendor's systems, services, or contractual obligations, the vendor may bear some responsibility. However, the existence of vendor liability does not eliminate the health information custodians' obligations under privacy legislation. Physicians remain responsible for taking reasonable steps to protect personal health information in their custody, including selecting appropriate vendors, implementing safeguards, training staff, and responding appropriately to incidents. In practical terms, a physician should not assume that a vendor's involvement automatically transfers all legal, regulatory, or operational responsibilities to the vendor. Understanding what protections, indemnities, security commitments, and incident response obligations are included in vendor agreements is an important part of managing risk.

Q3: Does moving to cloud-based platforms put the onus on the EMR provider and not on the individual user?

A3: Moving to a cloud-based platform may provide important security benefits, including centralized security management, monitoring, maintenance, and infrastructure controls. However, it does not transfer all responsibility from the physician or clinic to the EMR provider. The EMR provider is responsible for securing the platform it operates. The physician or clinic remains responsible for how the system is used within the practice. Risks can still arise through compromised credentials, phishing attacks, use of unsecure devices or networks, unauthorized access by staff, weak password practices, or other systems connected to the clinic environment. From a privacy perspective, the obligation to take reasonable steps to safeguard personal health information continues regardless of whether records are stored on-premises or in the cloud. Physicians should work closely with their EMR vendor to understand the security controls available, implement recommended safeguards such as multi-factor authentication, and ensure staff receive ongoing privacy and security training. Cloud adoption should be viewed as part of a broader cybersecurity strategy, not as a replacement for one.

Q4: Given we are all going to have to find our own cybersecurity now that the CMPA has dropped us, is the OMA going to find a group option for all of us to avoid adding this to our already full plates?

A4: If this is related to Insurance coverage – OMA Insurance has Cyber Insurance products that are available on an individual basis. To learn more email, us at info@omainsurance.com or call us at 1-800-268-7215 option 3.

Q5: To follow up on CMPA stance: business liability is not CMPA issue but is anything covered by CMPA in case of cyberbreach? Can we have an example of this to help us understand this CMPA?

A5: CMPA generally continues to provide medico-legal advice, including advice related to notification and reporting obligations, and assists members with civil legal actions, privacy commissioner complaints, and College, health authority or hospital proceedings relating to the professional practice of medicine, including those involving privacy and cybersecurity breaches. However, CMPA does not pay damages or settlements related to cyber breaches or to inappropriate collection, use or disclosure of personal health information, and does not generally pay the costs of forensics, breach notification or data restoration.

Q6: Can the CMPA/ OMA provide a list of what counts as a business/ medicine risk i.e. what will be covered or not?

A6:

- CMPA generally assists members (and their eligible clinics) with privacy-related matters, including complaints, investigations, and claims arising from the practice of medicine. CMPA does not assist with the payment of damages arising from a cyberbreach or a finding of inappropriate collection, use, or disclosure of personal health information (e.g., "snooping", inappropriate recording of patients), or settlements arising from such allegations; and

- CMPA does not typically assist with ransomware payments or costs of data restoration, privacy breach notification, forensic investigation, or hardware issues. CMPA also does not assist members in becoming privacy compliant nor does it pay fees, penalties, or other costs assessed for any privacy or cybersecurity breach.

For more information, members are invited to read our following publications

- CMPA - Privacy and cybersecurity matters
- CMPA - CMPA assistance: Cybersecurity and privacy matters
- CMPA - Cybersecurity threats: Are you prepared?

Members who wish to obtain more information or require clarification are invited to contact the CMPA at 1-800-267-6522, Monday to Friday between 8:30 a.m. to 4:30 p.m. ET.

Q7: For clinics who have their own cyber insurance, how does this extend to non-owner associate physicians? And is additional coverage required?

A7: HUB would suggest members ask the clinic owner or insurer whether the definition of "insured" includes associates, whether claims against them personally are covered, and whether the limit is shared across the clinic. If the answers are unclear, or they hold their own patient records, it's worth quoting an individual policy. Hospital-only physicians should ask the hospital about its coverage

Q8: Ideally there would be a recommendation on how to proceed with this OMA?

A8: You can contact CMPA for advice about your notification and reporting obligations or related medico-legal issues, or for information about CMPA's extent of assistance. **If you**



are seeking legal/privacy support you can contact legal affairs at OMA. Email us at legal.affairs@oma.org.

Q9: Is there a potential threat to cyber-attack if using AI

A9: As with any new tool, privacy risks should be considered. In the case of AI, the risks may come from two directions 1) Attackers are using AI to make phishing and voice scams more convincing, and 2) the AI tools clinics adopt (scribes, chatbots) add another vendor and another flow of patient data.

Before adopting a tool, members should ask where data is stored, who can access it, and what the vendor contract says about security and breach notification. Standalone comprehensive cyber insurance would often provide coverage to address cyber breaches associated with AI risk, depending on the policy terms. In addition, OntarioMD's free training now includes AI exposure content.

Q10: Does the OMA legal help with cybersecurity breaches or what kind of lawyer should we consider?

A10: The OMA legal department can provide some general information to assist in the event of a cybersecurity breach, but we do not provide individual legal advice or representation. We would recommend seeking independent legal counsel from an expert in the area of privacy law. Your insurer is likely to have a preferred legal counsel to whom they will refer you, with preferred hourly rates, so it is important to seek input from your insurer as soon as possible.

11. How do we start a cyber security plan?

A11: Each cyber security plan will depend on the clinic's needs and set up. We recommend beginning with a practical exercise: identify who you would call if your clinic could not access its EMR tomorrow morning. OMD offers free privacy and security training for Ontario physicians and their staff, which is a strong starting point for building cyber readiness. In addition, conducting a simple tabletop exercise with your team, such as walking through what would happen if your EMR became unavailable due to a ransomware attack, is one of the most valuable steps a clinic can take to identify gaps in its preparedness and to ensure you have an emergency contact list of technology support vendors (including EMR provider) and office staff that is outside of your computer system and always easily accessible.

Q12: When you say that showing we had safeguards in place in order to prevent liability, does that include the cybersecurity insurance? HUB is that now considered standard of care?

A12: No — insurance isn't a safeguard in that sense. Safeguards (privacy policy, MFA, tested backups, training, vendor contracts, a response plan) help prevent a breach and show reasonable steps to demonstrate compliance with privacy legislation. Cyber insurance can assist with financial risk and gives access to a response team after an incident.