Does Your Client Use Telehealth? Make Sure They Have Matching Coverage

November 25, 2020

The increasing use of virtual healthcare platforms has raised concerns about, (a), how patient health information will be protected, and (b), how privacy legislation will be applied to ensure data security. Specifically, the rise of virtual care raises some urgent questions:

- What happens if a virtual healthcare platform or app experiences a data breach?
- Who bears the responsibility?
- What sort of preventative measures should be taken to mitigate risk?

Privacy Exposure: Not Just A Problem For Big Companies

Whereas big brands tend to garner the bulk of media attention when it comes to data breaches, all types and sizes of business are vulnerable to cyber attacks. In a story in Canadian Underwriter Magazine, for example, one underwriter reported that 90% of her firm's cyber claims in 2017 were filed by small to medium sized businesses (1).

In the healthcare sector, which was among the early buyers of cyber coverage, non-hospital clinics and individual practitioners could face as much risk of a data breach as the big hospitals. The rise of virtual care and increasing dependence on technology - particularly internet-connected health devices - is at least partly to blame for this growing exposure.

On June 9, 2020, the remote healthcare services company Babylon Health advised that its app had suffered a data breach. One of Babylon Health's users discovered he had access to a video recording of a consultation between a physician and a patient. Rather than a malicious attack, the Babylon breach resulted from a software error. (2)

The Limitations Of Telehealth

According to a June report from the Canadian Medical Association (CMA), 47% of Canadians accessed some form of virtual care during the pandemic. Looking ahead, virtual care is expected to expand once the crisis is over.

With widespread adoption comes new risks and an urgent need for cyber coverage - especially given that the majority of healthcare providers, whether traditional or

telemedicine, are still uninsured for cyber attacks. In the event of a data breach, these uninsured healthcare providers will be left to pick up the tab.

But administrative and legal costs aren't the only concern. For example, ransomware attacks could potentially prevent a patient from getting their repeat prescriptions.

Another problem in the healthcare sector is that many traditional providers struggle to adhere to basic compliance requirements, especially during virtual care visits. For example, a doctor having a virtual visit with a patient could constitute a privacy breach if the patient has their partner or children in the background.

Before entering this space, physicians and companies developing virtual healthcare platforms should carefully consider the applicability of privacy legislation and prioritize the development of mitigation strategies designed to reduce or eliminate the risk associated with the use and transfer of sensitive information over virtual platforms.

Addressing Privacy And Security Risks

To secure the right protection for their clients, brokers should ensure that clients have insurance that is adequate for the services these healthcare clients are delivering. Traditional medical malpractice policies, for instance, are not really adequate for companies offering their services electronically. Brokers instead need to reconsider their renewals and assess whether or not the correct coverage is in place for their clients.

If their coverage doesn't extend to areas that arise out of technology activities or cyber events, then it's time to reconsider the current policy. While MedThree's policies extend to cyber coverage, few insurance providers will since cyber is still an emerging trend.

Recap

As careful as virtual healthcare platforms might be, data breaches may still occur regardless of the steps taken to secure sensitive information and data. That is why the healthcare practitioners who use these services need to be aware of the risks, and develop a plan of action to both mitigate and manage a data breach before it occurs. Physicians entering this space should acquire the right cyber security insurance coverage.

At MedThree, we understand the ever-changing landscape of digital health. Our underwriters work with brokers to provide the best possible coverage for their healthcare clients while staying ahead of the technological curve. Meanwhile, our

online platform allows the insured to purchase insurance at any time to receive instant coverage and documentation straight to their inbox.

Visit our website for more information about our policy features.

Content is current as of the date of broadcast and is subject to change without notice.

Sources:

1. https://www.canadianunderwriter.ca/citb/convincing-clients-cyber-coverage-is-crucial/
2. https://techcrunch.com/2020/06/10/babylon-health-admits-software-error-led-to-patient-data-breach/