GOWLING WLG

RISK MANAGEMENT: THE DIGITAL TRANSFORMATION IN THE HEALTH INDUSTRY

25 February 2020

This article is part of the "Practice Risk Solutions" series for regulated health professionals and health organizations, produced in partnership with BMS Group Ltd.

As the health industry migrates from paper-based to electronic clinical records, the risks associated with the collection, use and disclosure of personal health information changes. The requirements for electronic document security, encryption and transmission come to the forefront. The use of electronic repositories opens the door for cyberattacks and significant privacy breaches. With this change comes the need to identify organizational vulnerabilities and plan for them.

Digital risks to the health industry are real. Recently, one of Canada's largest medical service companies was the subject of a ransom attack after hackers gained access to personal information of up to 15 million customers. A few months prior to this attack, three Ontario hospitals were subject to a malicious software attack. Last year, the U.S. Department of Health and Human Services issued a warning of a malware called "Ryuk" that threatened health care organizations. Ryuk is a type of malware that can remain invisible to average users for an extended period while it surreptitiously attacks computer networks and collects information about the organization. Ryuk attackers typically exploit a system's vulnerabilities through malicious emails, which oftentimes drive users to sites that try to attack the computer exploiting various software vulnerabilities. After these malwares collect information, the hackers lock data and extort network owners to pay large sums of money to make the data accessible again.

Under Ontario's Personal Health Information Protection Act (PHIPA) (and under similar legislation throughout Canada), health information custodians must take reasonable steps to ensure the personal health information in their custody or control is protected against theft, loss and unauthorized use or disclosure and against unauthorized copying, modification or disposal. Health information custodians are also obligated to implement technical, physical and administrative safeguards to protect the personal health information of their patients.[1]

When developing your organization's risk plan for digital records, collaboration between all departments - including health professionals, legal, finance and IT - is important. Without a fulsome consideration of all of the types of risks from all of the stakeholders in the organization, certain risks may be overlooked and the risk mitigation strategies employed can be ineffectual.

In preparing a risk plan, the first step is to properly identify relevant risks. Through this process your organization will begin to classify a series of strategic, operational, financial and legal risks with varying likelihoods of realization and impact. For example, changing to an electronic document system could result in a data breach (operational risk), which would be a breach of PHIPA (legal risk) and which could in turn allow a competitor to gain market share (strategic risk), which could result in reduced cash flow and an inability to pay loans (financial risk). Once all of your organization's risks are identified, the appropriate mitigation strategies can be evaluated and employed for instance, through implementing policies, strengthening IT infrastructure, training staff and obtaining insurance.

It is the combined implementation of these techniques and the constant review and revision of your plans that will reduce your organization's exposure to risk and reduce the impact should risks be realized. For example, organizations can spend endless resources in developing a strong IT system; however, the risk of unauthorized collection, use and disclosure of personal health information will persist if proper policies are not instituted, education is not provided and best practices are not enforced for those dealing with patient data on a day-to-day basis.

Policies will unfortunately be ineffectual if employees are not trained to properly follow them. For instance, introducing a secure documents transfer system and policy is helpful, but if employees do not know it exists or how to use it, or are unaware of their obligation to use it, its implementation will be unsuccessful. Similarly, educating employees on how to recognize and report phishing emails is one of the simple means to impede malicious cyber attacks. These emails are one of the most common methods of attack employed by hackers to identify victims, gain unauthorized access to systems and deploy ransomware.[2] These email schemes can be exceptionally advanced and convincing (from a known contact, with the same writing style as the contact, with personal information about the contact, etc.) that they mislead even the most senior and experienced employees.

Organizations should also have a strategy to mitigate the consequences of a successful cyberattack. The inability to access patient records in a timely manner could pose a significant health risk to some clients and could cripple institutions' abilities to offer treatment. Organizations should ensure that (a) they remain able to access their data in the event of an attack (for example, through data backup procedures); and (b) that others are unable to read the data due to it being encrypted. Having such a plan in place serves to reduce the negative consequences and impact to patients in the event of a cyberattack.

Failing to develop safeguards to protect the personal health information of patients can lead to data breaches, which can ultimately result in privacy complaints, College complaints for the regulated health professionals involved, and lengthy and expensive lawsuits (individual or class action). Health information custodians that are subject to a cyberattack may be found negligent and/or liable under provincial and/or federal privacy legislation.[3] While the risk mitigation strategies reviewed above may not prevent the realization of every risk, a robust risk review and plan, as well as a seamless organization-wide implementation, can serve as valid defences to complaints and to claims.

As with any organizational change, there are risks coupled with all of the benefits that the program can bring. The best method to reduce the risks (and their negative effects) is to plan, prepare, continuously evaluate and revise.

[1] https://www.ontario.ca/laws/statute/04p03

[2] https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity-newsletter-fall-2019/index.html

[3] Hopkins v. Kay, 2015 ONCA 112 (CanLII).

NOT LEGAL ADVICE. Information made available on this website in any form is for information purposes only. It is not, and should not be taken as, legal advice. You should not rely on, or take or fail to take any action based upon this information. Never disregard professional legal advice or delay in seeking legal advice because of something you have read on this website. Gowling WLG professionals will be pleased to discuss resolutions to specific legal concerns you may have.

Related Tech, Insurance & Professional Liability

Authors

Jahmiah Ferdinand-Hodkin

Partner - Ottawa

Email

jahmiah.ferdinandhodkin@gowlingwlg.com

Phone

+1 613-786-0275

vCard

Jahmiah Ferdinand-Hodkin

Samaneh Frounchi

Associate - Ottawa

Email

samaneh.frounchi@gowlingwlg.com

Phone

+1 613-786-3252

vCard

Samaneh Frounchi