THE LAWYER'S DAILY

The Lawyer's Daily | 111 Gordon Baker Road, Suite 900 | Toronto, ON M2H 3R1 | www.thelawyersdaily.ca
Phone: (800) 668-6481 | Fax: (905) 479-3758 | John.Carson@lexisnexis.ca

Civil Litigation

Digital health care in a pandemic: Risks and rewards

By **David Young**

David Young

(October 28, 2020, 8:29 AM EDT) -- As the COVID-19 pandemic has pushed digital functionalities to the fore, it is impacting significantly the delivery of health care, in particular virtual care and access to medical records. However, as in other areas, privacy and security risks abound.

Digital health modalities are playing a key role in facilitating continuity of care in the pandemic. Providers of virtual medical services such as Maple and Cover Health have seen exponential growth; provincial public health insurance plans have expanded their eligibilities for services provided remotely.

Electronic medical records are a key facilitator of remote care, permitting health professionals to view a patient's record from any location and to upload their own care prescriptions and records, accessible by collaborating providers and care institutions as well as, potentially, the patients themselves.

Simplified patient access to their digital medical records speaks to patient-centric control, one of the key dictates of recent public policy manifestos. Such functionalities make more accessible to a patient their personal health information records — a legal requirement under privacy laws such as Ontario's *Personal Health information Protection Act, 2004* (PHIPA). Importantly, they also serve a health system purpose by lessening the need for one-on-one interactions with medical professionals for activities such as receiving test results and reviewing diagnoses.

However, making medical records accessible online presents privacy and security issues. Compared with a paper-based system, digital records enable wider potential points of contact, typically into a consolidated central database of all records of a patient's interactions with a health system. Not surprisingly, incidents of unauthorized access, surreptitious viewing and theft of records, as well as exposure to ransomware and other external threats, are becoming commonplace. The increased reliance on electronic medical records systems in the pandemic context is further exposing weaknesses in cybersecurity protections that in many cases have not been updated to align with the new and expanded virtual communications channels, or increasingly interconnected databases.

Even before the pandemic data breach incidents involving medical records were proliferating. The health sector and in particular hospitals, have been the subject of both targeted "snooping" scandals as well as systemwide attacks.

In a case that resulted in a multimillion-dollar class action — before it failed to gain certification — up to 14,450 expectant mothers were notified that their medical records might have been accessed by clerical staff for commercial exploitation purposes over a period of five years between 2009 and 2014.

More recently, last October, LifeLabs, a laboratory testing provider which enabled online reporting and patient access to lab results, notified some 15 million patients that their records had been subject to a cyberattack. At least two class actions have been commenced on behalf of affected patients and in June the B.C. and Ontario privacy commissioners completed an investigation which found LifeLabs deficient in its security safeguards.

In January of this year, a class action was certified in a case involving a hospital nurse at the William Osler Health System accessing 11,000 patients' records surreptitiously over a nine-year period. And

this past September, Medisys Health Group — an executive, personal and virtual health-care provider owned by Telus — notified 60,000 patients that its records may have been accessed in a ransomware attack for which the company's security firm paid an undisclosed sum to retrieve stolen records.

This surge of "snooping" and cyberattack incidents has led to increased regulator scrutiny as well as legislative responses. Outside of the legal system, there are calls for more resources to be applied to cybersecurity, to protect the interconnected digital networks as well as the internal electronic records systems of health-care institutions. However, experience suggests that the legal system, in particular privacy laws, has limited ability to prevent such breaches, or to provide the impacted persons with adequate compensation for the harms they incur.

While privacy laws provide for offences, punishable by fines or imprisonment, and in some instances, administrative monetary penalties, such remedies do not address the injury incurred by affected parties. Furthermore, they have little impact in preventing systemwide cyberattacks where no identifiable perpetrator can be found. Even where prosecutions have been taken against perpetrators who can be identified, the ability to obtain private compensation from such persons is limited.

The Ontario health privacy law, PHIPA, contains a provision for seeking damages from persons against whom an order, or successful prosecution, has been made. However, the scope for recompense is limited to "actual harm" — meaning personal injury, physical loss or financial loss — and if the breach was intentional or committed recklessly, damages "for mental anguish" up to $10,000. Establishing proof of such harm may be difficult, if not impossible.

The most likely scope for financial compensation can be found in the evolving common law tort of invasion of privacy, or as the leading case of *Jones v. Tsige* 2012 ONCA 32 characterized it, "intrusion upon seclusion." For liability to be found, the defendant's conduct must be intentional and they must have invaded, without lawful justification, the plaintiff's private affairs or concerns in circumstances where a reasonable person would regard the invasion as highly offensive, causing distress, humiliation or anguish. The courts have awarded damages against defendants in the range of $10,000 to $20,000.

Class action lawsuits, undertaken outside of the privacy laws against the organizations responsible for protecting the data, may provide some level of compensation to individual patients, and, while not a deterrent to unreachable perpetrators, should be an incentive for the health-care sector to invest in required enhancements to cybersecurity systems.

David Young is principal at David Young Law*, a privacy and regulatory counsel practice in Toronto.*

Photo credit / pandpstock001 ISTOCKPHOTO.COM

Interested in writing for us? To learn more about how you can add your voice to The Lawyer's Daily*, contact Analysis Editor Richard Skinulis at* Richard.Skinulis@lexisnexis.ca *or call 437- 828-6772.*