MediSecure data breach: Why is health data so lucrative for hackers?

May 20 2024, by Megan Prictor

Credit: Pixabay/CC0 Public Domain

The latest large-scale ransomware attack on a health technology provider, electronic prescription company MediSecure, was revealed last week.

MediSecure announced it had suffered a "cyber security incident" affecting people's personal and health information. Details of the attack are scant. We've been told it stemmed from a "third-party vendor," which means a company that provides services to another company.

In a general sense, ransomware attacks occur when a hacker gets access to a system, infects and locks up files, and then demands a ransom—usually in cryptocurrency—for their release.

Government agencies including the National Cyber Security Coordinator and Australian Federal Police are investigating the incident.

Cybercrime is big business, generating huge profits. This latest incident shines a light on the vulnerability of health data specifically.

What are e-prescriptions?

E-prescribing works by sending prescriptions to a digital exchange, essentially a secure database of prescription information. From there, patients control which pharmacy can access it, by showing pharmacy staff a token such as a QR code or barcode.

Electronic prescriptions contain personal information such as people's name, address, date of birth and Medicare number. They include details about prescribed medicines, as well as the prescriber's name, address and

other information.

The Digital Health Agency (an agency of the Australian government) reports that over the past four years, more than 189 million e-prescriptions have been issued by more than 80,000 clinicians.

Until late 2023, MediSecure was one of two national e-prescribing services, delivering prescriptions from health-care providers to pharmacies.

Last year, MediSecure was overlooked in a government tender process to appoint a single national e-prescribing provider. At that time, MediSecure held more than 28 million scripts.

MediSecure has noted the incident relates to data held by its systems up until November 2023.

While it's unclear who has been affected by this breach, the potential pool of patients and prescribers involved is large.

A worrying trend

This incident, which comes less than two years after the widely publicized Medibank hack, is alarming but unfortunately not surprising.

Health care is digitizing rapidly, with innovations such as patient-accessible electronic health records, remote monitoring and wearable devices. These developments can make health care more efficient and effective. They improve people's access to care, and mean that information—such as prescriptions—is readily available where and when it's needed.

Partly because of the scale of digital health data, breaches are very

common. The Office of the Australian Information Commissioner routinely reports that health services suffer the most breaches of any sector, mainly through malicious or criminal attacks.

Why is health data so lucrative?

Health data is very attractive to hackers because of its volume, and ease of access via system vulnerabilities. Historical under-investment in IT security in the sector, understaffing and overstretched staff (leading to human error), and high connectivity, all contribute to this risk.

Health data is also easy to ransom because of the value patients, clinicians and health organizations place on keeping it private. No one wants a repeat of the Medibank ransomware attack, where Australians' most sensitive health information—such as drug treatment or pregnancy termination details—was published online.

Beyond finding out how the MediSecure attack happened, patients want to know how to protect themselves from harm. At present it seems too early to say. The initial advice from the government is that no action is required.

Unfortunately, the usual measures we use to protect against hacks of financial and identity data don't work for health data. We cannot change our prescription or other medical history like we might change our passwords, get a new driver's license, or scrutinize our bank statements for fraud.

If someone's medication history is released it may indicate things about their health status, such as mental illness, gender transitioning, fertility treatment or care for drug and alcohol addiction. Not much can be done to stop the personal distress and stigmatization that may follow. People may be blackmailed through this information, or suffer harms such as

discrimination.

Data breach notification is a legal requirement on organizations to inform individuals about breaches affecting their data. It was touted as a solution to the problem of hacking when laws were introduced in Australia in 2018, but it doesn't help affected people very much in this situation. Being informed your prescription for an anxiety medication or a treatment for obesity is now public knowledge might simply cause greater distress.

Where does responsibility lie?

Hacking is a major threat to organizations holding health data, and the onus must largely be on them to protect against it. They must all have rigorous cyber-security protections, the capacity to respond rapidly when attacks take place, and resilience measures such as backups to restore systems quickly.

Patients are now taking steps against companies who don't protect their data. In the case of Medibank, affected customers have launched several class actions with the national privacy regulator and under Australian corporations and consumer law.

The introduction of a right to sue for serious invasions of privacy under an amended Privacy Act is an important, impending, change. It would mean people whose prescriptions and other sensitive health information were hacked could pursue breached companies for damages.

Companies facing heightened cyber threats, increased regulatory scrutiny and legal claims by those whose data has been breached find themselves in a tight spot. But so do patients, who watch unfolding news of the MediSecure attack, waiting to find out what information about their health may soon be on public display.

Provided by The Conversation