Protect your practice from cybercrime

Loryn Einstein is Managing Director at Medical Billing Experts.

Loryn Einstein provides an overview of the increasing incidence of cybercrime in medical practice, AND what to do about it.

Last week, a practice manager rang me in hysterics. She had opened an email that was sent to her by one of the doctors in her practice. Within moments of opening the email, the server for the entire practice was taken hostage and a ransom of several thousand dollars had been demanded. By the time she realised there was a virus in the email, it was too late.

When I sent my IT specialist out to her practice, he discovered that they had not done the most recent update of their server software and had left themselves vulnerable for attack. Further investigation revealed that the email account of the doctor had been hacked—the email with the ransomware had been sent by the hacker, not by the doctor. As a result, the practice had to close until they could access their practice software and their data. The practice had no recent backups which gave them no viable alternatives. They paid the ransom and their server was released.

The concept of criminals targeting our patient data was virtually unheard of a few years ago. But the digitisation of valuable patient information along with the emergence of highly sophisticated, well-funded global criminal outfits mean healthcare is now being targeted by cybercrime more than any other sector.

A March report by Trend Micro found that attacks on the healthcare industry accounted for almost one third of all data breaches worldwide, while 81% of healthcare executives say their organisations have been subject to at least one malware, botnet, or other cyberattack during the past two years, according to KPMG.

Last year, for example, sensitive information including patient names, social security numbers, birth dates and medical identification numbers of up to 80 million employees and customers was potentially stolen following a cyberattack on Anthem, one of the largest health insurers in the US. Earlier this year, the Hollywood Presbyterian Medical Centre was forced to pay a ransom of 40 Bitcoins, or about US$17,000, to regain access to their medical files after a ransomware attack.

Australia, with its widespread uptake of technology and strong economy, is now under increasing threat. The data analytics company Veda's 2015 *Cybercrime and Fraud Report* found that the Australian health sector would be squarely in the sights of cyber criminals due to the wealth of data it held and a weakness in its cyber defences. It's already happening: there was an attack on Melbourne Health earlier this year, when a virus infected all the computers at the Royal Melbourne Hospital's pathology department.

Private practice is not immune. In fact, small medical practices are a perfect soft target. Most have made limited investment in IT security and have not educated their staff in how to protect the practice from cyberattacks. Something as simple as a medical receptionist opening an email can now lead to the server for the entire medical practice being held for ransom. It's that quick and easy.

WHY HEALTHCARE?

Medical practices hold large amounts of highly valuable personal information in their practice software. Credit card numbers, personal details and sensitive health information can be combined to enable a number of criminal activities, including identity theft, fraud, access to pharmaceuticals and access to government benefits.

The Ponemon Institute estimates that a health record is worth about $20 on the black market, compared to about $2 for a credit card record. While a credit card can be easily cancelled and monitored, there are no such controls in place for health records, with many victims not even realising their data has been breached. Given that practices hold hundreds and sometimes thousands of health records, they are highly attractive targets for criminals anywhere in the world.

Another reason for the vulnerability of healthcare organisations is that they usually cannot afford to be offline. Cybercriminals know they can command a much higher ransom when their victims will go to extraordinary lengths to prevent downtime.

Unlike banks and retail businesses, which have been quick to put counter measures in place, the healthcare sector is woefully unprepared for this cyber onslaught. A recent US report from ESET and the Ponemon Institute, *The State of Cybersecurity in Healthcare Organisations in 2016*, found healthcare agencies in the US were averaging about one cyberattack per month. Yet only half had an incident response plan in place.

THE COSTS OF NOT BEING PREPARED

Becoming the victim of cybercrime can be costly both in terms of financial outlay and your reputation. Imagine the reaction of your patients if you need to inform them of a cybercrime incident. How would they deal with the fact that the personal information that they entrusted to your practice has fallen into the hands of a cybercriminal?

All organisations in Australia are required under the Privacy Act to "take reasonable steps to protect the personal information they hold from misuse, interference and loss, and from unauthorised access, modification or disclosure". This includes the preparation and implementation of a data breach policy and response plan.

If the security of your data is compromised, you may be required under the Act to notify every patient in your practice that their personal data may have been accessed by an unauthorised third party, and report this to the Office of the Australian Information Commissioner (OAIC).

At the very least, an attack will mean you will need to spend considerable resources on tracking the source of the breach and putting in place strategies to ensure it does not happen again. It is in every practice's interests to be prepared.

HOW TO PROTECT YOUR PRACTICE

The data of a medical practice is only as safe as its weakest component of software, hardware or IT service provider. Many of the recent cyberattacks have been easily perpetrated due to practices not doing something as simple as updating their server software. For a hacker, this is the equivalent of leaving your key in the front door of your office.

All your hardware and software should be properly maintained, and software updates always completed in a timely manner. You need to review data security risks regularly and take steps to introduce protection strategies. These might include advanced messaging solutions to help detect phishing scams, solutions that include specific anti crypto-ransomware technologies, top of the range Firewall and breach detection systems, and regular back-ups that mean you will be able to retrieve data faster if your system is compromised.

It is also essential you develop and maintain policies and procedures around data protection, and to ensure your staff are trained appropriately. All practice staff, including doctors and administrative staff, should err on the side of caution when opening emails containing attachments. They should also be kept aware of common phishing emails such as the recent spate of fake Australia Post and NAB emails, as well as emails purporting to have attachments regarding tax refunds from the ATO. All of the emails look legitimate on the surface and carry viruses in their attachments.

The Turnbull government recently announced a $230 million package of measures to beef up cyber security in Australia, including more powers for the Australian Corruption and Crime

Commission and Australian Federal Police, the creation of joint cyber threat centres, and the introduction of secure online sharing networks.

As part of the initiative, $15 million in grants has been made available to small businesses with less than 20 employees to have their systems tested and improved by accredited experts.

However, securing your data is not just about ensuring your own practice software and IT infrastructure is up to standard. Practices also need to conduct appropriate due diligence regarding IT security policies and practices in place for all vendors coming into contact with their practice software or patient data.

When selecting an outsourced medical transcription or medical billing company, the key questions you should be asking any third party vendor that comes into contact with your patient information are:

- Where is your vendor's data stored? Is it in a secure data centre or a server in a less secure location such an office?
- If the vendor stores data is it in a secure data centre and is that data centre located in Australia? [Note: The Privacy Act requires that all patient information is stored on servers in Australia]
- At what intervals does the vendor perform daily backups? Note: The more frequent the backups, the less data loss the practice will experience in the case of an IT failure]
- How are the backups stored? Are they in the same location as the server or in an alternate location? [Note: Storage of backups in a single location are more vulnerable to loss]
- How often is your vendor's backup data tested for its ability to be restored? Have these tests been successful? [Note: Simply having backups is not sufficient. The backups must be able to be restored to be of any use in the case of an IT failure]
- Are the vendor's backups encrypted to protect unauthorised access to the data?
- Does the vendor have a competent IT manager who is well versed in data security and protection?
- Is the vendor compliant with 2014 privacy legislation?
- Who is accessing your data whilst working for the vendor? Are the staff of the vendor located in Australia or is your patient information being viewed by staff in overseas locations?
- What security measures does the vendor have in place to protect your patients' data?
- How does the vendor educate their staff in the Privacy Act and other relevant legislation?

Small vendors, just like small medical practices, are not likely to have the requisite financial resources to purchase adequate IT infrastructure. It is essential that you conduct due diligence of all third party companies that you do business with, including outsourced billing companies and outsourced transcription companies.

Despite the ever evolving threat, most healthcare organisations aren't making the investment they need to keep their data safe.

This is no longer an option. The best advice is to keep yourself and your practice well informed and to rely on the experts to keep you safe. Ⓟ

ARE YOU OUTSOURCING YOUR MEDICAL BILLING OR TRANSCRIPTION?

Screen vendors carefully to protect your practice data

- Who is accessing your data whilst working for the vendor?
- Are the vendor's staff who are accessing the data located in Australia?
- Where is the vendor's data stored?
- How often is the data backed up?
- Are backups encrypted?
- Is the vendor compliant with privacy legislation?
- What security measures does the vendor have in place to protect your patients' data?
- How often is the vendor's data tested for its ability to be restored?