Understanding the Ransomware Threat

David Aafedt, Christianna Finnern, Gerald Fornwald, Cody Zustiak, and Chelsea Ahmann*

ran-som /'ransəm/

noun a sum of money or other payment demanded or paid for the release of a prisoner.

verb obtain the release of (a prisoner) by making a payment demanded.

Last August, cybercriminals released a ransomware attack that shut down computers in more than 400 dental offices around the United States. The attack targeted Digital Dental Record, a provider of IT software and data back-up services to dental practices.

Within the last few months, the information technology provider Complete Technology Solutions ("CTS") was also hacked, effectively shutting down the computers at more than 100 dental practices around the United States. CTS provided these practices with a range of services, including day-to-day operations, electronic patient records, and data back-up.

These two examples alone affected more than 500 dental practices, impacting what is conservatively estimated at more than one million patient records. We have provided incident response support to dentists and specialists impacted by these and other cyberattacks affecting practices in the upper Midwest.

Although readers are likely familiar with the general topic of ransomware, most are uncertain about the steps their practice should take to prevent such attacks, and what to do if a ransomware attack occurs.

Understanding Ransomware Threats

Ransomware is, at its essence, the release of malicious software that locks out a user from accessing its systems until a ransom is paid to the hackers. Hackers regularly target healthcare and dental providers because healthcare data is uniquely valuable on the black market, often containing all of a patient's personally identifiable information (PII) in addition to sensitive medical histories and financial information. A single attack compromising a dental or specialist practice with thousands of patients can reap quick gains for a cybercriminal, who may be able to fetch $80 to $250 per patient record on the black market, compared to $1 to $5 for a credit card number. In addition to financial gain, access to patient records can enable cybercriminals to:

- Fraudulently obtain health or dental care using a victim's insurance
- Gain access to opioids or other potentially dangerous prescription drugs
- Open fake accounts
- Extort ransoms from victims

Mitigating Ransomware Risks

Given the heightened target that cybercriminals have put on the backs of healthcare providers, it is critically important for dental practices to ensure compliance with HIPAA's security rule, which requires implementation of security measures that can help prevent the introduction of malware, including ransomware. Each dental practice should:

- Have a security management process, which includes performing a risk analysis to identify threats and vulnerabilities to electronic protected health information.
- Establish measures to mitigate or remediate those identified risks and regularly educate and train employees on detecting and identifying attempts to access electronic data through phishing attempts and other devious attacks.
- Ensure that access to health records is appropriately limited, both with respect to where they can be accessed and who can access them.

Importance of Patient Record Back-ups

While it is critical that your practice prevent improper access to health records, doing so is only one part of your duty. Under federal privacy laws and their state counterparts (such as the Minnesota Health Records Act), your practice also must ensure patient records are readily accessible. Of course, the best way to ensure such access is to maintain frequent back-ups of electronic records. However, our firm has worked with numerous clients who have no idea what scope of services are being provided by their IT and data security providers or the quality of their back-up systems.

Indeed, a long-time client recently contacted our firm after his entire practice's database, including all of his patient records, was locked down by ransomware. Upon reaching out to his local IT and data security provider for the patient records that were purportedly being backed up on the

Continued on next page

***Mr. Aafedt**, **Ms. Finnern**, **Mr. Fornwald**, **Mr. Zustiak**, and **Ms. Ahmann** are from the Dental and Health Care Group at Winthrop & Weinstine, representing dentists, specialists, and healthcare professionals in a variety of areas available at www.winthrop.com/health-law*

Continued from previous page

provider's servers (a service the practice had been paying monthly fees to receive), he learned that the IT provider had not been backing up his practice's records. As a result, against the advice of legal counsel, the practice paid the ransom. Even after paying the ransom, however, the practice was only able to recover about half of its patient records.

Why Quality IT Providers Matter

In each of these ransomware examples, the affected practices thought they were protected. Each hired what they believed to be a reputable IT vendor, paid for back-up services, and assumed they were receiving adequate security. In each instance, however, simply hiring an outside professional was not enough. The lesson from those examples is simple: trust, but verify. Your practice can, and should, regularly evaluate the IT services it is receiving. When evaluating an outsourced IT provider, take time at least every six months to make sure they:

- Back up your practice records automatically at preset regular intervals
- Maintain the same kind and quality of your back-up data as data in your office systems
- Enable access and use of backed-up information in almost real time
- Keep all back-up data on systems that are entirely separate from your practice's patient, administrative, and financial records

Know What is in Your IT Contract

It is also important to review your IT provider contracts, which routinely contain provisions that are incompatible with your own privacy obligations - or limit your remedies in the event of a breach. Such onerous provisions may include an IT provider's right to deny you access to your own electronic records, force practices to pay for security upgrades required by changes in the law, or even impose limitations on liability that will leave your practice holding the bag in the event of a security breach.

What to Do If Your Practice is Breached

If you find yourself the victim of a breach, it is imperative that you know your obligations and that you act quickly. Regardless of how many patients are impacted, you have a duty to promptly notify the specific patients whose records have been breached. You must also notify Health and Human Services' Office of Civil Rights. If the breach impacts more than 500 patients, the timing and extent of your notice requirements change, including the need to notify prominent media outlets in the states where your patients reside. These actions, while costly, distracting, and sometimes embarrassing, are absolutely necessary, and may spare you from increased regulatory scrutiny, fines, or other sanctions down the road.

> Never give ransomeware scammers your money. Doing so only invites cyber criminals to target you again.

While no practice is immune from cyber threats, how you react to a ransomware event can dramatically alter the resulting impact. Never give ransomware scammers your money. Doing so only invites cybercriminals to target you again. Moreover, paying a ransom does not guarantee that you will return to business as usual following payment. In the case of our client referenced above, the "released" data may still be compromised, the cybercriminal may still be using the data for his or her own use, or the underlying information may have already been duplicated and sold on the black market or the dark web. Above all, take the time to develop a thorough security policy, train your employees on how to handle electronic health records and identify cyber-threats, scrutinize the services you are receiving from your IT vendors, and know what your contracts say. Those simple ounces of prevention may save you the cost and headache of many pounds of cure. ■