REFLECTION

You Have Been Hacked!

Ed Bujold, MD, FAAFP

Family Medical Care Center, Granite Falls, North Carolina

ABSTRACT

On October 31, 2021, I learned the electronic health record in my independent, solo practice had been attacked by a Russian syndicate who was holding our data and our practice management system for "ransom." An encryption key could be given to our cloud provider once $5,100,000 was delivered in bitcoin to the hacking entity. After 3 long months of negotiations, with us going back to a completely paper-based system in the interim, our cloud provider paid the Russian syndicate and access was restored. There were many lessons to be learned from our experience. We were fortunate, and through the help of many of our business associates we were able to survive and live to see another day.

Ann Fam Med 2023;21:85-87. https://doi.org/10.1370/afm.2906

I have been in an independent, solo practice for 37 years. I have a staff of 9 employees which includes a nurse practitioner. My usual routine on the weekend is to log in to my electronic health record (EHR), review patient data, and make follow-up appointments for the next week. On Sunday October 31, 2021, I was unable to log in to my EHR. Our cloud-based data company has a 24/7 call center to address any issues we may have on weekends. I called their number and a recording stated, "Our phone system is currently out of order." I thought this was a bit odd, but didn't think much about it and figured this issue would be sorted out on Monday. My staff functions very much as a team and I assumed they would sort all this out and we would be up and running by the time I finished my hospital rounds on Monday morning.

I arrived at the clinic at 8:30 AM. I was informed by my staff all our computers were working but none of us had access to our EHR or our practice management (PM) software. Fifteen minutes later, I received an e-mail from our cloud provider informing us they had been attacked by ransomware. Ransomware is a type of malicious software designed to block access to a computer system until a sum of money is paid. I immediately called our cloud-based service to get more details. Our data (this included our EHR and our practice management system) was being held "ransom" and an encryption key would be given to our cloud provider once $5,100,000 was delivered in bitcoin to the hacking entity. Our cloud provider reached out to the FBI who was quickly able to determine the hacking entity was a Russian establishment preying on 2 to 3 companies daily. The FBI recommended hiring a cybersecurity team well versed in ransomware attacks to identify any additional threats. The cybersecurity team recommended containment procedures focused on limiting further damage, eradicating infected systems, wiping them clean and restoring them. This restoration requires systems to be rebuilt from backups; then recovery processes can be started to get everyone back online. In addition, the cloud-based service hired a professional negotiator. The cloud-based service had $2,100,000 in yearly gross revenue, much less than the $5,100,000 the Russians were asking to release the encryption key.

By noon of November 1, 2021, we knew our cloud-based service had an action plan in place, but the CEO had no idea when we would get our system back online. Naively, we thought we would have our PM and EHR up and running in a few days. After 2 weeks, my staff and I realized this was much more serious. Negotiations were going nowhere. In addition, we had not transmitted any insurance claims in 2 weeks because of having no access to our PM system. I have 4 interfaces to our EHR and PM; they include an accountable care organization (ACO), a major laboratory, a large hospital entity, and a data extraction company which pulls data from every

Conflict of interest: author reports none.

CORRESPONDING AUTHOR

Ed Bujold
Family Medical Care Center
4132 Hickory Blvd
Granite Falls, North Carolina 28630
bujold@embarqmail.com

patient record each night and prints a paper copy of each patient's *International Classification of Disease* (*ICD-10*) diagnostic codes, recent laboratory work, gaps in care, and the most recent updated list of patient medications. This document is known as a point-of-care (POC) report. The data extraction company had a server onsite which was not connected to the cloud-based provider and therefore was inaccessible to the Russians and their ransomware. As a result, we had accurate information on patients dating back to 1 day (October 30, 2021) before the ransomware attack. This proved invaluable as we had a mini version of each patient's chart in paper format.

Our first item of business was to reestablish cash flow. We electronically submitted our insurance claims through Payer Path, a claims management system, which was embedded within our PM system. Payer Path has an online site, and with a bit of instruction from our EHR provider, we were able to start transmitting insurance claims through this encrypted online site.

Next, we went back to a completely paper-based system just like in the "good old days." Our ACO and POC documents were printed daily and became our patient charts. Our laboratory and hospital reports were tracked and printed daily through an online access point. Prescriptions were written by hand on printed prescription pads.

Finally, we needed access to cash until we could establish cash flow again. I have a longstanding relationship with my certified public account (CPA) and bank. After explaining our predicament, we were able to establish a much larger business line of credit based on their recommendations.

After 3 long months of negotiations, my cloud provider paid the Russian syndicate $500,000 and they produced the encryption key providing access to our EHR and PM systems. Ironically, during this time frame I spent more time with patients, less time documenting medical records, and on average, left the office 1 hour earlier.

On a parallel track, our cloud company couldn't tell us if any patient's personal information had been exposed. This flies right in the face of HIPAA compliance issues.[1] I contacted our malpractice insurance company; fortunately they have a division of cybersecurity. Our cloud-based company believed there was no exposure to any individual patient's personal information, but they couldn't prove it. Our legal counsel suggested we had to assume there was a violation even though we could not prove or disprove it occurred. If an investigation was opened with the HIPAA compliance division of the federal government (which it eventually was), we wanted to make sure we were complying with the letter of the law. The Justice Department required we set up a patient call center. The legal team set up a guide for patients of steps to be taken if their private information was accessed by this Russian syndicate, sent letters to patients, notified our local news outlet, etc. We were lucky to have such experts at our side during this difficult time.

As of March 2022, we have a fully functioning EHR and PM and 3 of our 4 interfaces are functioning. Our POC interface was online by October 2022. Five years ago, we moved to a cloud service because it was a much cheaper alternative to maintaining servers on site. As our EHR software became more sophisticated, the hardware to support it became more expensive with each upgrade. Our EHR provider recommended a cloud-based provider specializing in small practices. This provider housed data for over 100 small medical offices on the East coast and was very reasonably priced. In the aftermath of the attack, we learned the company was underinsured for a ransomware attack and their backup protocols were not up to industry standards. Once our data was restored, we moved to a much larger cloud provider who backs up our data nightly and stores it in 3 different cities. It cost $8,000 to move to a more secure cloud service (also recommended by our EHR provider) and we recovered almost all our lost revenue by March 2022.

LESSONS TO BE LEARNED FROM OUR EXPERIENCE

First and foremost, have a trusted computer consultant to manage your hardware and have them do a cybersecurity check yearly, which should also include a very frank discussion with your staff about potential cybersecurity risks and vulnerabilities in your practice. This consultant is as important as a good CPA and banker for a small practice.

Your entire team should limit the number of devices connected to the Internet. Your trusted computer consultant can show you how to do this. Each connected device provides another access point through which ransomware can gain access.

The Cybersecurity and Infrastructure Security Agency (CISA) recently published "Cybersecurity Incident and Vulnerability Response Playbooks."[2] In it, they describe 6 phases of incident response: preparation, detection and analysis, containment, education, post-incident activity, and coordination. You may not want to take on this responsibility, but your trusted computer analyst should.[3]

The FDA recently posted an alert detailing how vulnerable medical devices are to ransomware attacks.[4] Attacking agents are known as Black Hats. Black Hats are defined as human agents seeking control over another person's devices for nefarious purposes. They come in 3 varieties: the thief stealing data—be it intellectual property, passwords, or credit cards; the vandal—wreaking havoc and destruction via something called a denial-of-service attack stopping a service from functioning; and the soldier/assassin, who goes the vandal one step better and seeks to cause death/damage via attacks on critical infrastructure (think remotely opening flood gates on a large dam). It is important to realize the same prop (a computer virus) can be used singly or in combination with other props to satisfy any of the above-mentioned motivations.

According to the Trust Wave Global Security Report of 2019, a single patient record or piece of personal data is worth $250 on the "black market." These ransomware attacks

are multibillion dollar businesses and very profitable for these criminal elements. They aren't going away anytime soon.

These attacks are starting to affect patient care all over the world. We were able to move back to the paper world quickly and fortunately had a scaled-down paper version of our EHR data available. We were lucky. The hundred other practices involved in this attack were not so fortunate. Many small medical practices never recover from a ransomware attack and file for bankruptcy.

Someday, an adverse cyber attack may occur affecting someone's life and potentially result in a death. Based on our experience I strongly recommend practices prepare for such attacks ahead of time.

Read or post commentaries in response to this article.

Key words: ransomware attack; independent practice; cloud-based data storage; HIPPA violations

Submitted April 29, 2022; submitted, revised, September 19, 2022; accepted September 27, 2022.

REFERENCES

1. Langer SG. Cyber-security issues in healthcare information technology. *J Digital Image*. 2017;30(1):117-125.
2. Cybersecurity and Infrastructure Security Agency. *Operational Procedures for Planning and Conducting Cybersecurity Incident and Vulnerability Response Activities in FCEB Information Systems*. Published Nov 2021. https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf
3. Perakslis E. Responding to the escalating cybersecurity threat to health care. *NEJM*. 2022;387:767-770. 10.1056/NEJMp2205144
4. US Food & Drug Administration. The Role of the FDA to Advance Cybersecurity: https://asprtracie.hhs.gov/technical-resources/resource/4331/the-fdas-role-in-medical-device-cybersecurity