Cracking Encryption: Despite Benefits, Technology Still Not Widely Used to Combat Multi-Million Dollar Breaches

By Mary Butler

In movies and on television lately, Hollywood has made encryption and decryption look exciting, glamorous, and world-saving. The film *The Imitation Game* and the BBC show *The Bletchley Circle* chronicle how British code breakers decrypted military strategy codes from the Nazi encryption tool called Enigma. History buffs know that decryption technology and the military advantage it provided shortened World War II by an estimated two years, saving untold thousands of lives.

Encryption and decryption—particularly encryption—is still a high stakes game today when it comes to protecting valuable data like personal health information.

Hackers and thieves, the enemies of secure health data, are waging a war against hospitals, insurers, Wi-Fi networks, and patients whose information is stored and transmitted by those entities.

The last several years have seen massive data breaches compromising the protected health information (PHI) of millions of people. In January, the thieves who hacked insurer Anthem, gained access to the names, birthdates, medical ID/Social Security numbers, addresses, employment information, and income data of an estimated 80 million people—the largest breach to date as of press time. And in August 2014, a group of Chinese hackers breached Community Health Systems' network, which stored the patient data of 4.5 million people. These breaches came shortly after the Federal Bureau of Investigation warned healthcare providers that hackers were expected to target facilities in the healthcare industry due to lax security practices.

One of the best tools for fighting breaches is data encryption, which health information management (HIM) professionals define as "the process of transforming text into an unintelligible string of characters that can be decrypted when it reaches a secure destination."[1]

While encryption can't prevent every kind of breach out there, it can lessen the blow when data is stolen by preventing sanctions from the government. If an encrypted device is stolen, the information is considered inaccessible by hackers and the Department of Health and Human Service's (HHS) Office for Civil Rights (OCR) waives monetary penalties. In other words, encryption is a "get out of jail free card" of sorts when done properly.

But even with perks like that—as well as preventing the loss of millions of dollars in fines and credibility with the public—healthcare entities have been slow to jump on the encryption bandwagon. Much of that is due to myths surrounding encryption. Healthcare organizations are concerned that encryption will slow down a number of operations, such as electronic health record (EHR) system functions, web portal communications, and business processes. Another concern is cost—though the costs of encrypting databases, mobile devices, data at rest (data that's stored), and cyber insurance policies vary broadly. Encryption also doesn't come with an easy or readily measurable return on investment, which can make it hard to justify during budget negotiations. Finally, for privacy officers, HIPAA is frustratingly vague on encryption requirements. Chris Apgar, CISSP, CEO of Apgar Solutions, which helps healthcare organizations perform HIPAA Security Rule risk analyses and build security response plans, notes that while the HIPAA Security Rule talks about encrypting laptops versus encrypting e-mail, it's not specific about how to do it.

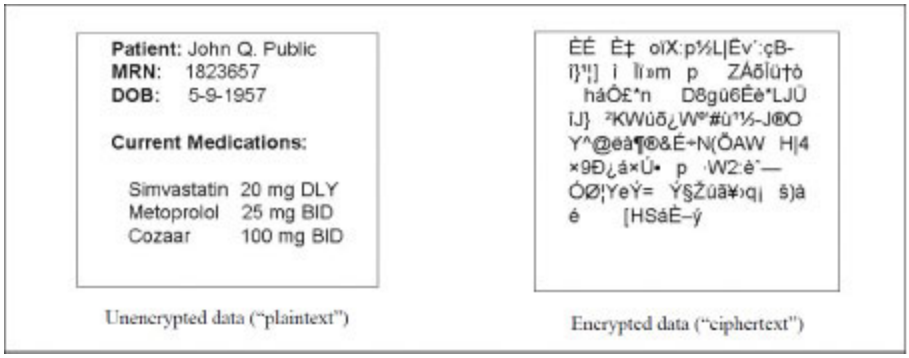
But the rewards of having stringent data protection programs—whether through encryption alone or encryption combined with other measures—are enormous as long as an organization knows what to encrypt, can identify why they're encrypting, and can see through the myths.

The healthcare industry is coming around to encryption, slowly but surely, security experts say. With an increasing number of data breaches occurring as the result of stolen laptops, encryption is getting a second look from many providers. According to

a 2014 Bitglass analysis of HHS breach reports, 68 percent of healthcare data breaches since 2010 were the result of lost or stolen files or devices. Forty-eight percent of breaches involved a laptop, desktop, or mobile device.[2]

How Encryption Works

One of the hurdles to getting organizations to adopt encryption is conveying its importance to senior management in terms they can understand. In layman's terms, encryption turns text data—such as information considered "sensitive," like PHI—into an undecipherable stream of characters, like this:



Graphic credit: Sharon Lewis, MBA, RHIA, CHPS, CPHQ, FAHIMA, Primeau Consulting.

Usually there is software or another mechanism that de-identifies the data in the original message so that only individuals who have a key—such as a password or another multifactor authenticator—can decrypt the data.

Health data security experts say that data sent around and within the same organization (a closed network) usually doesn't need to be encrypted. But if it's being transmitted outside of an organization, especially if it's PHI, it should be encrypted.

There are also different levels of encryption, and the strength is determined by a mathematical algorithm—depending on the algorithm, the encrypted data may or may not be considered secure. Healthcare organizations can look to organizations such as the National Institute of Standards and Technology (NIST) to provide recommendations for the level of encryption needed to protect various devices.

Encryption strength is measured in bits. For example, encryption strength for a laptop and its disk size might be 56 bits, which can be cracked in three days by someone who doesn't have the key or passcode. On the other hand, it could take six months of quantum computing to crack something employing 128-bit encryption, such as a large database, according to Apgar.

But as other experts have noted, encryption only works when the people using the data are properly trained. For instance, with some encryption technologies data on a laptop is only encrypted when the laptop is closed or shutdown. If a user walks away from the laptop the data is not secure until the system automatically signs the user out after a set period of time.

"In essence disk encryption technologies can be bypassed if an attacker gets a hold of the computer while it is sleeping or waiting for a password prompt. The attack exploits RAM chips in laptops that aren't cleared of data when the laptop is turned off," Bowen says.

To be certified for stage 2 of the "meaningful use" EHR Incentive Program, eligible professionals or hospitals "must conduct or review a security risk analysis that includes addressing the encryption/security of data stored in certified EHR technology," according to the program's final rule. For providers working on meaningful use, encryption should be a priority.

"If I'm using an EHR system, entering or updating patient records in the electronic system, then encryption should be seamless to the user," Bowen says. "They would be viewing the application inside a secure network,

and once they hit 'save' it would push that data to a database that automatically encrypts the data when it is no longer being accessed or used."

Encryption: Where to Start

Any dutiful security and encryption expert is going to advise a provider to hire a consultant to help implement an encryption strategy and select a vendor. But before they even get that far, Chris Bowen, MBA, CIPP/US, CIPT, founder and chief privacy and security officer at ClearDATA, says it's important for companies to know where their data is, literally. Does the data live in secure database rooms, or on laptops, EHRs, and mobile devices?

"Find out where your data is at, understand the safeguards around where that data is at, and then do what you'd normally do in any security risk analysis, and understand where your gaps are," Bowen advises. "Eliminate those gaps, then prioritize high severity items first."

This is exactly what Traci Waugh, RHIA, CHPS, CHC, senior director of compliance at North Valley Hospital, in Whitefish, MT, did when her facility first implemented encryption technology. Even though North Valley is a small 25-bed critical access hospital, the data they're protecting is valuable, says Waugh, who is also a member of AHIMA's Privacy and Security Practice Council. And because of its size, the cost of a breach at North Valley would hit very hard financially.

Waugh says her facility underwent a risk assessment, and the results uncovered vulnerabilities that helped her convince senior management that encryption and other security measures were worth the investment. Waugh found that the hospital's liability insurance had started offering a cyber liability plan, which, while it doesn't cover the cost of encryption or an OCR fine, it would help pay for fees associated with sending notification letters, getting outside public relations help, and publishing the required notices in the wake of a breach.

Waugh and her team also moved forward with a plan to encrypt every mobile device that the hospital deploys, such as laptops and iPads. They also chose to auto-encrypt e-mails when PHI is being transmitted. This decision was met with resistance by physicians and others in the organization who felt this slowed down their processes. In this case, the notion that encryption is slow turned out not to be a myth, but a reality.

Recipients had a hard time retrieving an encrypted message as well. After dealing with negative feedback, Waugh and her team changed the policy, leaving the decision to encrypt an e-mail in the hands of the sender. This step requires just one extra click for the sender, though the recipient still has to go through a couple steps to retrieve it. But overall Waugh described the process as "not too painful."

Elisa Gorton, RHIA, CHPS, MAHSM, assistant director of HIM and privacy officer at St. Vincent's Medical Center in Bridgeport, CT, says the cost of encryption and the potential for slower e-mail sending and receiving are the price organizations may pay for securing their systems. At St. Vincent's, e-mails leaving the organization are automatically scanned as they leave their internal e-mail system. The system will detect certain wording and numbering conventions that could be, or are, Social Security numbers or phone numbers, credit card numbers, account numbers, medical record numbers, etc. The system then sends an automatic reply back to the sender informing them that the e-mail did not transmit. The organization has a policy and procedure for encrypting such e-mails and when they are encrypted the email is transmitted. Gorton's organization also encrypts mobile devices owned by the hospital.

St. Vincent's e-mail security program is robust, but Gorton knows there are weaknesses in any organization. She says that in the back of her mind she's always worried about a person who uses their own personal mobile device for work. "I think that's always going to be pretty much where I see our greatest risk right now," she says.

Barriers to Encryption Adoption

Security of systems is always going to compete with revenue generating projects, says ClearDATA's Bowen. Some hospital management, or practices owned and run by physicians, will look at the financial cost of encryption—whose value can't be measured for a long time—weigh it against profit generators such as new surgical and radiology wings, and come to the conclusion they should put off encryption.

However, not every type of encryption is expensive. Apgar, who regularly reviews security products, says encrypting laptops can cost up to $150, but laptops can also be encrypted with USB devices that cost $15-$20 or less. Mobile devices such as Windows, Android, iPhones, and iPads are natively encrypted. Physicians can purchase encrypted text messaging platforms—which allow them to text message patient information to each other. Without encryption, the stakes are much higher. The loss of an encrypted laptop can cost an organization as little as $300 to replace it. However, a stolen unencrypted laptop can cause an organization millions of dollars in penalties and breach-related costs, and potential harm to patients.

Fortunately, security experts are seeing positive trends toward physicians and hospitals embracing encryption; it's just been slow in coming. But the recent string of large-scale breaches, both in retail and healthcare, are starting to sway healthcare providers to encrypt. Bowen says he's seeing this in his own cloud security firm.

"I see a trend absolutely going in that direction," Bowen says. "If you see the new protocols for sharing data, you'll see data protection and encryption built into the technology a lot more than the old days. That said, when you're dealing with a legacy system, [like] Anthem or others, it's harder to shore those things up.

"So the new things you're seeing coming out are really trending in the right direction."

Still, physicians need more education on security and encryption if they're going to be compliant. It's not that physicians don't want to communicate securely or protect their patient's information. "What they want is to be able to access the data in a way that allows them to care for the patients," Bowen says. "So sometimes they'll say 'I'm going to send this text of my patient chart, how can we act?' And it's just easier to communicate that way sometimes.

"They don't do it purposely, but a lot of physicians will bypass group controls because they need to make a decision in treating a patient in a very urgent manner. You can't fault them for that."

It's not just physicians who are slow to encrypt, but even senior executives, says Michael Frederick, CISSP, and Steven Penn, CISSP, ISSMP, ISSAP, CAP, HCISSP, both of the Frisco, TX-based HITRUST Alliance.

"The problem is when you start talking about the cyber security stuff, nobody believes that what you're saying is real. They think you're talking about a Tom Clancy novel," Penn says. "Some of them view the computer as this mystical box that just does things and [they] don't understand it. When you talk about cyber security stuff, and when you bring up state actors like Russia and China and organized crime, they really start to think you're spinning science fiction here. Hopefully the silver lining in some of the events that have transpired over the last 12 to 18 months, those types of issues are being shown to be real."

What to Encrypt, Remaining Vulnerabilities

In a perfect world, not only would every mobile device, every e-mail sent, and every EHR be encrypted, but so would data stored within servers, at rest, and in transmission. That would be the "holy grail supreme," according to Frederick and Penn. HITRUST is an organization that assists healthcare organizations with the implementation of cybersecurity systems by providing them with a cybersecurity framework tailored to each type of organization. They are also working with state governments to develop regulations around cybersecurity—regulations that are harder to achieve at a national level.

The easiest way to do this is by building security features such as encryption into the very beginning of the security lifecycle. But both Frederick and Penn note that one of the challenges of knowing what and how to encrypt is deciphering what the HIPAA Security Rule says about it. HIPAA guidelines are purposely vague so as not to be interpreted as prescriptive. With technology evolving so quickly, the government didn't want to tell stakeholders exactly how to encrypt their data.

As a result, it can be hard for organizations' security professionals to articulate their encryption needs to senior management. If an upper management official doesn't like how the IT department says something must be done, there isn't a lot in the HIPAA Security Rule saying that "x" has to be done.

"Even in those items that it [HIPAA] considers required, there is always use of the terms 'reasonable' and 'appropriate' and I tend to read those terms and think, 'That means "to be defined later by an attorney."' So I like to avoid those situations," Frederick says. "When they released that initial information or initial rule, they left it vague on purpose not realizing we're moving into the healthcare space. They needed little more than a vague rule to work with."

Even if a healthcare organization follows the government and industry best practices to the letter, nobody is 100 percent safe from a security breach. Organizations need to stay up-to-date on all of their vendors' security patches and updates since hackers are routinely testing new system weaknesses. For example, with the Anthem breach, the hackers manipulated authorized administrators to give them their credentials in order to access Anthem's database and run a query. Having that data encrypted on disks wouldn't have prevented the breach, Penn says.

Apgar points out that while encryption is great protection, it's useless unless the individuals using and deploying it have the right training. "The biggest risk out there [is if] people just focus on the technical safeguards, especially when you're working with vendors," Apgar says. "Your biggest risk is on the people side. If you don't have administrative safeguards in place, it doesn't matter what you do, you're going to land yourself in trouble."

The perfect example, he says, occurred when he and his wife were driving cross-country and Apgar's wife saw a home health nurse doing her charting on an unsecured network at Starbucks. In addition to using an open and unsecured Wi-Fi connection, the nurse had PHI on her laptop screen, easily readable by anyone who walked past her.

To that end, Penn and Frederick both say that even a massive breach like Anthem's isn't the worst kind of healthcare privacy breach, though to be sure, it's not a scenario anyone wants to live through. The most dangerous security risk is hackers who find a way into a hospital's networked medical devices—such as morphine IV lines, insulin pumps, pacemakers, and heart and oxygen monitors—and manipulate the operation of those devices.

"There is a large risk out there for life and limb for patients hooked to these devices and decisions that are made on information rendered in them," Frederick explains. "Historically with medical devices the device manufacturers have resisted providing malware protection, or secure network connectivity."

This leaves medical devices vulnerable to cyber terrorism. All it would take is for one hacker to install a malicious code causing one of these devices to malfunction. Although this might sound paranoid, it helps put encryption in perspective.

"We have been talking about security and encryption in the context of a breach, and people having their personal information stolen. When it comes to healthcare… that is probably the best case scenario for what could happen in a breach," Frederick says.

Notes

[1] AHIMA. *Pocket Glossary of Health Information Management Technology.* Chicago, IL: AHIMA Press, 2012.

[2] Bitglass. "The 2014 Bitglass Healthcare Breach Report: Is Your Data Security Due for a Physical?"

Reference

WinMagic Data Security. "Data Encryption Demystified: Seven Common Misconceptions and the Solutions That Dispel Them."

Mary Butler (mary.butler@ahima.org) is associate editor at the *Journal of AHIMA.*
