When Security Breaches Don't Have to Be Reported

New technologies allow healthcare organizations to ensure - and prove - that protected health information stored on mobile devices is never exposed.

iHT2
Institute for Health
Technology Transformation

Contributing Executives

Nathan Gibson
Director of IT Operations & Privacy Officer
WVMI Quality Insights

Lance Mueller
Director of Forensics
Magnet Forensics

Jeff Pelot
CIO
Denver Health

Stephen Treglia, Esq.
Legal Counsel, Investigations
Absolute Software Corporation

Foreword

2014 was a year of healthcare data breaches. Experian noted that 46% of all breaches their data resolution serviced in 2013 were healthcare related, and this number is expected to rise. The proliferation of digitized PHI, lack of comprehensive risk mitigation strategies, omnibus rulings and increased audits all served to create a hotbed for breaches. Data is big business and healthcare data makes for an excellent pay day for cybercriminals – it is very valuable on the black market.

In the past five years, 31.4 million people in the US have had their Protected Health Information (PHI) compromised in privacy and security breaches. To address this, industry regulations such as the Health Insurance Portability and Accountability Act (HIPAA) are tightening. These regulations put the onus for data security firmly on the healthcare organization. And as we've seen, failure to comply can result in costly penalties and severe reputational damage.

In an age of electronic health records, mobile devices, and a mobile workforce, keeping PHI secure is challenging. While much emphasis is placed on securing the network from hackers, over three quarters of breached healthcare records are as a direct result of lost or stolen devices.

While these challenges have increased the number of attack vectors, it is possible to succeed in securing healthcare data. IT vendors, healthcare organizations, and regulators are working together to ensure that data security solutions and strategies are constantly evolving to stay ahead of cybercriminals.

This paper has drawn insight from industry analysts, data security specialists, and healthcare IT leaders to form some interesting perspectives on the trends, shortcomings and implications with regard to data breaches, regulatory compliance and security strategies for healthcare organizations.

Waco Hoover
Executive Director
Institute for Health Technology Transformation (iHT^2)

Table of Contents

Introduction

The shift from desktops to laptops and mobile devices, combined with the increasing mobility of healthcare workers and the rapid growth of medical identity theft, has created a new healthcare security environment. To address the risks in this new world, healthcare IT security professionals must not only protect their computer networks; they must also use the latest technologies to secure the data on mobile devices used by healthcare professionals.

Healthcare is especially vulnerable in this respect. Lost or stolen mobile devices account for 39% of the security incidents in healthcare, and for 78% of the records that are compromised.[1] With criminals targeting laptops and tablets for the hundreds of medical records they contain, the importance of securing mobile devices cannot be overstated.

Security breaches can have very serious consequences for healthcare providers because of the federal and state regulations of protected health information (PHI). Large-scale security breaches can result in huge fines for healthcare organizations. Providers must also report security incidents to the government, to the affected patients, and in the most egregious cases, to the media. Class-action lawsuits can result in millions of dollars in damages. And even a well-regarded institution can have its reputation ruined by a major breach that involves thousands of patients.

Despite the devastating impact of such incidents on healthcare providers and on their patients, an astounding 41% of healthcare providers don't encrypt their endpoints.[2] And although federal law doesn't require encryption, penalties are severe for incidents in which unencrypted data is compromised. Moreover, encrypting devices may qualify healthcare organizations for a "safe harbor" that exempts them from the need to report certain security incidents. However, organizations must be able to prove that encryption was in place and operating at the time that a device went missing. Auditors will not accept assurances; they will want proof.

Encryption is only one part of a larger security strategy that healthcare providers must adopt to manage mobile devices and protect PHI. Besides deploying encryption, organizations should layer endpoint security and management software, institute policies prohibiting data storage on endpoints, train their staff thoroughly, and perform comprehensive security risk assessments. With all of these components in place, healthcare systems can greatly reduce the chance of security breaches.

Encryption is only one part of a larger security strategy that healthcare providers must adopt to manage mobile devices and protect PHI.

Mobility in Healthcare

A high percentage of physicians now use mobile devices in their clinical work. In a recent survey, 100% of responding doctors and mid-level practitioners said they used laptops; 86% used smartphones; and 53% used tablets. Nearly half of the respondents used all three kinds of devices.[3]

A high percentage of physicians now use mobile devices in their clinical work. In a survey, 100% of responding doctors and mid-level practitioners said they used laptops; 86% used smartphones; and 53% used tablets.

Healthcare professionals carry mobile devices outside of healthcare facilities. According to one study, about a third of healthcare employees work outside their offices at least once a week, and it can be presumed they take mobile devices with them.[4] Physicians are especially prone to travel with laptops if they practice in multiple facilities or take work home, according to the participants in the report.

In a Health Information Management and Systems Society (HIMSS) survey of health IT professionals, 80% said that physicians used mobile technology to facilitate patient care in their healthcare organizations, which were mostly hospitals or hospital systems. The most widely used mobile solutions were laptops and computers on wheels (COWs), but tablets were quickly growing in popularity.

Most respondents said that their organization provided clinicians with mobile devices to support their daily work. The largest number (89%) provided laptops, followed by COWs (87%), pagers (59%), smartphones (53%), and tablets designed for healthcare (47%). Three-quarters of the executives said their institution planned to expand the mobile devices offered to clinicians.[5]

Meanwhile, many physicians and other clinicians bring their personal laptops and handheld devices to work. This shift towards BYOD and mobile workers presents some difficult challenges to health IT security teams.

Black Market for PHI

Stolen medical records are very valuable to thieves. While stolen credit card information can sell for about $1 and personal identification information for $10-$12, patient records command $20-$50 each on the black market. A complete dossier, including a driver's license, health insurance information and other sensitive data, can fetch over $500.[6-8] Medical identity theft can be used in schemes to defraud payers or to obtain healthcare services fraudulently.

Security breaches have had a significant adverse impact on patients and healthcare organizations. Forty-three percent of all reported identity thefts in the U.S. in 2013 were medical identity thefts, and the number of victims shot up from 1.42 million in 2010 to 1.85 million in 2012.

With the digitization of healthcare information, there has been a vast upsurge in PHI theft. From 2012 to 2013, the volume of records included in data breaches involving more than 500 records jumped 138%. Theft accounted for 83% of the records that were compromised in 2013[9]. Given the value of the data stored on a mobile device, it's no surprise that stolen devices account for the lion's share of compromised data.

Security breaches have had a significant adverse impact on patients and healthcare organizations. Forty-three percent of all reported identity thefts in the U.S. in 2013 were medical identity thefts, and the number of victims shot up from 1.42 million in 2010 to 1.85 million in 2012. These people suffered financial consequences from lost health insurance, higher insurance premiums, lost time and productivity, lowered credit scores, and legal costs. The average out of pocket cost per person was $18,660 per incident.[10-11]

Healthcare organizations will also experience significant financial harm as the result of a security breach. Under the HIPAA Omnibus Final Rule, healthcare organizations that fail to protect PHI can be fined up to $50,000 per violation[12]. Most states also have privacy laws that require notification of patients and specify civil penalties for unauthorized disclosures of personal information, including PHI[13]. Moreover, security breaches have elicited class action suits, each involving thousands of patients. Finally, providers must contend with the financial consequences of a diminished reputation in the community.

Regulatory Landscape

HIPAA Security Rule

All healthcare providers must comply with the HIPAA security rule which includes six sections:

1) General rules
2) Administrative safeguards
3) Physical safeguards
4) Technical safeguards
5) Organizational requirements (including business associate agreements)
6) Policies and procedures and documentation requirements

The security rule states that some implementation specifications are required, while others are "addressable", that is, organizations must either use them, show they are using another approach that is just as good, or explain why the addressable specification is not relevant to them[14].

The security rule states that some implementation specifications are required, while others are "addressable", that is, organizations must either use them, show they are using another approach that is just as good, or explain why the addressable specification is not relevant to them.

Among other things, compliance with the security rule requires healthcare organizations to:

- Determine goals of incident response, including an understanding of what constitutes a true security incident
- Decide how to respond to security incidents, including the establishment of a reporting mechanism and a process to coordinate responses to incidents
- Mitigate harmful effects of security incidents
- Document security incidents and their outcomes
- Create a data backup plan and a disaster recovery plan, including procedures to create and maintain retrievable exact copies of PHI
- Establish procedures to restore any loss of data
- Formulate policies to limit physical access to electronic information systems and the facilities in which they are housed
- Conduct an analysis of physical security vulnerabilities
- Implement policies that govern the receipt and removal of hardware and electronic media containing PHI into and out of a facility, as well as the movement of such items within a facility
- Apply policies that protect PHI from improper alteration or destruction
- Identify users authorized to access PHI
- Identify any possible unauthorized sources that may be able to intercept the information and modify it
- Implement a mechanism to encrypt PHI whenever deemed appropriate[15]

Breach Notification

Under the HITECH Interim Final Rule (IFR) on breach notification, HIPAA-covered entities, including healthcare organizations, must notify affected individuals following the discovery of a breach of unsecured protected health information. Such notification must be made within 60 days after the discovery of the breach.

All security breaches must be reported to the Department of Health and Human Services (HHS). These reports can be annual, but incidents involving the records of 500 or more patients must be reported within 60 days. The media must also be notified of these large security breaches.

Safe Harbor

HIPAA regulations offer a "safe harbor" that exempts organizations from having to report security incidents under certain circumstances. If an organization can show that the PHI on a mobile device was not compromised and that it was deleted, the security incident is non-reportable.

This is a huge advantage for healthcare organizations. If an incident does not have to be reported, it cannot trigger an investigation, and patients do not have to be informed. That eliminates the potential for an individual or a class action lawsuit, as well as adverse publicity.

To fall into this safe harbor, data must be encrypted. However, encryption alone is not sufficient. For example, an employee may deactivate encryption because they consider it to be bothersome (slows down the device, multiple logins, etc.). Or a disgruntled employee may target the data themselves – in which case they already have the encryption key. And sometimes it's simply human error, where an employee keeps their encryption key details with the device. There are also other possibilities: for instance, an armed robber recently stole a laptop from a physician on the staff of Boston's Brigham and Women's Hospital and forced him to yield his password.[21]

So it is crucial to be able to prove that the device was fully encrypted at the time of the incident and that no files were accessed.

"If you can prove that everything was in place and that nothing was accessed or lost, there has been no breach of data, so you don't have to report a breach," states Stephen Treglia, legal counsel for Absolute Software, a Vancouver-based security software firm. "That's what the HIPAA rules say: if there's a low probability that the data has been breached, and no data was lost, there is no breach and it doesn't have to be reported."

Lance Mueller, director of forensics for Executive Forensics, which helps forensic specialists find and analyze legal evidence on computers, agrees. If a healthcare organization can show that encrypted data hasn't been compromised before they delete it from a mobile device, the security incident is not reportable.

"From a technical perspective, there was a security breach, but you can prove the data is secure," states Mueller. "And under HIPAA, the requirement to report has to do with the data being exposed. If the bad guys stole the computer, but I can show I deleted the data before they accessed it, then I don't have to report it. It's not a reportable offense."

The most important technical safeguards for PHI on mobile devices are encryption and endpoint security software, which enables security personnel to protect and manage mobile devices remotely. Neither of these strategies can ensure security alone; but together they offer the best chance of preventing data exposures. Of course, they should be used in combination with robust policies and procedures, enforcement, and education. The following sections explain these approaches and how they should be used to secure mobile devices.

> **If you can prove that everything was in place and that nothing was accessed or lost, there has been no breach of data, so you don't have to report a breach," states Stephen Treglia, legal counsel for Absolute Software, a Vancouver-based security software firm.**

Policies and Procedures

When mobile devices began to gain popularity among clinicians, healthcare providers were caught off guard. But in recent years, most hospitals and health systems have expanded their formal security policies to cover mobile devices. Sixty-eight percent of respondents to the HIMSS survey reported that their organization had a mobile technology plan in place in 2012, up from 38% in 2011. Another 27% of respondents said their organizations were developing such a plan.[16]

What should these policies include? Among the recommendations of a Forrester Research report on improving mobile data security are the following:

- *Move controls closer to the data.* This strategy includes full disk and file-level encryption of mobile devices so that if criminals steal these devices, they cannot access the PHI on them. Also, desktop virtualization and prohibitions on local storage of data can be very helpful.
- *Discover where the data is located, diligently control access, and watch user behavior.* This is a matter of tracking where data is being stored and limiting access to those people whose job function requires it.
- *Focus on behavioral changes, not simply security awareness, for data security and policy.* Employee awareness and behavior are critical aspects of protecting data on mobile devices. Security incidents involving lost or stolen devices are often the result of carelessness. Staff should be made aware of the corporate and personal consequences of inappropriate actions.[17]

Periodic security risk assessments that include mobile devices are another essential element of a security strategy, says Nathan Gibson, director of IT operations/privacy officer, WVMI Quality Insights. "It's really important to perform a security risk assessment, so all aspects of security are addressed," he stresses.

Periodic security risk assessments that include mobile devices are another essential element of a security strategy, says Nathan Gibson, director of IT operations/privacy officer, WVMI Quality Insights. "It's really important to perform a security risk assessment, so all aspects of security are addressed," he stresses.

Among other things, he says, such an assessment should include how to prepare and implement an incident response plan. Such a plan should cover what to do when a breach occurs and how to meet incident reporting requirements. Also, he recommends that healthcare security teams find out what kind of data is on their laptops and handheld devices, whether it is encrypted, and how they can prove that it is encrypted.

Security Technology

Encryption

Not encrypting devices is an invitation to a security breach. So why don't all healthcare organizations encrypt mobile devices? Treglia says some providers don't because encryption is difficult and expensive and because the HIPAA security rule doesn't require it. Jeff Pelot, CIO of Denver Health has another explanation: data encryption delays clinicians when they're trying to log onto the system.

"It makes a laptop unbearable to use, because it slows it down tremendously. Logons are from 5-10 minutes, and that makes it really hard to use," he says. "It's getting better with recent updates, which reduce it to a couple of minutes. But if you're used to dealing with a tablet, which is instant on, it's incredibly annoying."

An interview was also done with a CISO at a major health system in Northern California, who says that older encryption software slowed down logons significantly. But the encryption that his organization uses doesn't degrade performance on mobile devices, and he regards it as essential for mobile security.

"Many healthcare organizations still are not encrypting hard drives on their laptops," he says. "That's a necessary precaution to take, and it's not expensive anymore. Having an appropriate encryption management process is the key to making sure you don't have a breach when these devices are lost."

"Many healthcare organizations still are not encrypting hard drives on their laptops," the CISO says. "That's a necessary precaution to take, and it's not expensive anymore. Having an appropriate encryption management process is the key to making sure you don't have a breach when these devices are lost."

Endpoint Management

Today, most institutions allow clinicians to bring their own mobile devices to work. This "bring your own device" (BYOD) trend, Pelot notes, creates problems for security, because the smartphones and tablets are not controlled by the organization and may not be encrypted. So Denver Health and many other healthcare providers require that mobile device management (MDM) software be installed on personal smartphones and tablets. Mueller emphasizes the importance of mandating the use of MDM where BYOD is permitted: "No company should ever allow an employee to use their personal device unless it's under the control of an MDM program," he says.

Endpoint Security

Endpoint security solutions can be used with desktop and laptop computers, as well as on smartphones and tablets. These applications offer key security functions in the following areas:

- *Governance:* Remotely monitor and control devices.
- *Risk management:* Receive alerts when predefined conditions occur and remotely secure device before data is accessed.
- *Compliance:* Use certificates and reports as proof that devices and data were properly secured when a device is lost or stolen.

If a mobile device is in a healthcare facility, it might be mislaid or lent to someone other than the authorized user. But endpoint security software can monitor where each device is at all times, whether it is in the building or somewhere else. Such tracking can often help users locate missing devices before they are stolen and before the organization decides to delete the data it contains.

Some organizations go so far as to delete the data on a missing device, whether or not there is any indication if it has been stolen. "We feel if it's not in control of the owner, then it is at risk, and therefore we'd wipe the data," the CISO from Northern California mentioned. "The MDM solution might compartmentalize our business information, which is available on our server and other storage devices. So it could be restored very easily."

Another important aspect of endpoint security solutions is their ability to detect whether the device encryption is working and whether anybody other than an authorized user has opened or tampered with any of the files on the device. By using endpoint security software in this way, organizations can establish whether or not a security breach has occurred.

Good endpoint security solutions should also include an audit trail that shows who viewed the data, whether someone changed it, where it resides, and how it's protected. Also, when files are deleted, the audit trail must show what was deleted and when.

An advanced endpoint security program will include persistence technology, providing them with a connection to the device that cannot be removed. Persistence technology is embedded in the firmware of desktops, laptops, and mobile devices at the factory. If an unauthorized user tries to eliminate the endpoint security software agent, a remote server will automatically re-install it on the device.

Good endpoint security solutions should also include an audit trail that shows who viewed the data, whether someone changed it, where it resides, and how it's protected. Also, when files are deleted, the audit trail must show what was deleted and when.

Remote endpoint security software can be used to convey commands to the device, such as to delete or retrieve data, freeze the device, and other security options. In its simplest form, Mueller notes, this setup synchs a device with a mail server such as Microsoft Exchange, which can be used to delete everything in a device's mailbox. But message attachments might have been stored elsewhere on the device. So an endpoint security solution should provide options that will definitively delete all files regardless of where they are stored within the endpoint.

To keep track of devices when they are carried outside a facility, look for geotechnology capabilities including geofencing. This allows the organization to build perimeters on an internet map to contain their devices. If an endpoint strays, IT will be alerted so they can investigate further.

Most importantly, an endpoint security solution must be flexible enough to support the unique requirements of the organization. For example, a user name change on a device may be a red flag for certain healthcare IT departments, while for others – perhaps where devices are often shared – this condition is quite acceptable. The same can be said for changes to IP address, physical location, hardware configurations and other conditions. Organizations should invest in technology that provides them with the ability to design security protocols that work best for them.

Most importantly, an endpoint security solution must be flexible enough to support the unique requirements of the organization. For example, a user name change on a device may be a red flag for certain healthcare IT departments, while for others – perhaps where devices are often shared – this condition is quite acceptable.

Conclusion

The best technical approach to device security is a layered approach that doesn't depend upon a single component such as encryption, remote device management, or endpoint security. All of these elements should be applied as part of a robust mobile security solution.

Endpoint security applications are capable of tracking and securing devices, remotely deleting data at risk, and locating lost or stolen mobile devices. They also allow the organization to show it has mitigated the security risk enough so that it doesn't have to report the incident.

However, no technical solution is perfect. Unless it is combined with appropriate policies and procedures, as well as thorough training of mobile device users, security breaches will continue to occur. Security risk assessments must always be updated to counter new threats as they emerge. But a comprehensive approach that includes all of the components listed above can minimize the chance that an organization will experience a significant security breach.

Notes

1. Chris Sherman, Heidi Shey, Stephanie Balaouras, and Jennie Duong, “Brief: Stolen and Lost Devices are Putting Personal Healthcare Information at Risk,” Forrester Research, Sept. 4, 2014.
2. Ibid.
3. “Epocrates 2013 Mobile Trends Report: Maximizing Multi-Screen Engagement Among Clinicians,” http://www.epocrates.com/oldsite/statistics/2013%20Epocrates%20Mobile%20Trends%20Report_FINAL.pdf
4. “Brief: Stolen and Lost Devices are Putting Personal Healthcare Information at Risk”
5. HIMSS, “2nd Annual HIMSS Mobile Technology Survey,” Dec. 3, 2012, http://www.himss.org/files/himssorg/content/files/FINALwithCOVER.pdf
6. Medical Identity Fraud Alliance, “The Growing Threat of Medical Identity Fraud: A Call To Action,” July 2013, accessed at http://medidfraud.org/wp-content/uploads/2013/07/MIFA-Growing-Threat-07232013.pdf.
7. David Carr, “Healthcare Data Breaches to Surge in 2014,” InformationWeek Healthcare, Dec. 26, 2013, accessed at http://www.informationweek.com/healthcare/policy-and-regulation/healthcare-data-breaches-to-surge-in-2014/d/d-id/1113259.
8. Adam Greenberg, “Health Insurance Credentials Fetch High Prices In The Online Black Market,” SC Magazine, July 16, 2013 (http://www.scmagazine.com/health-insurance-credentials-fetch-high-pricesin-the-online-black-market/article/303302/).
9. Redspin, “Breach Report 2013: Protected Health Information (PHI),” February 2014, accessed at http://www.redspin.com/docs/Redspin-2013-Breach-Report-Protected-Health-Information-PHI.pdf.
10. “The Growing Threat of Medical Identity Fraud.”
11. Ibid.
12. HIMSS, “Introduction to the Risk Assessment Toolkit and Security Risk Assessment Basics,” March 7, 2013, http://www.himss.org/files/HIMSSorg/Content/files/RA01_RA_Toolkit_Intro_1362425663131_1.pdf
13. National Council of State Legislatures, “Security Breach Notification Laws,” http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.
14. HIMSS, “2nd Annual HIMSS Mobile Technology Survey
15. “Brief: Stolen and Lost Devices are Putting Personal Healthcare Information at Risk”
16. NIST, “An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountable Act (HIPAA) Security Rule.”
17. Ibid.

About The Institute for Health Technology Transformation

The Institute for Health Technology Transformation (IHT²) is the leading organization committed to bringing together private and public sector leaders fostering the growth and effective use of technology across the healthcare industry. Through collaborative efforts the Institute provides programs that drive innovation, educate, and provide a critical understanding of how technology applications, solutions and devices can improve the quality, safety and efficiency of healthcare.

The Institute engages multiple stakeholders:

- Hospitals and other healthcare providers
- Clinical groups
- Academic and research institutions
- Healthcare information technology firms
- Healthcare technology investors
- Health plans
- Consumer and patient groups
- Private sector stakeholders
- Public sector stakeholders

Mission and Vision

The mission of the Institute for Health Technology Transformation: to drive improvement and the effective use of technology throughout the continuum of care through education and collaboration among multiple stakeholders. Technology in-and-of itself will not solve the deep challenges facing our healthcare system nor will it alone ensure more accessible and higher quality care. Realizing the benefits of technology across the healthcare continuum is a complex, under utilized and often misunderstood process. Stakeholder collaboration underscores the Institute's focus working to ensure technology has a transformative effect at all levels of the healthcare sector.

What We Do

The Institute for Health Technology Transformation (iHT²) provides programs that drive innovation, educate, and provide a critical understanding of how technology applications, solutions and devices can improve the quality, safety and efficiency of healthcare. We do this though a number of vehicles including: educational workshops, access to industry thought leaders, peer reviewed research, high level conferences, webinars, focus groups, topic specific committees, and other unique initiatives allowing individuals and organizations access to resources that will enable them to leverage the full value of healthcare technology.

Institute for Health Technology Transformation
244 5th Ave #2150
New York, NY 10001

iHT2
Institute for Health
Technology Transformation