Meeting the Challenges of HIPAA Compliance, Phishing Attacks, and Mobile Security

A Proofpoint White Paper
Contents

Healthcare IT Challenges...........................................................................................................3

HIPAA and Healthcare IT Regulations ......................................................................................3
  HIPAA: Broader and Tougher than Ever..............................................................................3
  Other Regulations ..................................................................................................................5

Inbound Threats: Low Volume and High Risk.........................................................................6

The Mobile Revolution and the Consumerization of IT.........................................................7

Putting It All Together:
Proofpoint Security-as-a-Service Solutions...........................................................................8
Healthcare IT Challenges

Healthcare organizations (HCOs) are facing three major IT security and compliance challenges. First, IT regulations such as HIPAA are getting stricter and enforcement actions are becoming more common and costly. Second, hackers and criminal syndicates are attacking HCOs with new forms of intrusive IT attacks that steal valuable data such as login credentials, customer records, proprietary research data, and other forms of intellectual property. Third, like other industries, healthcare is undergoing an IT revolution enabled by consumer-class mobile devices like iPads and Android phones. Smartphones and tablets are giving healthcare workers unprecedented access to patient records and other medical data on the go. But this new decentralized infrastructure often makes it more difficult for HCOs to protect confidential data. This so-called Bring Your Own Device (BYOD) trend potentially puts HCOs at greater risk of violating industry regulations and succumbing to inbound security threats.

Let’s examine each of these challenges—stricter regulations, inbound threats, and mobile IT—in turn.

HIPAA and Healthcare IT Regulations

HIPAA: Broader and Tougher than Ever
The most important healthcare IT regulation in the United States is HIPAA1. In addition to establishing guidelines for how HCOs continue insurance coverage for employees changing jobs, HIPAA put in place three big rules that govern healthcare IT:

- The EDI Rule (162.1000), which establishes standard health information terminology and electronic code sets
- The Security Rule (164.306), which establishes safeguards to protect the confidentiality, integrity, and availability of electronic protected health information (PHI)
- The Privacy Rule (164.502), which orders HCOs to protect PHI and defines the allowable uses and disclosures of PHI, in contrast to “de-identified” health information2

In recent years, all three of these rules have been updated, and another major update to the Privacy Rule is pending3. In addition, the federal government has become much more aggressive about enforcing HIPAA regulations and imposing financial penalties on organizations it decides have violated HIPAA rules4.

In a sense, the pressure on HCOs has been building since the original HIPAA legislation passed. HIPAA regulations went into effect in April 2003. For the next five years, regulators investigated and closed about 8,000 cases of HIPAA violations without imposing any significant financial penalties or sentencing any violators to jail. But in 2009, the FTC imposed a $2.25 million fine on CVS Caremark for violating HIPAA privacy regulations.

1 For a detailed look at HIPAA, the HITECH Act, and new data privacy regulations, see the Proofpoint white paper HIPAA Update: Staying Compliant with the Latest Healthcare Email Security Regulations.
2 “De-identified” information is information that excludes any details, such as a complete Social Security Number, that could be used to identify a specific person.
4 Resolution agreements and civil monetary penalties for the most serious HIPAA violations to date can be found here: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/index.html
The case originated in 2006 when pharmacy employees discarded patients’ prescription information in public dumpsters—clearly a violation of HIPAA mandates to ensure that PHI is always private. The CVS Caremark penalty proved to be the first of many multi-million dollar penalties against HIPAA violators.

Even government agencies are not immune to regulatory scrutiny and financial penalties. The Office of Civil Rights announced a $1.7 million penalty for Alaska’s Medicaid agency, the Alaska Department of Health and Social Services. The original violation was the loss of a hard drive containing PHI for 501 patients. But regulators upped the penalty when they discovered that the department had failed to conduct a risk analysis exercise as required by the Security Rule, had not adequately trained its workforce on regulations and data security practices, and had not implemented adequate encryption and other security controls for data and media.5

Regulators are penalizing small organizations as well. In April 2012, regulators fined Phoenix Cardiac Surgery $100,000 for posting PHI on a publically accessible cloud-based calendar program and for transmitting PHI through personal, inadequately secured email programs.6

We expect penalties against HCOs for HIPAA violations to continue for three reasons.

First, HIPAA violations, especially data breaches, continue, and PHI continues to be leaked or lost.7 The numbers are often dishearteningly big: 228,000 South Carolina Medicaid records were recently leaked through email.8 Over the past 3 years, more than 20 million patient records have been compromised in data breaches large enough to require reporting to the federal government.9

Second, the government recently expanded the scope of HIPAA and added requirements for data breach notifications and timely responses to patient inquiries.

The scope of HIPAA broadened considerably with the passage of the American Recovery and Reinvestment Act (ARRA) of 2009. In addition to enacting a financial stimulus for the U.S. economy, the ARRA included another piece of legislation called the Health Information Technology for Economic and Clinical Health (HITECH) Act. The HITECH Act extended the scope of HIPAA data privacy laws to cover the partners of HCOs. Accounting firms, IT consultancies, and other organizations who work with HCOs are now legally responsible for protecting the privacy of PHI.

The HITECH Act also introduced a strict data breach notification rule. If an employee discovers a PHI security breach, the employee’s organization has only 60 days in which to notify each patient whose privacy has been compromised. If an HCO is unable to contact ten or more of the affected individuals, it must either disclose the security breach on its Web site or issue a press release about the breach to broadcast and print media. If the breach affects 500 or more individuals, the organization must additionally notify the Secretary of the Department of Health and Human Services (HHS), along with major media outlets. The HHS will then report the breach on its own Web site. Failure to comply with these new data breach guidelines can result in penalties.

5 http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/alaska-agreement.html/
8 http://www.postandcourier.com/article/20120419/PC16/120419166&slid=2
9 http://www.computerworld.com/s/article/9230028/\_Wall\_of\_Shame\_exposes\_21M\_medical\_record\_breaches
The HITECH Act also strengthened patients’ rights to know who has accessed their PHI. Patients can now ask their HCOs to provide detailed accounts of how they have shared their PHI. HCOs must comply with these requests within 60 days. To have any chance of processing these requests on time, HCOs must be systematically tracking all PHI communications and be able to sort them by patient. Fulfilling this requirement will also entail the centralized storage, search, and retrieval of large volumes of information—services provided by email archiving systems. The sender, recipient, content, and timestamp of all email carrying PHI must be logged so they can be listed in responses to patients.

Regulators have already shown that they take these new requirements seriously. When Cignet Health of Prince George’s County in Maryland failed to respond in a timely manner to requests from 13 patients for their PHI records, regulators imposed a $1.3 million fine and opened an investigation into other possible HIPAA violations. By the time the investigation had finished, the penalty had grown to $4.3 million.

Third, the government has re-organized its enforcement of HIPAA. HIPAA is now enforced by the Office of Civil Rights, and financial penalties accrue directly to the department. In other words, HIPAA penalties now help fund the enforcement of HIPAA regulations.

As these developments show, HCOs and their partners have more impetus than ever before to take HIPAA security regulations seriously.

Other Regulations
HIPAA is not the only set of data security and data privacy regulations that affect HCOs. The list of laws and regulations calling for HCOs and other businesses to protect private data is long and getting longer.

- **Federal Trade Commission (FTC)**
  The FTC has its own data privacy regulations that apply to companies like WebMD and Google that sell healthcare information online. The FTC rules include a data breach notification rule.

- **Department of Health and Human Services (HHS)**
  As part of the HITECH Act, the HHS introduced new data security regulations that provide safe harbor for HCOs who encrypt PHI. These rules build on the HIPAA data security and data privacy rules but impose additional requirements on organizations that collect and store PHI.10 Like the new FTC rules, the new HHS rules require companies to notify the public of data breaches.

- **State Laws**
  States are passing their own data security and data breach notification laws, which are becoming increasingly broad. California SB 1386 requires any business, regardless of its location, to publicly disclose the compromise of the private information involving a California resident. The original focus of SB 1386 was on private data such as a resident’s name, driver’s license number, and credit card number. In 2007, California legislature passed AB 1298, which extends the scope of SB 1386 to cover medical information and health insurance information as well. The Massachusetts Data Privacy Law (201 CMR 17), which took effect in 2010, requires that personal information about any Massachusetts resident be encrypted when stored or transmitted. Businesses must disclose data breaches affecting the privacy of even a single Massachusetts resident. That same year, Nevada strengthened its own data

---

privacy laws and now requires all businesses storing or transmitting private data in the state to comply with the Payment Card Industry Data Security Standard (PCI DSS), a data security standard developed and adopted by the credit card industry. Forty-six states have now passed data breach notification laws.

- **Canadian Laws**
  In 2002, the coverage of Canada’s Personal Information Protection and Electronic Documents Act (PIPEDA) was extended to the healthcare industry. Since then, four Canadian provinces have also passed privacy laws that are similar to PIPEDA.11 As of January 2012, Ontario’s Freedom of Information and Protection of Privacy Act (FIPPA) has been extended to hospitals, requiring them to protect confidential data in email and to service public requests for records.

- **Other National Laws**
  Other nations have passed their own data privacy laws that apply to HCOs as well as other types of organizations. In Japan, the nation’s Privacy Law requires HCOs and other organizations that store records of 5,000 or more people to secure all personal information (including information as “public” as names and phone numbers) and release it only with the express permission of the individuals affected. Compliance failures can result in financial penalties and prison sentences.12 Since 1995, European companies have been required to abide by the European Data Protection Law, which gives individuals control over how their personal information, including healthcare information, is collected, stored, and distributed. A new European Data Protection Regulation draft from January 2012 would, among other things, extend Data Protection Law rules to all organizations, including HCOs based in the U.S. and Canada, that process the personal data of European residents.13 As these draft European regulations show, data privacy and data security laws worldwide are becoming increasingly strict and comprehensive.

Bottom line: HCOs and their business partners need to continue monitoring PHI and ensuring they have security infrastructure in place to protect PHI at all times.

**Inbound Threats: Low Volume and High Risk**

While regulations about data security are getting stricter, inbound threats that attempt to steal confidential data are becoming more stealthy and effective. Email remains the number one vector for initiating such attacks.

Five years ago, email threats came mainly in the form of high volume spam, malware attachments, and phishing attacks that attempted to lure large numbers of email recipients into logging into fake banking portals or other fraudulent Web sites.

Over time, email security systems reduced the effectiveness of these attacks. In response, hackers and criminal syndicates changed their strategy. Why hawk cheap pharmaceuticals and counterfeit goods when they could steal data that can be monetized on the black market? That stolen data might be customer records with credit card information, addresses, and Social Security Numbers; or it might be confidential research, patent descriptions, chemical formulas, business plans, or other data that might give one company a significant competitive edge in the marketplace.

---

To steal well-guarded data requires an attack far more subtle and sophisticated than a botnet blasting out spam. The attack of choice is a low-volume email phishing attack in which a small number of personal email messages are sent to a small number of individuals, such as members of the executive team. The messages include links to Web sites or, occasionally, booby-trapped attachments. Once clicked, those links install keyloggers or some other form of malware that enables remote parties to monitor the desktop system or server that has been compromised. Eventually hackers learn to navigate the internal network and find their way to valuable data. They then “exfiltrate” that data; they copy it in a slow trickle that is too subtle to be noticed by most network monitoring tools. Exfiltration might last for days, weeks, months, or even years. The sophistication and duration of these attacks has earned them the name Advanced Persistent Threats (or “Advanced Targeted Attacks”).

Advanced Persistent Threats pose a new challenge for HCOs. The attacks are notoriously difficult to detect. Each attack is custom-tailored for its target. To lure recipients into clicking on a link, the phishing messages often include personal data gleaned from social networks or other public sources—data that the recipients might assume is known only to friends or colleagues. Because the message contents are unique, they lack virus signatures and don’t appear on AV blacklists. Because their danger lies in email links rather than in malware attachments, the messages can slip past firewalls that scan email for malware. And the links themselves might be benign most of the time. Attackers might load them with rootkits or keyloggers only intermittently to avoid detection by IT systems that evaluate Web links for hidden threats.

Even after the attack has begun and valuable research or customer data is flowing out through a surreptitious, encrypted network tunnel, email recipients often have no idea that they’ve been attacked.

Ironically, at the same time that regulations are requiring even tighter control over confidential data, HCOs find themselves battling the most sophisticated attacks yet on data security. They need to detect and defeat those attacks, while continuing to defend against all the traditional attacks, such as spam, malware, and more conventional forms of data leaks.

The Mobile Revolution and the Consumerization of IT

Adding to the complexity of stricter regulations and stealthier forms of inbound attacks is the revolution taking place in mobile computing. Like their peers in other industries, healthcare workers are bringing their own mobile devices to work. HCO IT networks are now busy with traffic from “non-business” devices such as iPhones, iPads, and Android phones. Roughly 22% of physicians in the U.S. now use iPads in their practices.14 Mobile devices become even more practical as HCOs, at the government’s urging, adopt EHRs for everyday work.15

---

14 http://www.tuaw.com/2011/03/30/ipads-are-becoming-as-important-to-doctors-as-their-stethoscope/
15 http://americanmedical.com/ehr-stimulus-center/meaningful-use/
The proliferation of consumer mobile devices, their lack of rigorous security controls, and new exploits against mobile devices are combining to create new security risks for HCOs. These security risks take several forms:

- **Higher incidence of data breaches**  
  When mobile devices become more popular in an organization, data breaches increase. For example, a study by Manhattan Research found that when doctors’ use of smartphones rose by 9%, data breaches rose 32%.\(^{17}\)

- **Lost devices**  
  The average cell phone user loses a phone each year.\(^ {18}\) When that phone is a smartphone carrying PHI, data privacy, data security, and regulatory compliance are jeopardized.

- **Loss of perimeter protection**  
  Many HCOs have installed firewalls and Web gateways that monitor inbound and outbound traffic on enterprise networks. When users access email and other services from remote locations such as home networks and Wi-Fi hotspots such as hotel lobbies and cafes, those perimeter defenses become useless. There’s no longer an IT filter between the employees device and a phishing site or malware payload. When infected devices return to the internal network, they become a new unchecked vector for attack.

HCOs need security services that extend to cover mobile devices and that assess threats—such as URLs in email messages—even when users encounter them in remote locations far beyond the security of the organization’s firewall.

### Putting It All Together:  
**Proofpoint Security-as-a-Service Solutions**

HCOs need to protect PHI and other confidential data, even while they’re under attack from sophisticated hackers and criminal syndicates, and even while their employees are carrying more mobile devices and communicating over more channels—email, IM, SMS, etc.—than ever before.

Proofpoint offers security and compliance solutions that enable HCOs to embrace new technology such as mobile computing while defending against new forms of security attacks.

Email remains the top IT attack vector for enterprises such as HCOs. Proofpoint Enterprise Protection provides the industry’s most comprehensive email security threat classification and email security management solution against phish, virus, spam, and other email borne malware. Proofpoint Enterprise Protection minimizes spam, while ensuring that malware and phishing attacks never reach employee mailboxes.

Proofpoint Targeted Attack Protection applies advanced Big Data analytics techniques to detect new forms of attack, including low-volume phishing attacks, before they strike. Proofpoint Targeted Attack Protection features Proofpoint Anomalytics, a service that examines hundreds of variables in real time—including email message characteristics, but also the email traffic history of the message recipient—to identify anomalies that indicate

---

\(^{17}\) [http://www.ama-assn.org/amednews/2011/12/19/bil21219.htm](http://www.ama-assn.org/amednews/2011/12/19/bil21219.htm)  
a potential threat. Another component of Proofpoint Targeted Attack Protection, URL Clicktime Defense Service, examines URLs at clicktime to ensure that Web destinations are safe and not infected with malware. The URL Clicktime Defense Service protects employees and their devices even when their accessing email at remote locations, such as at home or at Wi-Fi hotspots, outside the network perimeter.

Finally, to track PHI communication and be able to comply with patient requests for records of PHI distribution, HCOs can rely on Proofpoint Enterprise Privacy and Proofpoint Enterprise Archive. Proofpoint Enterprise Privacy inspects outbound communications for PHI and other forms of regulated, sensitive and confidential data and then automatically applies policies — such as blocking or encrypting email messages that contain PHI, ensuring that sensitive healthcare data is transmitted in compliance with HIPAA rules. Proofpoint Enterprise Archive provides rule-based archiving for HCOs, and offers lightning fast search responses, enabling email administrators and compliance officers to respond quickly to content requests from individuals through regulatory inquiry.

To ensure that archived email remains private and secure, Proofpoint Enterprise Archive applies DoubleBlind Key Architecture, ensuring that only authorized users within the HCO can decrypt archived content. Proofpoint Enterprise Archive combines rigorous security with a high performance Discovery service that saves HCOs valuable time and money when retrieving archived content.

For more information about Proofpoint solutions for HCO security and compliance, please visit www.proofpoint.com or call +1 (877) 634–7660.