

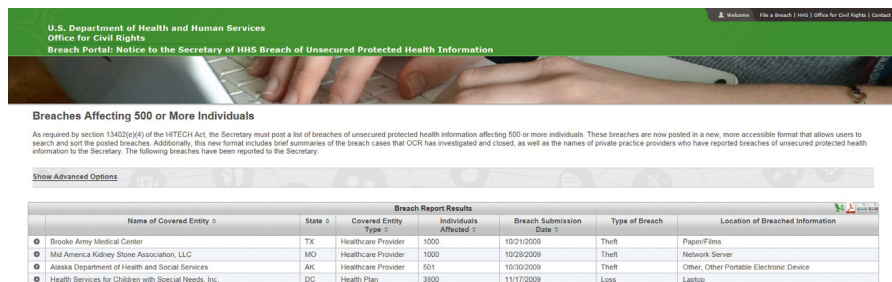
# How Well Protected is Your Protected Health Information? Perception Versus Reality

“Motives aside, data privacy, security, and breach response planning efforts are often not a fiscal priority in the C-suite, leaving patients, reputations—and the bottom line—at severe risk.” That assessment was made in a 2012 article in *Forbes Magazine* [1]. Does it still hold true today?

Statistics bear out the fact that many healthcare executives believe that there are many other fiscal priorities that need to come before investment in stronger cybersecurity. For example, a recent survey conducted by the Healthcare Information Management Systems Society (HIMSS) found only 64% of hospitals and medical practices have put encryption software in place to protect patient data as it is transported from one location to another [2]. Similarly, a survey conducted by the Ponemon Institute, a research center focused on data security, found that 73% of healthcare organizations have yet to implement the necessary resources to prevent data breaches or detect them once they occurred [1]. A separate survey found that only 42% of healthcare providers were planning to put encryption in place and only 44% are planning to set up single sign on and authentication on their web-based applications and portals [3].

These statistics strongly suggest that decision makers in the healthcare community still see the need for more security as unwarranted. Some may even suspect that the call for more security is just an alarmist rant by information security specialists or vendors hoping to sell more software and hardware. That argument might stand up to scrutiny, were it not for the long list of data breaches that have been reported in the last few years—many of which were preventable.

The United States Department of Health and Human Services Office of Civil Rights (OCR) publishes a comprehensive list of healthcare data breaches in the US (Fig. 2.1). As of March 27, 2015, it contained 1184 breaches that affected 500 or more individuals. This so-called “Wall of Shame,” which can be viewed at [https://ocrportal.hhs.gov/ocr/breach/breach\\_report.jsf](https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf), includes some massive attacks, such as the one that compromised 78,800,000 individuals at the large medical insurer Anthem—reported to HHS on 3/14/13—the breach that exposed 11,000,000 members of Premiera Blue Cross (3/17/2015), and the one



U.S. Department of Health and Human Services  
Office of Civil Rights  
Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information

**Breaches Affecting 500 or More Individuals**

As required by section 13420(e)(4) of the HITECH Act, the Secretary must post a list of breaches of unsecured protected health information affecting 500 or more individuals. These breaches are now posted in a new, more accessible format that allows users to search and sort the posted breaches. Additionally, this new format includes brief summaries of the breach cases that OCR has investigated and closed, as well as the names of private practice providers who have reported breaches of unsecured protected health information to the Secretary. The following breaches have been reported to the Secretary.

Show Advanced Options

Name of Covered Entity	State	Breach Report Results				
		Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location of Breached Information
Brooke Army Medical Center	TX	Healthcare Provider	1000	10/21/2009	Theft	Paper/Film
Mid America Kidney Stone Association, LLC	MO	Healthcare Provider	1000	10/29/2009	Theft	Network Server
Alaska Department of Health and Social Services	AK	Healthcare Provider	501	10/30/2009	Theft	Other, Other Portable Electronic Device
Health Services for Children with Special Needs, Inc.	DC	Health Plan	3800	11/17/2009	Loss	Laptop

**FIGURE 2.1** Healthcare data breaches affecting 500 or more individuals.

that occurred at Community Health Systems (4.5 million), which was submitted to HHS on 8/20/2014. Several smaller organizations and individual clinicians have also been embarrassed by having their breaches posted on the site. Clinicians in Ohio, Texas, and California, for example, are included on the list by personal name, along with how many patient records were exposed in each facility and the type of breach that occurred, for example, theft, hacking, unauthorized access or disclosures, and/or improper disposal of records.

OCR is required by Section 13402(e)(4) of the Health Information Technology for Economic and Clinical Health (HITECH) Act to post any breach of unsecured protected health information (PHI) affecting 500 or more individuals. Even more disturbing for small medical practices and community hospitals is the fact that federal officials are now going after providers who have experienced PHI leakages that affect *fewer* than 500 individuals. In 2013, Health and Human Services announced that the Hospice of North Idaho had to pay \$50,000 for violations of the Health Insurance Portability and Accountability Act (HIPAA) because the facility allowed an unencrypted laptop with PHI for 441 patients to be stolen. In the words of Leon Rodriguez, the Director of the Office of Civil Rights at the time: “This action sends a strong message to the healthcare industry that, regardless of size, covered entities must take action and will be held accountable for safeguarding their patients’ health information.... Encryption is an easy method for making lost information unusable, unreadable and undecipherable.” [4].

OCR is currently making plans to not only investigate healthcare organizations that have reported data breaches but to catch delinquent providers off guard by re-launching a program that audits providers who have not reported any incidents. A pilot project that started in 2011–2012 revealed several shortfalls. Mark Fulford, a partner at LBMC, an accounting and consulting firm in Brentwood, TN, explains: “The 2012 OCR audits revealed the healthcare industry at large had not yet begun to take compliance seriously. An astounding two-thirds of

audited entities had not even performed a complete and accurate risk assessment, which is the first step in putting a security strategy in place.” [5].

That initial series of about 100 audits found that many providers had neither taken basic steps to protect their networks, nor were they able to identify their vulnerabilities—an important requirement spelled out in the federal regulations that I will discuss in chapter 4: Risk Analysis. Some organizations did not even know *where* their PHI resided. And they could not say definitively what data had been stored in those mysterious locations.

Adding insult to injury, OCR found many employees were accessing data from unsecured mobile devices in public locations. Similarly, the audits indicated that many healthcare organizations were not training staff on how to manage PHI. The Civil Rights office has not only published the general approach it used for auditing providers, which will give you some sense of what you may face in the future, but it also warns that these protocols are in the process of being updated for use in the next round of audits. In the past, OCR has divided its approach to the auditing process into three broad categories: administrative risks, physical risks, and technical risks. In all likelihood, it will take a similar approach when it launches its next series of audits.

## THE COST OF INSECURITY IS STEEP

If you are responsible for the financial welfare of your organization, no doubt one question that comes to mind is: How much will it cost me if I do not adequately safeguard our PHI? Although protecting patient information involves legal and ethical issues, let us just focus on the financial issues for the moment.

It is estimated that healthcare organizations spend about \$6 billion a year as a result of data breaches. Since that does not tell you much about the cost of a breach to an individual provider, one has to look more closely at specific expenses. If your patients’ PHI is compromised and a federal investigation determines that your organization shares some of the responsibility for that data loss, expect each violation to cost between \$100 and \$50,000. That is per patient record. So a stolen laptop containing unencrypted records of 1,000 patients can cost the practice between \$100,000 and \$1.5 million in penalties alone. (Although  $\$50,000 \times 1000 = \$50$  million, the government caps these penalties at \$1.5 million.)

The Department of Health and Human Services (HHS) provides more detail on how it calculates the fines, breaking them down into four categories. If HHS determines that you unknowingly allowed the data breach and had exercised reasonable diligence, the fine is still between \$100 and \$50,000 per violation. However, if the breach occurred due to a “reasonable cause,” that range then jumps to \$1,000 to \$50,000 per violation. A third category, for a breach

resulting from willful neglect that was corrected in a timely manner, will result in a fine of \$10,000–\$50,000. And lastly, if your organization has willfully neglected to take precautions and did not correct the problem in a reasonable amount of time, the fine is at least \$50,000 per violation, with a cap of \$1.5 million per calendar year [6].

In addition to these broad criteria, numerous factors go into the HHS determination of how much to fine a healthcare provider, including how much harm results from the violation and the facility's history of prior compliance with the HIPAA regulation. And although the OCR is most interested in breaches of more than 500 patient records, the government will go after smaller incidents when they believe it serves the cause of justice, as mentioned above.

In 2009, for instance, Massachusetts General Hospital (MGH) agreed to pay \$1,000,000 to settle a HIPAA violation that only affected 192 patients. The Office of Civil Rights had MGH sign a resolution agreement requiring it to “develop and implement a comprehensive set of policies and procedures to safeguard the privacy of its patients.” The agreement resulted from an OCR investigation that started with a complaint filed by a patient whose PHI was exposed. Since the 192 patients affected by the breach were being treated by Mass General's Infectious Disease Associates outpatient practice, which included patients with HIV/AIDS, the exposure of patients' data not only threatened to expose them to the possibility of identity thief, but it also revealed their HIV status, clearly a very personal piece of information that most patients would want to keep confidential. And although the incident involved paper documents, the same judgment would likely have been made had this been an electronic breach [7].

## A CLOSER LOOK AT DATA BREACH FINES

Although OCR has posted the data breaches of over 1000 healthcare providers on its web site, this is only a small percentage of the HIPAA complaints it has received over the years. A closer look at the statistics makes it clear that OCR is not “out to get you.”

Since April 2003, it has received over 100,000 complaints. In more than 10,000 cases, its investigation concluded the entity in question had not violated the HIPAA rules. In more than 69,000 cases, OCR said the complaint was not “eligible” for enforcement for a variety of reasons, including the fact that some organizations are not covered by the HIPAA rules.

OCR investigated more than 23,000 cases that required changes in privacy and security practices by the provider, but most of these healthcare organizations never wound up among the 1,000+ that saw their “sins” posted on the Wall of Shame. And even fewer providers were actually fined for their violations, which

begs the question: When do you get fined? A review of some of the violators who were penalized can assist executives as they review their security policies and practices.

Anchorage Community Mental Health Services (ACMHS) agreed to pay \$150,000 for “potentially” violating HIPAA rule. The data breach, which affected more than 2700 individuals, occurred because, although the organization had put security rule policies in place in 2005, over time these policies were never actually implemented. Anchorage also allowed malware to compromise its records system. As the OCR report explained it: “The security incident was the direct result of ACMHS failing to identify and address basic risks, such as not regularly updating their IT resources with available patches and running outdated, unsupported software.” [8]. In a bulletin released by OCR, director Jocelyn Samuels stated: “Successful HIPAA compliance requires a common sense approach to assessing and addressing the risks to electronic protected health information (ePHI) on a regular basis. This includes reviewing systems for unpatched vulnerabilities and unsupported software that can leave patient information susceptible to malware and other risks.”

Parkview Health System, a nonprofit healthcare system that provides community-based healthcare services to individuals in northeast Indiana and northwest Ohio, paid \$800,000 for violating HIPAA rules. (Once again the official OCR report refers to this and most other breaches as “potential” violations of the HIPAA Act.) The violation occurred because Parkview did not properly handle patient records of about 5000–8000 patients. Parkview had taken custody of the records while helping a retiring physician transition her patients to new providers. Parkview employees left 71 cardboard boxes containing this sensitive material in the physician’s driveway, unattended. As OCR pointed out, providers “must appropriately and reasonably safeguard all PHI in its possession, from the time it is acquired through its disposition... All too often we receive complaints of records being discarded or transferred in a manner that puts patient information at risk... It is imperative that HIPAA covered entities and their business associates protect patient information during its transfer and disposal.” Notice that the bulletin describing this data breach also mentioned a healthcare provider’s business associates. (HHS defines business associate as “a person or entity that performs certain functions or activities that involve the use or disclosure of PHI on behalf of, or provides services to, a covered entity.”) Several violations have involved BAs, which we will discuss in a chapter 9: HIPAA, HITECH, and the Business Associate [9].

New York-Presbyterian Hospital (NYP) and Columbia University (CU) recently had to accept the largest fine yet to be levied against a healthcare organization. The two organizations, which work together as New York-Presbyterian Hospital/Columbia University Medical Center, were fined \$4.8 million for

exposing electronic PHI of 6800 individuals. The data included patient status, vital signs, medications, and lab results. The breach occurred because a physician employed by Columbia University had developed applications for both institutions and then attempted to deactivate a personally owned computer server on the network containing NYP electronic PHI. Because of a lack of technical safeguards, deactivation of the server resulted in patient information being accessible on Internet search engines.

The medical center was cited for several other infractions. OCR's investigation found that neither NYP nor CU made efforts prior to the breach to ensure that the server was secure and that it contained appropriate software protections. It had not conducted an accurate and thorough risk analysis to identify all systems that had access to NYP's ePHI, which meant it was not able to develop an adequate risk management plan that addressed the potential threats and hazards to the security of ePHI from both institutions. Finally, OCR states in its bulletin that "NYP failed to implement appropriate policies and procedures for authorizing access to its databases and failed to comply with its own policies on information access management." [10].

Concentra Health Services was fined more than \$1.7 million because one of its facilities, the Springfield Missouri Physical Therapy Center, had an unencrypted laptop stolen. What is interesting about this investigation was the fact that Concentra had done the required risk analysis before the incident occurred but did not follow through afterward. According to the OCR, "Concentra had previously recognized in multiple risk analyses that a lack of encryption on its laptops, desktop computers, medical equipment, tablets, and other devices containing ePHI was at critical risk. While steps were taken to begin encryption, Concentra's efforts were incomplete and inconsistent over time leaving patient PHI vulnerable throughout the organization." [11].

The data breach at Adult & Pediatric Dermatology, P.C., illustrates the impact data breach violations can have on small- to mid-sized medical practices. The group practice, with offices in Massachusetts and New Hampshire, was cited because an unencrypted thumb drive containing the ePHI of approximately 2200 individuals was stolen from the vehicle of one its staff members. The practice agreed to pay \$150,000 for the violation. OCR faulted the practice because it had failed to do a risk assessment to detect vulnerabilities in its security system. In other words, it never really took the time needed to figure out just how much protection they were providing for their PHI. The group neither had written policies and procedures in place to instruct staff on how to manage PHI nor had they been training workers as required by HIPAA regulations [12].

The dermatology group agreement with HHS also necessitated that the practice implement a corrective action plan requiring it to develop a risk analysis and risk-management plan to address and mitigate any security risks and vulnerabilities,

as well as to provide an implementation report to OCR. Such agreements often require a provider to hire a third party such as a security firm to monitor its progress as it puts the new plan in place—a rather expensive arrangement.

A review of other violations that resulted in fines reveals several security missteps made by various healthcare organizations [13]. Among those mistakes are the following:

- Leaving backup tapes, optical disks, and laptops with unencrypted PHI unattended, which were then stolen (Seattle-based Providence Health & Services)
- Disposing of sensitive patient information in dumpsters that could be accessed by the public (CVS retail pharmacies)
- Disclosing ePHI to a third party that did not have administrative, technical, and physical safeguards in place. The third party was using the data for marketing purposes (Management Services Organization Washington, Inc.)
- Intentionally disclosing of PHI to a national media outlet (Shasta Regional Medical Center)
- Exposing patient data as a result of security weaknesses in an online application database (Wellpoint)
- Failing to erase PHI from the hard drives of several leased photocopiers before the machines were returned to a leasing agent (Affinity Health Plan)
- Moving PHI to a publicly accessible server (Skagit County government, Washington)
- Allowing unauthorized employees to view PHI

This last breach, which occurred in the UCLA Health System, resulted in an \$865,500 fine because unauthorized employees were snooping into the patient records of celebrity patients who were being cared for at the UCLA facility. That HIPAA violation raises an important concern of many security specialists, who say the risk of internal hackers is worse than the threat coming from outsiders. The OCR bulletin describing the breaches states: “Employees must clearly understand that casual review for personal interest of patients’ PHI is unacceptable and against the law.”

A global look at all the OCR investigations offers some lessons learned that will help you concentrate on the most likely causes of a data breach. HHS lists the following issues as those most often investigated, in order of their frequency:

1. Impermissible uses and disclosures of PHI
2. Lack of safeguards of PHI
3. Lack of patient access to their PHI
4. Lack of administrative safeguards of electronic PHI
5. Use or disclosure of more than the minimum necessary PHI



These breaches were most likely to occur in private practices, general hospitals, outpatient facilities, pharmacies, and health plans, in that order of frequency.

## DO NOT IGNORE INDIVIDUAL STATES IN BREACH INVESTIGATIONS

A PHI breach at Beth Israel Deaconess Medical Center (BIDMC) in 2012 illustrates the fact that federal regulators are not the only officials eyeing your security efforts—or lack thereof. The Boston medical center had to pay \$100,000 to the state of Massachusetts because it failed to protect the PHI and other personal information of nearly 4000 patients, as well as personal information of 194 state residents, including 102 BIDMC employees. This happened despite the fact that BIDMC had policies in place that required staffers to encrypt laptops and physically secure them. The incident resulted from the fact that an unauthorized person broke into a BIDMC physician's office and stole his unencrypted personal laptop. According to the office of Maura Healey, the state's Attorney General "The laptop was not hospital-issued but was used by the physician with BIDMC's knowledge and authorization on a regular basis for hospital-related business." [14].

You are likely to see more states taking action when data breaches involving PHI are uncovered because the federal government is encouraging it. The HITECH Act gives state Attorneys General the authority to bring civil actions on behalf of its residents when they get wind of HIPAA violations. In fact, the Office of Civil Rights has even developed a training course to help AGs investigate these claims. In the words of the civil rights office, "OCR welcomes collaboration with SAG seeking to bring civil actions to enforce the HIPAA Privacy and Security Rules, and OCR will assist SAG in the exercise of this new enforcement authority. OCR will provide information upon request about pending or concluded OCR actions against covered entities or business associates related to SAG investigations. OCR will also provide guidance regarding the HIPAA statute, the HITECH Act, and the HIPAA Privacy, Security, and Enforcement Rules as well as the Breach Notification Rule." [15]. Chapter 4: Risk Analysis will go into more detail on state and federal regulations that apply to PHI.

Despite all the high profile cases in which government authorities have imposed heavy fines on healthcare organizations, a recent analysis indicates that only a small percentage of providers who report breaches and found themselves on the federal "Wall of Shame" actually are fined. A recent report on more than 1140 large breaches from ProPublica, a nonprofit investigative journalism group, revealed that only 22 resulted in fines [16]. That translates into less than a 2% likelihood of being fined.

The same report did not, however, discover such laxness on the part of the California Department of Public Health, which imposed 22 fines in 2014 alone,



and an additional 8 in January and February of 2015. One possible reason the federal government has penalized so few healthcare providers is because it is understaffed and overwhelmed. The Office only has about \$39 million to spend and fewer than 200 staffers. That would also explain the long interval between the time a data breach is reported and the time a fine is imposed.

Nonetheless, the Office of Inspector General at the Department of Health and Human Services issued a rather severe critique of the OCR in 2013, stating that it has not carried out its responsibility to perform security audits outlined by the HITECH Act.

## **FINES ARE ONLY PART OF THE PROBLEM**

A manager who is comfortable with taking risks might reason that a 2% risk is acceptable and provides no incentive to strengthen one's security protocols. That logic is faulty for several reasons.

Since the Office of Inspector General's critique, the Office of Civil Rights has promised to ratchet up its auditing program, so that will likely increase the odds of a security shortfall being exposed in your organization.

More importantly, federal fines are only part of the expense an organization would incur should a PHI breach occur. You may also be responsible for having a forensic evaluation performed to determine how the breach happened. Assuming for the moment that your practice or hospital does not have the expertise and personnel to do this expert analysis, you may have to spend on average between \$200 and \$2000 per hour for third-party assistance [17].

Depending on the circumstances surrounding a data breach, you may also have to notify those patients and employees whose personal information has been exposed. That will likely cost up to \$5 per notice, so in the 1000 patient scenario described previously that would add another \$5000 to the bill.

Patients who have had their PHI exposed are also entitled to some type of protection to reduce the risk of identity theft. According to a 2012 analysis from Zurich American Insurance Company, you can expect to pay \$30 per patient per year to cover the cost of credit monitoring, identity monitoring, and restoration [17]. But that figure may be outdated and is likely to be higher now. An identity protection service like Lifelock costs about \$110 per year retail, which would translate to \$220,000 for the same 1000 patients over 2 years [18].

You also have to consider the cost of a legal defense. If the incident reaches the mass media, it is very likely that you will face a class action lawsuit. On average that will cost an organization about \$500,000 in lawyer fees and \$1,000,000 for the settlement [17]. Of course, many cautious healthcare executives would naturally think twice about informing the local media about a data breach, but

the law does not give you a choice in the matter. The HIPPA breach notification rule states that following a breach of unsecured PHI involving more than 500 individuals, an organization not only has to promptly inform all the patients individually, it must provide “prominent” media outlets within the State or jurisdiction of the breach. That will probably require a press release put out within a reasonable amount of time—no more than 60 days after you detect the breach.

Speaking of data breach-related lawsuits, a class action suit was filed against Kaiser Permanente because it lost a thumb drive containing medical records of nearly 49,000 patients, a violation of the California’s Confidentiality Act. The relevant state law stipulates that each affected patient is entitled to statutory damages of \$1000 [19].

Cottage Health System and Insync Face Health Care likewise faced a data breach class action suit alleging that they were responsible for 32,500 patient records finding their way onto the Internet. The suit, also filed in a California court, claimed that Insync, a technology vendor, did not encrypt the data or take other necessary security measures [20].

Unfortunately such expenses do not take into account the cost of a public relations firm to repair a damaged reputation, call centers to handle questions from patients who have had their personal information exposed, and the amount of revenue lost because patients no longer trust your hospital or medical practice and decide to seek treatment elsewhere. According to Mac McMillan, chief executive for CynergisTek, a security firm, “the average patient spends about \$150,000 on medical care in a lifetime.” Multiplying that figure by our 1000 patients may mean the loss of \$150 million [21].

The HIPAA violations that occurred at BlueCross BlueShield of Tennessee (BCBST) in 2009 can give you a sense of the price tag of a data breach above and beyond the federal fines. BCBST agreed to pay the Department of Health and Human Services \$1.5 million for violating HIPAA rules because it lost data on over 1 million members after a burglary. But within a few short years of the breach, the health insurer had spent \$17 million for various corrective actions. They had to identify the affected members and providers and notify them of the breach. It spent \$7 million to tighten IT security, which included encryption of all at rest data. (At rest data can include information that is stored on desktop computers, mobile devices, and servers. At rest data is distinguished from data in motion, which refers to data being transported from place to place.) [22]

The BCBST incident also should alert decision makers to some of the more unexpected ways in which their organization’s patient data can become exposed. In this case, the PHI was located on 57 hard drives that were located in a secured closet at a former call center that the insurer no longer used. The official

resolution agreement between HHS and Blue Cross Blue Shield explained that: “The hard drives in the network data closet were part of a system which recorded and stored audio and video recordings of customer service calls. The hard drives that were stolen contained data which included the PHI of health plan members, such as member names, member ID numbers, diagnosis codes, dates of birth, and social security numbers. The stored audio and video data from the recorded calls had to be manually and individually reviewed to obtain access to PHI. BCBST’s internal investigation confirmed that the PHI of 1,023,209 individuals was stored on the hard drives.” [23].

As I will discuss in later chapters, improperly disposing of patient records is only one of several ways to get in trouble. If you discard an old fax machine, chances are that sensitive patient data in its memory can be easily retrieved by thieves or hackers. Likewise, you may decide to give away outdated desktop computers to a nearby school or charity. Unless those hard drives are properly scrubbed, you are giving away PHI. If on the other hand, you are trashing old computers, one safe way to prevent data loss is to remove the hard drives and drill a hole into each of them so they are useless.

## FACTORING IN THE MEANINGFUL USE PROGRAM

Although we have been focusing on the cost of fines, forensic analysis, credit monitoring services, and public relations nightmares, there is another potential expense that can result from lax security measures. The federal government may take back the financial incentive a hospital or medical practice received when it signed up for the Meaningful Use program and received payments to help install an electronic health records (EHR) system.

In 2009, the American Reinvestment & Recovery Act was enacted, which included measures to improve the nation’s infrastructure, including the record keeping systems in US hospitals and medical practices. Under the leadership of the Centers for Medicare and Medicaid Services, it authorized grants to eligible health professionals and to hospitals to put EHRS in place that would have a meaningful impact on patient care. The incentive payments range from \$44,000 per eligible clinician over 5 years for Medicare providers and \$63,750 over 6 years for Medicaid providers. (Eligible hospitals can receive \$2 million or more.)

To qualify for these incentives, eligible providers had to meet a long list of criteria for each stage of the program—to date we are up to Stage 3. The criteria were initially published in the Federal Register on July 28, 2010.

So far, hundreds of thousands of physicians and hospitals have received these payments, which required that they also attest to the fact that they met the aforementioned criteria. Unfortunately, many providers attested to these criteria without fully understanding what they were signing up for.

Jennifer Searfoss, JD, chief executive officer for SCG Health, recently pointed out that “The biggest problem for many providers is that they are checking off the box that says they have done a security analysis, and none of them have.... One hospital had to return \$1.5 million because it hadn’t done the security assessment.”

The check box relates to one of the core measures that healthcare organizations must attest to when they apply for Meaningful use incentives. For medical practices, the measure requires your office to conduct or review a security risk analysis in accordance with the requirements and implement security updates as necessary and correct identified security deficiencies as part of its risk management process [24]. The Meaningful Use security regulations for hospitals are very similar to those outlined for medical practices.

Essentially the Meaningful Use program has taken the HIPAA regulations and plugged them into its set of regulations. In plain English, the MU regulations require providers to analyze the practice’s ability to withstand a data breach, either internally or externally. The assessment starts with a review of your existing IT setup and then looks for threats and vulnerabilities. Once these are identified, you need to estimate how likely they are to actually cause a breach and the impact they will have on the practice. Once that step has been accomplished, the practice needs to find ways to mitigate those risks and monitor the results over time. I will go into more detail on this process in a future chapter, but for now, the point I want to drive home is simple: If the practice has not done a formal risk assessment and addressed those risks, you may be asked to return the \$44,000 you received for each eligible professional in your practice if the practice is audited.

Once again, a pragmatic physician executive is going to ask: What are the chances of being audited? That question was recently answered at the 2014 HIMSS conference. It is no longer a question of if you will be audited but *when* was the answer from several health IT experts. Currently, the Centers for Medicare and Medicaid Services has been doing prepayment and postpayment audits on 5–10% of healthcare providers. But that 10% figure can be misleading. If CMS audited 10% of providers in 2014 and 10% in 2015, it is only a matter of time before they get to you [25]. One organization has been forced to return \$31 million in EHR incentives because an error was found in the way the facility was using its EHR; Detroit Medical Center fired its chief medical information officer for similar issues.

## CALCULATING THE COST OF SECURITY

How much will it cost to create an airtight security system that will prevent PHI from being exposed? There is no such thing. No matter how much you invest, you cannot guarantee complete protection to your records. Fortunately, government regulators do not expect it. They expect organizations to take

reasonable measures to prevent a breach, and to report data exposure should it occur. I will go into much more detail on what these measures consist of in the chapters on risk analysis, preventive strategies, and HIPAA regulations.

One such measure—data encryption—is one component of “good data hygiene.” Encryption, which essentially makes electronic information unreadable by converting it into gibberish until it is unlocked with an encryption key, should be installed on any laptop or other mobile device containing PHI, personally identifiable information (PII), as well as a variety of other types of sensitive data. There are numerous ways to accomplish that, depending on your resources, the skill set of the person who handles your IT operations, and your budget.

If a small practice has only a shoestring budget for information technology and there is a consultant or someone on staff with the technical know-how, it is possible to encrypt data on Windows computers by turning on Bitlocker, a build-in encryption tool—assuming you have the correct Windows operating system. Apple computers have a similar tool, called FileVault2.

As you would expect, a more sophisticated encryption system will cost more. You can pay between \$250,000 and \$500,000 for an enterprise encryption system [21]. The Ponemon Institute has estimated that the average cost of installing full hard disc encryption on a laptop or desktop computer in the United States will run \$235 per year. But it also estimated that you are likely to save \$4650 as a result of not having your data exposed with said encryption. Put another way, the Ponemon research, which surveyed over 1300 individuals in IT and IT security in the United States, Great Britain, Germany, and Japan, concluded that the benefits of full-disk encryption “exceeded cost in all four countries by a factor ranging from 4 to 20.” The study looked at costs in several industries, and broke down the results industry by industry. Finance and healthcare had the highest costs, \$388 and \$363, respectively [26].

Unless you have an IT professional on staff or an employee with extensive knowledge of healthcare IT, you may need to bring in third-party experts to implement many of the other security features needed to be compliant with HIPAA regulations. I will discuss those regulations in more depth in another chapter, but for the sake of our discussion on the cost of security, you can estimate that it will cost between \$50 and \$100 an hour for someone to do basic computer and network work; if you want to bring in a security specialist, expect to spend \$150–\$250 per hour [27].

A 2005 cost analysis from Carnegie Mellon University concluded that a small private practice may have to spend about \$10,000 to upgrade its computers to comply with HIPAA regulations; that translates into about \$12,000 in 2015 inflation-adjusted dollars. A large organization can expect to spend millions for the upgrade, though estimates differ widely [28].

Similarly, one security and compliance vendor recently estimated that a small provider would have to pay between \$4,000 and \$12,000 to comply with HIPAA rules [29].

The same vendor estimated the cost for a medium to large organization as \$50,000+. Obviously, average figures like this are no substitute for case-by-case cost analyses. The same report found that Children's Hospital of Pittsburgh spent about \$88,000 to develop and implement HIPAA compliance, or about \$105,700 in 2015 dollars. It also budgeted \$5,000 in 1 year for staff training and promotion (\$6,000 in 2015 dollars).

Since the HIPAA regulations mandate employee training, that expense can be significant and ongoing. An American Hospital Association study found that on average such training can really add up, about \$22 per employee in 2015 inflation-adjusted dollars [28].

Decision makers also have to factor in the cost of firewalls, antispymware, and antimalware software, also discussed in more detail in chapter 5: Reducing the Risk of a Data Breach. McAfee, for instance, charges about \$22–\$25 per license for a software package that will cover 250 or fewer devices.

Another approach to PHI security is to hire a HIPAA auditing firm to analyze your weaknesses and strengths. In some respects, it is like asking the Office of Civil Rights to come in *before* a breach occurs to investigate where one is likely to happen. These companies review your existing safeguards, do their own risk assessment, and create a risk management plan. You can expect to spend up to 3 months with the auditor and spend at least \$40,000 [30].

Believing a bare bones security system that includes a firewall and an antiviral program is enough to keep your PHI safe is a lot like believing that condoms protect against sexually transmitted disease. Granted, they can reduce the risk of STDs transmitted through the exchange of body fluids—think HIV/AIDS. But there are many infections that are transmitted by skin-to-skin contact, for which condoms offer very limited protection—genital herpes and genital warts come to mind. Likewise putting a weak security system in place may prevent your computers from being infected with a few common threats, but it will do little to prevent several other infections. And since “abstinence” is not an option for most healthcare providers—that would require cutting the cord to the Internet—the most cost-effective solution is a full-throttled security program.

## References

- [1] R. Kam, L. Ponemon, Why healthcare data breaches are a C-Suite concern, Forbes. <http://www.forbes.com/sites/ciocentral/2012/12/07/why-healthcare-data-breaches-are-a-c-suite-concern/>, 2012.
- [2] J. Conn. Advocate data breach highlights lack of encryption, a widespread issue, Modern Healthcare. <http://www.modernhealthcare.com/article/20130830/NEWS/308309953>, 2013.

- [3] E. McCann. Healthcare's slack security costs \$1.6B, Healthcare IT News. <http://www.healthcareitnews.com/news/healthcares-slack-security-costs-16b>, 2014.
- [4] U.S. Department of Health & Human Services. HHS announces first HIPAA breach settlement involving less than 500 patients, Hospice of North Idaho settles HIPAA security case for \$50,000. <http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/honi-agreement.html>, 2013.
- [5] M. Fulford. OCR audits: don't fall victim to past mistakes. <http://www.informationweek.com/healthcare/security-and-privacy/ocr-audits-dont-fall-victim-to-past-mistakes/a/d-id/1317645>, 2014.
- [6] Privacy Rights Clearinghouse. Fact Sheet 8a: health privacy: HIPAA basics, How does HHS determine a penalty for a violation? <https://www.privacyrights.org/content/health-privacy-hipaa-basics#hhs-determine-penalties>.
- [7] U.S. Department of Health & Human Services. Massachusetts General Hospital Settles Potential HIPAA Violations. <http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/mass-generalra.html>.
- [8] HHS Anchorage. BULLETIN: HIPAA settlement underscores the vulnerability of unpatched and unsupported software. <http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/acmhs/acmhbulletin.pdf>, 2014.
- [9] HHS.gov. \$800,000 HIPAA settlement in medical records dumping case. <http://www.hhs.gov/news/press/2014pres/06/20140623a.html>, 2014.
- [10] HHS.gov. Data breach results in \$4.8 million HIPAA settlements. <http://www.hhs.gov/news/press/2014pres/05/20140507b.html>, 2014.
- [11] HHS.gov. Stolen laptops lead to important HIPAA settlements. <http://www.hhs.gov/news/press/2014pres/04/20140422b.html>, 2014.
- [12] HHS.gov. Dermatology practice settles potential HIPAA violations. <http://www.hhs.gov/news/press/2013pres/12/20131226a.html>, 2013.
- [13] Office of Civil Rights. Case examples and resolution agreements. <http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/index.html>.
- [14] Office of Attorney General Maura Healey. Beth Israel Deaconess Medical Center to pay \$100,000 over data breach allegations: hospital to take steps to prevent future data security violations. <http://www.mass.gov/ago/news-and-updates/press-releases/2014/2014-11-21-beth-israel-data-breach.html>, 2014.
- [15] US Department of Health and Human Services. Health information privacy: state attorneys general. <http://www.hhs.gov/ocr/privacy/hipaa/enforcement/sag/index.html>.
- [16] C. Ornstein. Policing patient privacy: fines remain rare even as health data breaches multiply, ProPublica. <http://www.propublica.org/article/fines-remain-rare-even-as-health-data-breaches-multiply>, 2015.
- [17] T. Stapleton. Data breach cost: risks, costs, and mitigation strategies for data breaches, Zurich American Insurance Corporation. <http://www.zurichna.com/internet/zna/sitecollectiondocuments/en/products/securityandprivacy/data%20breach%20costs%20wp%20part%201%20%28risks,%20costs%20and%20mitigation%20strategies%29.pdf>, 2012.
- [18] D. Munro. Assessing the financial impact of 4.5 million stolen health records, Forbes. <http://www.forbes.com/sites/danmunro/2014/08/24/assessing-the-financial-impact-of-4-5-million-stolen-health-records/>, 2014.
- [19] A. Bucher. Class action lawsuit filed over kaiser permanente data breach, Top Class Actions. <http://topclassactions.com/lawsuit-settlements/lawsuit-news/11339-class-action-lawsuit-filed-kaiser-permanente-data-breach/>, 2014.
- [20] BigClassAction.com. Cottage health system and insync face health care records data breach class action lawsuit. <http://www.bigclassaction.com/lawsuit/cottage-health-system-insync-face-care-records-data.php>, 2014.



- [21] M. McMillan, P. Cerrato. Healthcare data breaches cost more than you think, InformationWeek Healthcare Report, 2014.
- [22] E.J. Albright. BlueCross BlueShield's Data Breach leads to costly HITECH infraction, InsideARM.com. <http://www.insidearm.com/daily/collection-technologies/data-security/bluecross-blueshields-data-breach-leads-to-costly-hitech-infraction/>, 2012.
- [23] Department of Health and Human Services. Resolution agreement. [http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/resolution\\_agreement\\_and\\_cap.pdf](http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/resolution_agreement_and_cap.pdf), 2012.
- [24] Department of Health and Human Services Office of the National Coordinator of Health Information Technology. Guide to privacy and security of health information: Chapter 2 Privacy & security and meaningful use. <http://www.healthit.gov/sites/default/files/privacy-and-security-guide.pdf>.
- [25] P. Cerrato. Meaningful use EHR audits: when, not if, InformationWeek Healthcare. <http://www.informationweek.com/healthcare/electronic-health-records/meaningful-use-ehr-audits-when-not-if/a/d-id/1297456>, 2014.
- [26] Information Week NetworkComputing. Calculating the cost of full disk encryption. <http://www.networkcomputing.com/careers-and-certifications/calculating-the-cost-of-full-disk-encryption/d/d-id/1233859>, 2012.
- [27] R. Herold, K. Beaver, *The Practical Guide to HIPAA Privacy and Security Compliance*, second ed., CRC Press, Boca Raton, FL, (2015).
- [28] R. Arora, M. Pimentel. Cost of privacy: a HIPAA perspective. <http://lorrie.cranor.org/courses/fa05/mpimenterichaa.pdf>, 2005.
- [29] T. Ferran. How much does HIPAA compliance cost? <http://blog.securitymetrics.com/2015/04/how-much-does-hipaa-cost.html>.
- [30] T. Ferran. How much does a HIPAA Risk management plan cost?, Security Metrics Blog. <http://blog.securitymetrics.com/2015/01/how-much-does-hipaa-risk-management-cost.html>, 2015.