WHAT CAUSED THE BREACH? AN EXAMINATION OF USE OF INFORMATION TECHNOLOGY AND HEALTH DATA BREACHES

Posted on October 1, 2014 by Administrator

Category: Electronic Records

Tags: health data breaches, Health Information, health information technology, personal health information, privacy

by Suanu Bliss Wikina, PhD

Abstract

Data breaches arising from theft, loss, unauthorized access/disclosure, improper disclosure, or hacking incidents involving personal health information continue to increase every year. As of September 2013, reported breaches affecting individuals reached close to 27 million since 2009, when compilation of records on breaches began. These breaches, which involved 674 covered entities and 153 business associates, involved computer systems and networks, desktop computers , laptops, paper, e-mail, electronic health records, and removable/portable devices (CDs, USBs, x-ray films, backup tapes, etc.). Even with the increased use of health information technology by health institutions and allied businesses, theft and loss (not hacking) constitute the major types of data breaches encountered. Removable/portable devices, desktop computers, and laptops were the top sources or locations of the breached information, while the top six states—Virginia, Illinois, California, Florida, New York, and Tennessee—in terms of the number of reported breaches accounted for nearly 75 percent of the total individual breaches, 33 percent of breaches in covered entities, and about 30 percent of the total breaches involving business associates.

Keywords: health data breaches, health information technology, personal health information, privacy, health information

Introduction and Background

The Privacy Rights Clearinghouse (PRC) began tracking data breaches in 2005 and has reported that as of October 2012, more than 563 million records have been leaked. The PRC believes that this number is significantly lower than the actual figure because in many cases, the number of exposed records either is not known or is not reported to the news media or to state and federal reporting authorities.[1] In the health sector, data breaches affecting 500 or more individuals are required by law to be posted by the US Department of Health and Human Services (DHHS) as public information. Section 13402(e)(4) of the Health Information Technology for Economic and Clinical Health (HITECH) Act mandates that the secretary of DHHS post a list of breaches involving unsecured protected health information involving 500 or more individuals. This list is available at the DHHS website.[2] Data breaches represent the most prevalent privacy risk arising from loss of control of information in either electronic or paper form by an organization, its vendors (business associates), or a malicious third party.[3] The unfortunate events of health data breaches have been attributed to issues including outright theft, loss, unauthorized disclosure or exposure, hacking, improper disposal, or unknown (indeterminate or undisclosed) causes.

According to DHHS, a breach is generally "an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information such that the use or disclosure poses a significant risk of financial, reputational, or other harm to the affected individual."[4] This definition holds true except under the following three conditions: (a) "the unintentional acquisition, access, or use of protected health information by a workforce member acting under the authority of a covered entity or business associate," (b) "the inadvertent disclosure of protected health information from a person authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the covered entity or business associate," and (c) "if the covered entity or business associate has a good faith belief that the unauthorized individual, to whom the impermissible disclosure was made, would not have been able to retain the information." In the case of (a) and (b), "the information cannot be further used or disclosed in a manner not permitted by the Privacy Rule."[5]

By law, the Health Insurance Portability and Accountability (HIPAA) Privacy Rule applies only to covered entities—healthcare providers, healthcare clearinghouses, and health plans—but in practice it extends to business associates who are engaged by covered entities provided that they (1) obtain satisfactory assurances that the business associate will use the information only for the purposes for which it was engaged by the covered entity, (2) will safeguard the information from misuse, and (3) will help the covered entity comply with some of its duties under the Privacy Rule. By definition, business associates include persons or entities that perform certain services or activities that involve the use or disclosure of protected health information on behalf of covered entities. As a result, the functions that business associates can perform include claims processing or administration; data analysis, processing, or administration; utilization review; quality assurance; billing; benefit management; practice management; and repricing, while the services they can perform include legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, and financial services.[6]

A number of major health data breaches have been reported in the news in recent times. For instance, Health Information Trust Alliance (HITRUST), a data security organization based in Texas, reported in May 2013 that its system was hacked, thereby expositing 111 health records, including information from test data. The breach involved data such as real names, organizations, addresses, e-mail addresses, phone numbers, and six encrypted passwords. Hackers were said to have injected malicious code targeting a noncritical standalone public web server, resulting in some test data being compromised. According to the company, the breach did not involve personal health information or other sensitive data.[7]

Jackson Health System in Florida reported that paper medical records were lost while in transit to or from a location where they were electronically scanned, and notified the 1,407 patients affected in January 2013. Organization officials maintained that the documents did not contain Social Security

numbers or financial data. In another case, Sonoma Valley Hospital in California reported a data breach that occurred on February 14, 2013, during a routine website software update and notified the 1,350 surgery patients that were affected. These patients were treated between July 1, 2011, and June 30, 2012. In that case, data such as patient names, dates of service, procedures, surgeons, insurer names, and hospital charges were temporarily made available through a search engine during the software update. Hospital officials said that the breached information did not include Social Security numbers, birth dates, driver's license numbers, or addresses.[8]

When these incidents occur, the organizations, in addition to notifying the individuals affected, usually take actions internally to minimize the damage as well as instituting corrective actions and measures to prevent a recurrence. For instance, HITRUST paid for an independent security assessment program for associates of five insurance plans and pharmacy chains. Jackson Health System offered credit and identity protection services to affected individuals and implemented new security measures, such as managerial approval for paper record releases, installation of security cameras, and response training for missing medical documents. Sonoma Valley Hospital apologized to the affected patients, took actions to understand the cause of the breach, and then strengthened policies and controls protecting patients' personal health information.[9]

The cases mentioned above exemplify the various ways in which personal health information can be breached (hacking, improper disposal, loss/theft, and unintentional access or disclosure) and the location of the breached information (computers, paper records, electronic health records , etc.). With the increasing use of health information technology (HIT) in healthcare institutions coupled with increasing concerns about privacy and security of data, to find ways to avert these breaches it has become necessary to look at where they originate and the magnitude of their impact in terms of the number of individuals affected. Also, it is important to examine if widespread use of information technology is playing a role in the increasing number of data breaches.

This analysis is necessary because data obtained from the PRC[10] indicate that as of March 2009, 245 million records were reportedly breached, a number that increased to 563 million breaches as of 2012—an increase of 230 percent over a three-year period. Not all of these breaches involved health information. However, the 2011 Benchmark Study on Patient Privacy and Data Security by the Ponemon Institute showed that data breaches are increasing because of employee mistakes and that data breaches in healthcare organizations have increased 32 percent, representing an average of four data breaches per provider (hospitals and healthcare) .[11] However, Eastwood (2012) suggested that healthcare organizations need to be aware of the activities of hackers, even though hacking accounts for just 8 percent of data breaches, because personal health information is worth 50 times more to hackers and data thieves than credit card or Social Security numbers.[12]

Although the major causes of data breaches are known, HIT researchers are divided on where the

main causes emanate from. Although some lay the blame on the increasing use of information technology (IT) such as EHRs and the possibility of hackers' getting access to private health information, others believe human error causes most of the breaches[13] and that "85 percent of security breaches occur off-network."[14] Kegley (2010) reported that between 2007 and 2009, at a major multinational healthcare company, 75 percent of all security breaches were caused by fraud and/or failure to follow procedure.[15] Hong and Linden (2012) suggested that attackers have shifted from directly attacking computer systems toward exploiting human vulnerabilities and using social engineering tactics, such as tricking people to install malware, tricking people into opening malicious documents, exploiting poor interfaces that are difficult to understand or easy to misconfigure, and attempting to gain access via guessable passwords or reused passwords.[16]

With the increasing use of HIT, such as with EHRs, this study attempts to examine where health data breaches are actually occurring and what can be done to stem the tide.

Methodology

Data for the study were obtained from the DHHS Health Information Privacy website.[17]

As of September 22, 2013, data breaches that have been reported to DHHS as required by law have affected 674 covered entities, 153 business associates, and about 27 million individuals from all parts of the country since 2009, when the data were first compiled. The types of breaches included hacking or IT incidents, theft, loss, unauthorized access or disclosure, improper disposal, and other or unknown types. The breaches occurred on computer systems, desktop computers, laptops, e-mail, EHRs, network servers, paper records, and other sources of information.

The data for the study were downloaded into a spreadsheet and then sorted into tables by type of breach, location of breached information, and the state in which the breaches took place, using Microsoft Excel tools such as pivot tables. Where the type or location was linked to more than one source (for example, theft/loss, unauthorized disclosure/hacking/loss, or computer/laptop/e-mail), the researcher used the information contained in the notes entered under the column marked "Summary," where available, to determine where to place the breach to avoid double counting. For the purpose of this study, a distinction was made between theft, which is a deliberate attempt by a determined person to steal health data or information, and loss, which could result from carelessness. In some cases, however, one can lead to the other, making the cause difficult to determine when reporting the loss. Finally, the number of individuals affected and the number of covered entities and their business associates involved in a particular type of breach were then counted. The results obtained are shown in Table 1, Table 2, and Table 3.

Results

The contribution of each breach type or location to the total number of breaches was calculated as a percentage, as shown in Table 4 and Table 5. Bar charts depicting these contributions are shown in Figure 1 and Figure 2. The results for breaches affecting individuals suggest that theft (47.5 percent) and loss (27.4 percent) are the major types of breaches encountered, whereas improper disposal and unauthorized access or disclosure are the least, at 2.4 percent and 5.0 percent respectively. More than half of all the data breaches involving covered entities and slightly more than a third of breaches involving business associates consisted of stolen data. Although unauthorized access or disclosure accounted for 5.0 percent of the breaches affecting individuals, for covered entities and business associates the percentage of this type of breach was much greater, with this type accounting for 20.2 percent and 28.8 percent, respectively, of their breach incidents. Hacking or IT incidents represented only 7.1 percent of the total for individuals, 8.6 percent for covered entities, and 13.1 percent for business associates (see Figure 1), which is consistent with the percentage of health data breaches attributed to hacking generally as reported by Eastwood (2012).[18]

Results show that 44.6 percent of the breaches affecting individuals were attributed to sources categorized as "others." This type of breach occurs in removable or portable electronic devices or other media such as CDs, backup tapes, x-ray films, and so forth. Desktop computers alone accounted for close to 16 percent of breaches affecting individuals, while paper was the source of 4.4 percent of the breaches affecting individuals. Computers (excluding desktop computers and laptops), laptops, and network servers accounted for 8.8, 9.0, and 9.7 percent, respectively, of the total for individual breaches. In terms of breaches affecting covered entities and their business associates, the results showed that other sources, paper, and laptops were the major sources or locations of the breaches, followed by network servers and desktop computers (see Figure 2).

The 10 states with the largest number of individuals affected by breaches accounted for 86.6 percent of all data breaches, 41.4 percent of the total number of breaches involving covered entities, and 43.9 percent of breaches involving business associates. Out of this, the top five states represented 69.6 percent of the total number of individuals affected by data breaches, about 30 percent of breaches in covered entities, and 25 percent of the breaches involving business associates (see Table 6).

Even though California was third among the states in terms of the total number of data breaches, it had the highest number of covered entities involved (81, or about 10 percent) and was followed by Texas (11th on the list of states), with 58 covered entities, or 8.6 percent of the total. This finding is not surprising considering the size and population of these states. The data breaches reported from Texas represented only 2.1 percent of the total number of individuals affected. Virginia, which had the highest number of data breaches reported, had only 1.3 percent of the breaches involving covered entities and 2.0 percent of the breaches involving business associates, compared with New

York (fifth on the list), which accounted for 9.1 percent of data breaches in terms of individuals affected but had 6.2 percent and 7.2 percent, respectively, of the breaches involving covered entities or business associates.

Discussion, Recommendations, and Conclusions

Even with the increasing use of IT in healthcare, the vast majority of data breaches affecting individuals appear to be the result of theft and loss, not hacking or IT incidents. A huge cost is associated with data breaches in organizations; estimates suggest that on average, each lost or exposed customer record costs the organization $202.[19] In fact, data breaches are estimated to cost the US healthcare industry a whopping $6.5 billion on average annually, which would be enough to fund 216 million flu vaccinations or hire 81,000 registered nurses.[20] Unauthorized access or disclosure accounted for only a small percentage of the breaches affecting individuals but played a much greater role in the number of breaches in covered entities and business associates, suggesting the need for stricter controls (physical and electronic) to prevent breaches. In this regard, covered entities have a duty to ensure that continuous monitoring and evaluation of security and privacy controls are in place in the organizations they use as their business associates because third-party mistakes accounted for 46 percent of the data breaches reported in the 2011 Benchmark Study on Patient Privacy and Data Security.[21] According to Jaeger (2013), enforcing access controls by limiting access to sensitive information to those who need it as well as continuously monitoring networks, computer systems, and data for activity is an effective preventive measure to ward off internal and external threats of data breach.[22]

In terms of the source or location of the breached information, removable or portable electronic devices or media (CDs, backup tapes, x-ray films, etc.) and desktop computers appear to be where most of the breached information was located in breaches involving individuals, but for covered entities and business associates, removable or portable electronic devices or media, paper, and laptops came up as the top locations for most of the breaches. This finding reinforces the need for increased physical and electronic controls to guard against unauthorized access, theft, loss, or improper use of physical records and paper files, IT hardware, and storage facilities that are used to store protected personal health information. Also, data encryption and strong passwords should be introduced along with physical and electronic measures to help ensure data security and privacy in the event of loss or theft. Encryption is a best practice for security but should not be used as the sole method of defense. Encryption codes, as tough as they are, can be broken by determined professionals who are bent on cracking them.

The buck falls on covered entities not only to check and manage their own process for ensuring security and privacy of the information at their disposal but to ensure that the business associates to

whom they lawfully disclose information follow the terms of their contract and safeguard the information in their care. According to Kegley (2010), while healthcare managers pay much attention to opportunities for technology advancements, not much attention is being paid to the largest security weakness, which is old IT; thus he advocated for proper IT asset disposition: "Only after securing your disposition process can you buy new IT assets with complete confidence that your old ones are not exposing you to danger."[23]

Interestingly, the top six states (Virginia, Illinois, California, Florida, New York, and Tennessee) in terms of reported breaches accounted for close to three-fourths of total individuals affected by breaches and close to a third of all breaches involving covered entities and business associates. Although this study focuses on the types of breaches and where the information breached is located, it is important to examine the states where breaches are occurring in an attempt to uncover ways to mitigate this rising trend. Federal and state health authorities need to come up with ways to combat the trend. Apart from providing the necessary technology infrastructure for enhancing health information privacy and security, much work remains to be done in addressing human vulnerabilities.

Training and education are needed for people who handle personal health information to educate them on their role in enhancing the privacy and security of the information they encounter in the course of their duties, and this training needs to be taken seriously. We may be focusing on procuring the most advanced technological gadgets to protect and secure health information while the key lies in addressing the softer side of the equation. Proper disposal processes and procedures for removable electronic devices, paper records, desktop computers, laptops, and other computer equipment need to be put into place and adhered to. The 2011 Benchmark Study on Patient Privacy and Data Security reported that 73 percent of respondents say they lack sufficient resources to prevent or detect unauthorized patient data access, theft, or loss.[24] Staff responsible for the data need to be trained on basic security procedures to recognize deceptive techniques used by fraudsters and identity thieves, such as social engineering, and must report these techniques to the appropriate computer incident response team in a timely manner. Therefore, organizations desiring to establish an effective data privacy and security program should be aware that such a program hinges on the following pillars: (1) governance (leadership); (2) awareness, education, and training; (3) actions (implementing internal controls, including the use of data encryption, strong passwords, physical security, and electronic controls, as well as compliance testing); and (4) monitoring and evaluation.

Suanu Bliss Wikina, PhD, is an adjunct professor of information systems at Strayer University and Grantham University.

Notes

1. Privacy Rights Clearinghouse. "Data Breaches: Our Latest YouTube Video and Tips for Consumers." October 1, 2012. Available at https://www.privacyrights.org/data-breaches-video-and-tips-alert-2012 (accessed September 22, 2013).
2. US Department of Health and Human Services. "Data Breaches Affecting 500 or More Individuals." Available at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html (accessed September 16, 2013).
3. Pierson, C. T. "Data Breaches Highlight the Importance of Privacy." *Financial Executive* 25, no. 2 (2009): 62–63.
4. US Department of Health and Human Services. "Definition of Breach." Available at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html (accessed October 6, 2013).
5. Ibid.
6. US Department of Health and Human Services. "Business Associates." Available at http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.html (accessed October 12, 2013).
7. Conn, J. "Data Security Group HITrust Reports Breach." *Modern Healthcare*. May 29, 2013. Available at http://www.modernhealthcare.com/article/20130529/NEWS/305299952 (accessed January 18, 2014).
8. iHealthBeat. "Several Health Data Breaches Reported across Three States." May 30, 2013. Available at http://www.ihealthbeat.org/articles/2013/5/30/several-health-data-breaches-reported-across-three-states (accessed September 22, 2013).
9. Ibid.
10. Pierson, C. T. "Data Breaches Highlight the Importance of Privacy."
11. "Data Breaches Cost the Healthcare Industry an Estimated $6.5 Billion." *International Journal of Micrographics & Optical Technology* 29, no. 3 (2011): 3–5.
12. Eastwood, B. "How to Prevent Healthcare Data Breaches (and What to Do If You're a Victim)." *CIO.* 2012. Available at http://www.cio.com/article/724463/How_to_Prevent_Healthcare_Data_Breaches_and_What_to_Do_If_You_re_a_Victim_?page=3&taxonomyId=3147 (accessed January 18, 2014).
13. Jaeger, J. "Human Error, Not Hackers, Cause Most Data Breaches." *Compliance Week.* February 2013. Available at http://www.complianceweek.com/news/news-bulletin/human-error-not-hackers-cause-most-data-breaches (accessed September 26, 2013).
14. Kegley, J. "Avoid Being the Next Data-Security-Breach Headline." *Health Management*

Technology. September 2010. Available at http://www.healthmgttech.com/articles/201009/avoid-being-the-next-data-security-breach-headline.php (accessed August 9, 2014).
15. Ibid.
16. Hong, J., and G. Linden. "Protecting against Data Breaches; Living with Mistakes." *Communications of the ACM* 55, no. 6 (2012): 10–11.
17. US Department of Health and Human Services. "Data Breaches Affecting 500 or More Individuals." Available at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html (accessed September 16, 2013).
18. Eastwood, B. "How to Prevent Healthcare Data Breaches (and What to Do If You're a Victim)."
19. Kegley, J. "Avoid Being the Next Data-Security-Breach Headline."
20. "Data Breaches Cost the Healthcare Industry an Estimated $6.5 Billion."
21. Ibid.
22. Jaeger, J. "Human Error, Not Hackers, Cause Most Data Breaches."
23. Kegley, J. "Avoid Being the Next Data-Security-Breach Headline."
24. "Data Breaches Cost the Healthcare Industry an Estimated $6.5 Billion."

Printer friendly version of this article.

Suanu Bliss Wikina, PhD. "What Caused the Breach? An Examination of Use of Information Technology and Health Data Breaches." *Perspectives in Health Information Management* (Fall 2014): 1-16.

There are no comments yet.