Data Breach Locations, Types, and Associated Characteristics Among US Hospitals

Meghan Hufstader Gabriel, PhD; Alice Noblin, PhD, RHIA, CCS; Ashley Rutherford, PhD, MPH; Amanda Walden, MSHSA, RHIA, CHDA; and Kendall Cortelyou-Ward, PhD

ABSTRACT

OBJECTIVES: The objectives of this study were to describe the locations in hospitals where data are breached, the types of breaches that occur most often at hospitals, and hospital characteristics, including health information technology (IT) sophistication and biometric security capabilities, that may be predicting factors of large data breaches that affect 500 or more patients.

STUDY DESIGN: The Office of Civil Rights breach data from healthcare providers regarding breaches that affected 500 or more individuals from 2009 to 2016 were linked with hospital characteristics from the Health Information Management Systems Society and the American Hospital Association Health IT Supplement databases.

METHODS: Descriptive statistics were used to characterize hospitals with and without breaches, data breach type, and location/mode of data breaches in hospitals. Multivariate logistic regression analysis explored hospital characteristics that were predicting factors of a data breach affecting at least 500 patients, including area characteristics, region, health system membership, size, type, biometric security use, health IT sophistication, and ownership.

RESULTS: Of all types of healthcare providers, hospitals accounted for approximately one-third of all data breaches and hospital breaches affected the largest number of individuals. Paper and films were the most frequent location of breached data, occurring in 65 hospitals during the study period, whereas network servers were the least common location but their breaches affected the most patients overall. Adjusted multivariate results showed significant associations among data breach occurrences and some hospital characteristics, including type and size, but not others, including health IT sophistication or biometric use for security.

CONCLUSIONS: Hospitals should conduct routine audits to allow them to see their vulnerabilities before a breach occurs. Additionally, information security systems should be implemented concurrently with health information technologies. Improving access control and prioritizing patient privacy will be important steps in minimizing future breaches.

Am J Manag Care. 2018;24(2):78-84

Instances in which private information has been breached are becoming more commonplace in the United States,[1] making the security of this type of information a significant concern.[2] Healthcare information is particularly vulnerable, due to the sensitivity of these data and how they can be used by criminals.[3] Demographic data, Social Security numbers, and clinical information, including medical diagnoses, are housed in both paper and electronic health records (EHRs).[3] For these reasons, multiple attempts have been made through federal legislation to help curtail the occurrences of healthcare privacy breaches, including the 1996 Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health Act of 2009, and the Omnibus Final Rule in 2013.[4-6] Despite these initiatives, however, large data breaches are still occurring in US hospitals.

The adoption of EHRs among hospitals has increased rapidly over the past several years.[7,8] As healthcare systems digitized to keep up, the healthcare sector was unable to adopt electronic security components at the same pace, leading to vulnerabilities in record systems.[7] In some cases, technology purposed to assist healthcare delivery processes are now having costly difficulties.[9,10] The majority of small- and medium-size health organizations do not possess the financial or personnel resources necessary for sufficient information technology (IT) and security investments.[11,12] This, along with their highly valuable data, has left hospitals vulnerable to breaches of sensitive information.[13,14]

Hospitals have begun to implement strategies to help prevent data breaches that most often occur through theft, loss, unauthorized access, or hacking.[15] Strategies include the adoption of systems that include 2-factor authentication requirements to ensure that patients' health information is only accessible to and usable by those with rights to access it.[16] Two-factor authentication often incorporates a biometric component to verify the user's identity, such as a fingerprint, voice recognition, or iris scan, along with a password, personal identification number, or physical verification object, such as a token or key.

The objectives of this study were to describe the locations in hospitals where data are breached, the types of breaches that occur most often at hospitals, and hospital characteristics, including health IT sophistication and biometric security capabilities, that may be predicting factors of large data breaches that affect 500 or more patients. In spite of these health IT strategies, it is unclear what the most common types of breaches are and where patients' health information is most vulnerable. Under federal legislation, if a healthcare privacy breach affects 500 or more patients it must be reported to the Office of Civil Rights (OCR). Then, information regarding the breach is publicly posted on the OCR data breach portal.[13,17] Although several studies have examined OCR data breach information,[11-13] none have specifically focused on pediatric, academic, and nonfederal acute care hospitals, which house millions of patient records.

TAKEAWAY POINTS

- Even with sophisticated health information technology (IT) systems in place, security breaches continue to affect hundreds of hospitals and compromise thousands of patients' data; this gives cause to believe that other hospital factors, such as area characteristics, region, bed size, health system membership, hospital type, hospital governance, and market concentration, may play a vital role in breach risk.
- This study's results showed that of all types of healthcare providers, hospitals accounted for approximately one-third of all data breaches and hospital breaches affected the largest number of individuals.
- Paper and films were the most frequent mode or location of data breaches. However, although network servers were among the most infrequent locations of data breaches, breaches of this type impacted the most patients overall.
- Adjusted multivariate results showed significant associations among data breach occurrences and some hospital characteristics, including type and size, but not others, including health IT sophistication or biometric use for security.

METHODS

Data Sources

The OCR data breach portal provides an online database describing data breaches of protected health information (PHI) that affect 500 or more individuals.[15,18] This portal provides users the option of examining breach information from 3 types of covered entities: health plans, healthcare clearing houses, and healthcare providers. As of July 2016, the OCR portal included 1085 healthcare providers that had PHI breaches affecting 500 or more individuals between October 2009 and July 2016. Of these, 185 were nonfederal acute care hospitals and 27 were Veterans Affairs (VA) hospitals. Nonfederal acute care hospital breach information was linked with the 2015 Health Information and Management Systems Society (HIMSS) analytic data file (HIMSS Analytics, unpublished data) and information from the 2015 American Hospital Association (AHA) Health IT Supplement Survey regarding the use of 2-factor authentication.[19]

Variables to Characterize Data Breaches

Hospital data breaches of PHI that affected 500 or more individuals were characterized by: 1) type of breach and 2) location or mode of breached information. Data breach types included 6 categories: 1) hacking/IT incident, 2) improper disposal, 3) loss, 4) other/unknown, 5) theft, and 6) unauthorized access/disclosure. Data breach locations or modes included 7 categories: 1) desktop computer, 2) EHR, 3) email, 4) laptop computer, 5) network server, 6) paper/films, and 7) other location. To gain a more detailed view of which provider types were most frequently breached and had the most individuals affected, the OCR data were further categorized by "name of covered entity" into 9 health provider categories: 1) colleges/universities; 2) emergency response; 3) government; 4) group/physician practices; 5) health systems; 6) hospitals; 7) nursing homes, home/hospice care, and treatment facilities; 8) pharmacies; and 9) research facilities, laboratories, and medical supply companies.

Inclusion/Exclusion Criteria

Only nonfederal acute care hospitals, which include children's, teaching, and public or private hospitals, were included in this study. All other health provider categories were excluded.

Variables to Characterize Hospitals

Variables to characterize hospitals included area characteristics, region, bed size, health system membership, hospital type, health IT sophistication, hospital governance, and market concentration at the hospital referral region (HRR) level. A binomial variable for area characteristics was created that assessed whether the hospital was located in a rural or urban area; hospitals were considered to be urban if they were located in a metropolitan core–based statistical area. Regions (Northeast, Midwest, South, and West) were categorized based upon the US Census Bureau classification system. Hospitals were categorized into small (<100 staffed beds), medium (100 to 399 staffed beds), and large (≥400 staffed beds). Hospital types included academic, general medical and surgical, pediatric, critical access, and other specialty. A second binomial variable was created to measure health IT sophistication, and high levels were defined as having a HIMSS Electronic Medical Record Adoption Model (EMRAM) score of 6 or 7. The EMRAM score ranges from Stage 0, which is paper-chart–based, to Stage 7, which is defined by a complete EHR system.[16] A third binomial variable characterizing biometric security use was created by combining the hospitals that used biometric technology for security on the HIMSS analytics survey and/or the hospitals that answered that they supported an infrastructure for 2-factor authentication, including biometrics, in the AHA Health IT Supplement Survey. Hospital governance characteristics included

TABLE 1. Number of Data Breaches Affecting 500 or More Individuals Among US Hospitals, 2009-2016

Number of Breaches	Number of Hospitals
1	185
2	24
3	5
4	1

TABLE 2. Characteristics of US Hospitals With and Without Data Breaches Affecting 500 or More Individuals, 2009-2016

Variable	Hospitals Without Breaches n = 5295	Hospitals With ≥1 Breach n = 185	*P*
Area Characteristics			
Rural	21%	17%	.205
Urban	79%	83%	.205
Hospital Region			
West	19%	23%	.111
Midwest	29%	27%	.786
South	40%	36%	.764
Northeast	13%	14%	.555
Health System Membership (yes/no)			
Health system membership (yes)	69%	68%	.762
Hospital Size			
Small	53%	37%	.572
Medium	36%	36%	.928
Large	10%	26%	<.001
Hospital Type			
General medical and surgical	58%	48%	.758
Teaching hospital	3%	18%	<.001
Critical access hospital	25%	21%	.322
Other specialty hospital	12%	6%	<.001
Pediatric hospital	2%	6%	<.001
Biometric Security Use (yes/no)			
Biometric security use (yes)	39%	42%	.746
Health IT Sophistication (high/low)			
High health IT sophistication	30%	33%	.611
Hospital Ownership			
Government, nonfederal	19%	18%	.744
Not-for-profit	58%	67%	.398
Investor-owned, for-profit	22%	15%	.003

IT indicates information technology.

hospital status, such as not-for-profit, investor-owned (for-profit), and government (nonfederal). In addition, a hospital was considered to be a member of a hospital system if it belonged to an integrated healthcare delivery system. Market concentration was measured by the Herfindahl-Hirschman Index,[20] constructed on bed shares within systems at the HRR level.[21]

Data Analysis

Descriptive analyses to characterize provider facility, data breach type, and location/mode in hospitals were performed. Number of patients affected by data breaches was log transformed and a factorial 2-way analysis of variance (ANOVA) was conducted to examine the differences between data location/mode and type of breach and the number of patients affected by data breaches. Univariate analyses were conducted on hospital and area characteristics. To explore factors associated with hospitals having a data breach affecting 500 or more individuals, multivariate logistic regression analyses were performed using SAS Enterprise Guide (SAS Institute Inc; Cary, North Carolina). Significance was determined at the P <.05 level.

RESULTS

In total, 215 breaches, each affecting 500 or more individuals, occurred at 185 nonfederal acute care hospitals that reported to the OCR during the study period. Thirty hospitals had multiple breaches during that time. Twenty-four hospitals had 2 breaches, 5 hospitals had 3 breaches, and 1 hospital had 4 breaches (**Table 1**).

Descriptive Results

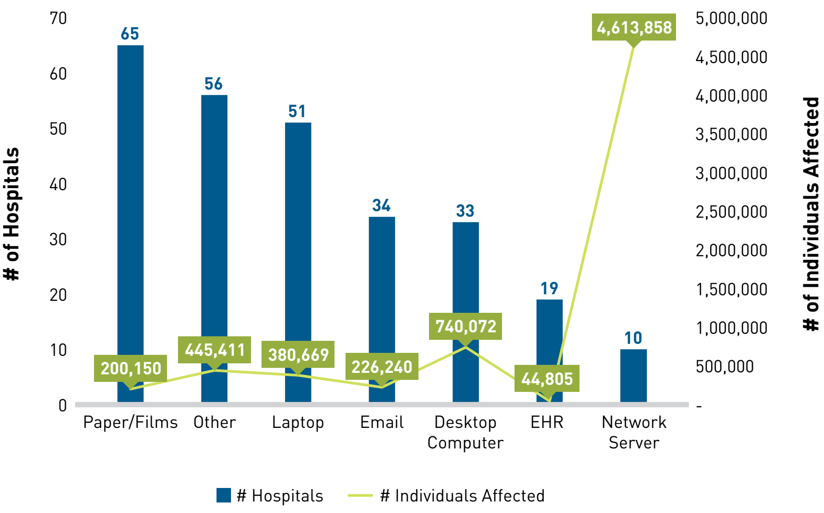
Significant differences were found between hospitals that had at least 1 breach and hospitals that did not have a breach affecting 500 or more individuals during the study period (**Table 2**). Bivariate descriptive statistics comparing hospitals with and without data breaches showed unadjusted differences in terms of hospital type, size, and ownership. Specifically, teaching hospitals (18% with a data breach vs 3% without a breach) and pediatric hospitals (6% with a breach vs 2% without) had higher percentages of data breaches. Larger hospitals also had a higher percentage of data breaches (26% with a data breach vs 10% without). In addition, a lower percentage of investor-owned (for-profit) hospitals (15% with a data breach vs 22% without) and other specialty hospitals (6% with a data breach vs 12% without) had at least 1 data breach. In bivariate descriptive analyses, health IT sophistication, biometric security use, health system membership, hospital region, and area characteristics were not significantly different in terms of data breach percentages.

Location of Data Breaches in Hospitals

The location of breached data and the number of individuals affected varied greatly among hospitals (**Figure 1**). Data breaches of paper/

films occurred most frequently (65 hospitals). Data located in "other locations" (eg, breaches not from paper/films, laptop computers, email, desktop computers, EHRs, or network servers, which were reported in 56 hospitals) and in laptops (in 51 hospitals) were the second and third most prevalent, respectively. The numbers of unsecured PHI breaches from email (in 34 hospitals) and desktop computers (in 33 hospitals) were approximately equal during the study period. EHR data were breached in 19 hospitals. Although network server breaches occurred most infrequently (in 10 hospitals), these breaches compromised the highest number of individuals (4,613,858 affected).

FIGURE 1. US Hospital Data Breaches Affecting 500 or More Individuals by Data Location, 2009-2016



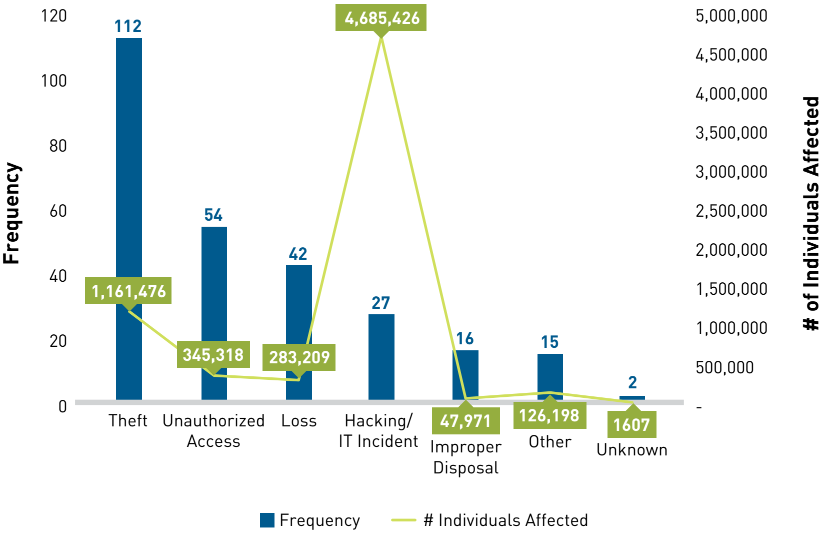
EHR indicates electronic health record.

Types of Data Breaches in Hospitals

Types of data breaches and the number of individuals affected by those types of breaches varied significantly among hospitals (**Figure 2**). Thefts occurred most frequently (in 112 hospitals), followed by unauthorized access/disclosure (in 54 hospitals), whereas hacking/IT incidents from 27 hospitals affected the most individuals (4,685,426).

Two-way ANOVA indicated no statistically significant differences in the number of patients affected between data location/mode (*P* = .455) or type of breach (*P* = .443). There were, however, statistically significant differences between frequency of data breaches occurring from network servers and EHRs (*P* = .018) and between network servers and paper films (*P* = .003).

FIGURE 2. US Hospital Data Breaches Affecting 500 or More Individuals by Type of Breach, 2009-2016



IT indicates information technology.

Multivariate Results

Adjusted results showed similar associations among biometric use for security and hospital characteristics, including type and size. Pediatric hospitals (odds ratio [OR], 5.1; 95% CI, 2.5-10.2) and teaching hospitals (OR, 5.0; 95% CI, 2.9-8.4) were associated with an increased risk of data breaches compared with other types of hospitals. In addition, small (OR, 0.3; 95% CI, 0.2-0.6) and medium (OR, 0.6; 95% CI, 0.3-0.9) hospitals by bed size were associated with a decreased risk for data breaches compared with larger hospitals. Hospital setting, health system membership, health IT sophistication, federal status, market concentration, and ownership status were not predicting factors of a data breach affecting 500 or more patients (**Table 3**).

DISCUSSION

Approximately one-third of all healthcare data breaches occurred in hospitals, and the most individual patients were impacted when hospitals were breached compared with other types of healthcare providers, such as doctors, nurses, and social workers. Therefore,

TABLE 3. Predicting Factors of Large Data Breaches Affecting 500 or More Individuals Among US Hospitals, 2009-2016[a]

	Point Estimates and 95% CIs	
Variable	**Estimate**	**95% CI**
Area Characteristics		
Rural	Ref	
Urban	0.705	0.401-1.238
Hospital Region		
Northeast	Ref	
West	1.594	0.906-2.804
Midwest	1.265	0.729-2.197
South	1.179	0.697-1.997
Health System Membership (yes/no)		
Health system membership	0.804	0.547-1.183
Hospital Size		
Large bed size	Ref	
Medium bed size	0.601	0.382-0.946
Small bed size	0.313	0.168-0.584
Hospital Type		
General medical and surgical	Ref	
Teaching hospital	5.028	2.989-8.459
Critical access hospital	1.553	0.815-2.957
Other specialty hospital	1.103	0.531-2.290
Pediatric hospital	5.103	2.550-10.215
Biometric Security Use (yes/no)		
Biometric security use	1.122	0.806-1.561
Health IT Sophistication (high/low)		
High health IT sophistication	0.907	0.631-1.303
Hospital Ownership		
Not-for-profit	Ref	
Government, nonfederal	0.761	0.478-1.212
Investor-owned, for-profit	0.887	0.533-1.475
Market Competition (HHI)		
Market competition	0.670	0.189-2.370

HHI indicates Herfindahl-Hirschman Index; IT, information technology; Ref, reference.

[a]Data source: HHS, Office for Civil Rights: Breaches affecting 500 or more individuals; HIMSS Analytics Data 2015; and American Hospital Association Health Information Technology Supplement 2015.

despite the the high level of hospital adoption of EHRs and the federal incentives to do so,[7] the most common type of data breach in hospitals occurred with paper records and films. These paper and film breaches occurred mostly due to theft, improper disposal, and unauthorized access. However, the overall number of patients affected by these breaches was relatively small. Conversely, network servers were found to be the least frequent location of data breaches, but these breaches impacted the most patients overall. In addition, this study found that there were large numbers of thefts of laptops, which can easily be physically removed and stolen regardless of EHR or biometric security system implementation. Adjusted results showed significant associations among data breach occurrences and hospital characteristics, including type and size. Pediatric hospitals and teaching hospitals were found to be at increased risk for breaches. The presence of capability and infrastructure support for biometrics and high health IT sophistication were not significantly associated with data breach risk.

Medical identity theft has long-lasting repercussions that can affect an individual's health and financial well-being; it cannot be remedied by closing an account, as one would do with a financial breach of a credit card number, for instance. Hospitals are vulnerable to data breaches, but investment in data security is lacking.[12] Although hospital investments in technology have been implemented to meet Meaningful Use and other federal requirements, protecting digitized patient data has not been a central focus. The findings of this study point to a need to integrate security measures in areas where patient information is kept to reduce the theft risk for both paper files and computers with PHI.

As shown by the findings of this study and others, computers have served as a source of data breaches because generic usernames and passwords make them easily accessible.[13,21] Hospital unit computers are easy targets because they contain patient and staff information, such as referral letters, nursing reports, patient charts, audits, handovers, and staff sick leave lists, directly on the desktop. Biometric technology is a valuable means of reducing username and password reliance by utilizing fingerprint, gesture, eye, facial, and voice recognition modalities. This is further strengthened via 2-factor authentication protocols, which often combine a username and password with a physical biometric scan to grant access.[20,22] Given that the most common location of breaches in a hospital is currently paper files/films, the addition of biometric technology is not likely to impact this number. However, as the diffusion of EHR technology continues in the United States and cyber threats become more prevalent, these hard-copy breaches will presumably continue to be minimized as long as necessary security policies are upheld and security audits are practiced.[22,23]

Previous studies have reviewed the characteristics of privacy breaches, but little research has been done since the revision of HIPAA in 2013.[5] This policy revision represented a significant change in the definition of what constitutes a breach and how covered entities and their business associates operationalize the regulations.

As hospitals are now faced with additional evolving threats to PHI, the impact of these breaches is a significant concern.[11] An emerging threat includes crypto-ransomware attacks on hospitals. Instead of stealing and selling patient data, hackers are now locking down entire systems and threatening to damage or disable computers unless hospitals pay a ransom. Users have the option to attempt to restore their system data from backups, lose the data, or pay the requested ransom.[9,11,12] Healthcare policy under HIPAA has tried to adapt quickly to these new threats; however, OCR addressed the issue of ransomware attacks only relatively recently, through guidance delivered in July 2016.[24]

As annual hospital budgets are planned, including a line item for information security will be important for many reasons, including reputation.[25] A recent review found that, on average, healthcare organizations are spending 95% of their IT budgets on attempts to comply with federal initiatives, such as health IT implementation and adoption, and only 5% on security.[13] Hospitals would be judicious to include a compliance plan with consistent audits to verify who is accessing patient information. In addition, it is critical that hospital administrators support overall plans and penalties for those staff members who deliberately and maliciously access patient data outside of their job requirements. Access control to protected patient data in larger facilities is difficult to manage and adds to the vulnerability of patient information.[11] To protect patient information and to keep in line with the Minimum Necessary Rule under HIPAA, which states that PHI should not be used or disclosed unless necessary,[26] it is important to maintain and enforce a policy of access to the minimum necessary information for job performance. Finally, the Health Care Industry Cybersecurity Task Force, established in the Cybersecurity Act of 2015, has put forth guidance for hospitals to improve cybersecurity.[27] They recommend that insurance companies provide incentives specifically for small- and medium-size healthcare providers to transfer patient records to more secure environments. In addition, hospitals may consider cyber-insurance policies, which require security audits as a condition of coverage, to help protect their facilities from breaches and ransomware attacks.[12,27]

Limitations

Although many aspects surrounding healthcare privacy and data breaches were included in this study, not all could be accounted for. One limitation was that the OCR only had data available on breaches that affect 500 or more patients per case. Information on breaches and the at-fault facilities for all breaches affecting 499 patients or less was not accessible. In addition, the policy language around what is considered reportable in privacy breaches is vague, so these occurrences may have been under- or over-reported depending on the individual facility. The OCR data did not give specific dates and months of data breaches, only the year, and the 2016 data were not all available when we conducted the analysis. In addition, the survey questions used to measure biometric security systems only measured capability and infrastructure support and did not reflect use. Furthermore, all data used for this analysis were self-reported. Not all hospitals in the OCR database could be matched to the HIMSS and AHA analytics data files due to the possibility of facility closure, unverified city of breach, or inadequate information. In total, 15 hospitals were unable to be matched. VA hospitals were also unable to be matched because HIMSS does not monitor VA information. This study focused on hospitals due to the number of individuals affected by breaches in these types of facilities. However, other types of facilities, including physician practices, health plans, and clearinghouses, do have breaches and should be an area of focus for future research. Finally, it is important to note that most states have passed additional legislation that is more or less strict than the current federal iteration, which may or may not impact breach reporting.[28]

CONCLUSIONS

Although there are more group/physician practices within the United States than hospitals, the overall number of individual patients treated, and who thus have data created and stored within the record system, is greater within hospitals. Routine audits required by cyber-insurance coverage may help healthcare facilities recognize, and repair, their vulnerabilities before a breach occurs. Accordingly, information security systems should be concurrently implemented alongside health information technologies. Improving access control and prioritizing patient privacy will be important steps in minimizing future breaches. ■

Author Affiliations: College of Health and Public Affairs, University of Central Florida (MHG, AW, AN, KCW), Orlando, FL; United States Air Force (AR), Joint Base Charleston, SC.

Source of Funding: None.

Author Disclosures: The authors report no relationship or financial interest with any entity that would pose a conflict of interest with the subject matter of this article.

Authorship Information: Concept and design (MHG, AN, AR, AW, KCW); acquisition of data (AR, MHG); analysis and interpretation of data (MHG, AN, AR, KCW); drafting of the manuscript (MHG, AR, AW); critical revision of the manuscript for important intellectual content (MHG, AN, AR, AW, KCW); statistical analysis (MHG, AR); administrative, technical, or logistic support (KCW); and supervision (AR, MHG).

Address Correspondence to: Meghan Hufstader Gabriel, PhD, University of Central Florida, 4364 Scorpius St, HPAII, Rm 213, Orlando, FL 32816. Email: meghan.gabriel@ucf.edu.

REFERENCES

1. Dezenhall E. A look back at the Target breach. *HuffPost*. April 6, 2015. huffingtonpost.com/eric-dezenhall/a-look-back-at-the-target_b_7000816.html. Accessed July 22, 2016.
2. Anwar M, Joshi J, Tan J. Anytime, anywhere access to secure, privacy-aware healthcare services: issues, approaches and challenges. *Health Policy Technol.* 2015;4(4):299-311. doi: 10.1016/j.hlpt.2015.08.007.
3. Liginlal D, Sim I, Khansa L, Fearn P. HIPAA privacy rule compliance: an interpretive study using Norman's action theory. *Computers & Security.* 2012;31(2):206-220. doi: 10.1016/j.cose.2011.12.002.
4. Heubusch K. Little breaches: OCR releases first "small breach" data. *J AHIMA.* 2011;82(10):56-57.
5. Wilder M, Bennett B, Bianchi M, Peters N. HHS issues new HITECH/HIPAA rule: top ten changes. Hogan Lovells website. ehoganlovells.com/cv/07d443ca1b960fd9814fc6ae023b59c3661538c5. Published January 22, 2013. Accessed July 22, 2016.
6. LaTour KM, Eichenwald-Maki S, eds. *Health Information Management: Concepts, Principles, and Practice.* Chicago, IL: American Health Information Management Association; 2006.
7. Henry J, Pylypchuck Y, Searcy Y, Patel V. Adoption of electronic health record systems among U.S. non-federal acute care hospitals: 2008-2015. ONC data brief no. 35. Office of the National Coordinator for Health Information Technology website. dashboard.healthit.gov/evaluations/data-briefs/non-federal-acute-care-hospital-ehr-adoption-2008-2015.php. Published May 2016. Accessed September 1, 2016.
8. Adler-Milstein J, DesRoches CM, Kralovec P, et al. Electronic health record adoption in US hospitals: progress continues, but challenges persist. *Health Aff (Millwood)*. 2015;34(12):2174-2180. doi: 10.1377/hlthaff.2015.0992.
9. Sittig DF, Singh H. A socio-technical approach to preventing, mitigating, and recovering from ransomware attacks. *Appl Clin Inform*. 2016;7(2):624-632. doi: 10.4338/ACI-2016-04-SOA-0064.

10. Pal S, Biswas B, Mukhopadhyay A. Can HIT work alone? a security and socio-economic perspective of healthcare quality. Social Science Research Network website. papers.ssrn.com/sol3/papers.cfm?abstract_id=2740951. Published February 23, 2016. Accessed July 22, 2016.
11. Yaraghi N. A health hack wake-up call. *U.S. News & World Report*. April 1, 2016. usnews.com/opinion/blogs/policy-dose/articles/2016-04-01/ransomware-hacks-are-a-hospital-health-it-wake-up-call. Accessed July 22, 2016.
12. Yaraghi N. Hackers, phishers, and disappearing thumb drives: lessons learned from major health care data breaches. Brookings Institution website. brookings.edu/research/papers/2016/05/05-health-care-data-breaches-yaraghi. Published May 5, 2016. Accessed July 14, 2016.
13. Kruse CS, Frederick B, Jacobson T, Monticone DK. Cybersecurity in healthcare: a systematic review of modern threats and trends. *Technol Health Care*. 2017;25(1):1-10. doi: 10.3233/THC-161263.
14. Blanke SJ, McGrady E. When it comes to securing patient health information from breaches, your best medicine is a dose of prevention: a cybersecurity risk assessment checklist. *J Healthc Risk Manag*. 2016;36(1):14-24. doi: 10.1002/jhrm.21230.
15. Liu V, Musen MA, Chou T. Data breaches of protected health information in the United States. *JAMA*. 2015;313(14):1471-1473. doi: 10.1001/jama.2015.2252.
16. Gabriel M, Charles D, Henry J, Wilkins TL. State and national trends of two-factor authentication for non-federal acute care hospitals. ONC data brief no. 32. Office of the National Coordinator for Health Information Technology website. healthit.gov/sites/default/files/briefs/oncdatabrief32_two-factor_authent_trends.pdf. Published November 2015. Accessed September 1, 2016.
17. HHS Office for Civil Rights. How OCR enforces the HIPAA privacy & security rules. HHS website. hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/how-OCR-enforces-the-HIPAA-privacy-and-security-rules/index.html. Published 2011. Accessed February 2, 2016.
18. HHS Office for Civil Rights. Breach portal: notice to the secretary of HHS breach of unsecured protected health information. HHS website. ocrportal.hhs.gov/ocr/breach/breach_report.jsf. Accessed September 1, 2016.
19. AHA healthcare IT database: a supplement to the AHA annual survey of hospitals. American Hospital Association website. aha.org/research/rc/stat-studies/data-and-directories.shtml. Published January 2016. Accessed September 1, 2016.
20. Furukawa MF, Patel V, Charles D, Swain M, Mostashari F. Hospital electronic health information exchange grew substantially in 2008-12. *Health Aff (Millwood)*. 2013;32(8):1346-1354. doi: 10.1377/hlthaff.2013.0010.
21. Data by region. The Dartmouth Atlas of Healthcare website. www.dartmouthatlas.org/data/region. Accessed July 22, 2016.
22. Claunch D, McMillan M. Determining the right level for your IT security investment. *Healthc Financ Manage.* 2013;67(5):100-103.
23. Kwon J, Johnson ME. Security practices and regulatory compliance in the healthcare industry. *J Am Med Inform Assoc*. 2013;20(1):44-51. doi: 10.1136/amiajnl-2012-000906.
24. Thiemann T. Picking the right path to mobile biometric authentication. *Biometric Technology Today.* 2016;2016(2):5-8. doi: 10.1016/S0969-4765(16)30034-0.
25. Hoppszallern S. Skimping on IT security is costly. *Hospitals & Health Networks*. May 13, 2014. hhnmag.com/articles/4221-skimping-on-it-security-is-costly. Accessed September 1, 2016.
26. Sethi N, Lane G, Newton S, Egan P, Ghosh S. Disaster easily averted? data confidentiality and the hospital desktop computer. *Int J Med Inform.* 2014;83(5):385-391. doi: 10.1016/j.ijmedinf.2014.02.002.
27. Health Care Industry Cybersecurity Task Force. Report on improving cybersecurity in the health care industry. HHS Public Health Emergency website. phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf. Published June 2017. Accessed July 20, 2017.
28. Lopez VJ. Health data privacy: how states can fill the gaps in HIPAA. *University of San Francisco Law Review*. 2016. heinonline.org/HOL/LandingPage?handle=hein.journals/usflr50&div=17&id=&page=. Accessed July 22, 2016.

Full text and PDF at **www.ajmc.com**