Information Governance for Offsite Data Security

Save to myBoK

By Devendra Saharia

Disruptive technology can turn any industry on its head—virtually overnight. Just five years ago, summoning a taxi was an inefficient, time-consuming effort that often involved dialing up a dispatcher, who contacted a driver, who would then make their way to your location, perhaps in an hour or more. Today, competing smartphone apps connect drivers and passengers directly, resulting in a streamlined ordering and payment process that puts drivers at your doorstep almost immediately in major urban areas.

Now it's healthcare's turn, and the $3 trillion industry is learning firsthand the opportunities and challenges that come along with disruptive technologies like telehealth, electronic health records (EHRs), and Big Data—all of which promise to unlock healthcare's full potential in the United States. With each of these exciting new tools, however, come privacy concerns that require a comprehensive, proactive, and uniform approach to data security across an entire organization.

Use Information Governance-based Precautions to Manage Security Challenges

Awareness is perhaps the biggest information management challenge in today's global healthcare environment. Providers can be sometimes insular and there can exist many cultural differences regarding privacy even within departments of a singular organization.

The growing adoption of clinical and consumer-facing technology also poses unique challenges for the healthcare system. Many of these convenient technologies use cloud-based data storage services that may make life easier for patients and providers, but require special precautions to ensure data doesn't become a target for the latest sophisticated hacking techniques such as ransomware, advanced persistent threat (APT), and social engineering.

For example, the ongoing adoption of computerized technology allows providers to access patient health records and the latest medical research in real time. While it promises better treatment options and outcomes, it requires the digitizing and offsite storage of vast amounts of highly sensitive protected health information (PHI), which has become a rich target for hackers and identity thieves.

According to a 2015 Ponemon Institute study, healthcare data breaches in the United States are up 125 percent since 2010—a rate that's likely to increase as more and more healthcare systems go digital.[1] These breaches can also financially cripple a hospital system, physician practice, or ambulatory surgery center. The same study also found cyberattacks cost the US healthcare system over $6 billion each year.

Adding an additional layer of complexity, healthcare organizations must comply with strict privacy-related rules from federal, state, and local governments that may mandate specific administrative, physical, and technical safeguards to protect PHI. While the challenges may be numerous, they're not insurmountable. Providers can protect patient data, thrive in this new global environment, and limit exposure to attacks by implementing best practices in the following four areas.

Technical Safeguards

According to rules in the Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH) Act, providers should utilize a certified EHR system for exchanging electronic PHI. Furthermore, it is recommended that electronic PHI exchanges be encrypted to ensure transactions are not observed or interfered with.[2] Providers must be able to produce proof that PHI in their possession has not been altered or destroyed in an

unauthorized manner. Data corroboration controls, such as the use of checksums, digital signatures, and message authentication, are all approved under the data authentication HIPAA regulation.

In addition, providers should maintain written documentation showing network configuration settings. Beyond HIPAA and HITECH regulations, it is advantageous to employ two-factor authentication (secure hard tokens and SMS soft tokens) and e-mail encryption technology, and to disable USB, video recording, screen capture, CD drives, and paper printing for unauthorized users and devices.

Physical Safeguards

Placing limitations on removing or adding hardware and software from the network helps ensure PHI remains secure. Also, proper placement and visibility of workstations allows administrators to more closely monitor staff computer usage. Hardware and software access should be limited to authorized individuals only.

Providers looking for additional security measures should consider the use of physical location requirements to limit certain operations (i.e., coding) to designated delivery centers. Moreover, requiring coding operations staff to store personal electronics and bags in lockers, and the use of security guards and closed-circuit video cameras is also effective.

Administrative Safeguards

Providers should maintain a written set of policies and procedures encompassing all aspects of information security, including: anti-virus requirements; application considerations; presence of a designated privacy officer; business continuity and disaster recovery plans for unexpected incidents; and a ticketing system to track and record all systems' access requests and administration.

Per the HITECH Omnibus Final Rule, any cloud-based service provider processing or storing PHI must be deemed a business associate, who is now also an entity covered by HIPAA. For this reason, onsite staff members also should be required to wear photo ID badges at all times, and follow a robust entrance and exit policy.

Training Safeguards

To ensure HIPAA and HITECH regulations are followed, employees with access to electronic PHI should receive periodic information security training.[3] Additionally, administrators should embed information security best practices training in every stage of the employee lifecycle through the use of onboarding training, refresher assessments, poster campaigns, and newsletter articles from senior leadership.

Regular Audits Important for Ensuring Security Compliance

Regular internal audits should be carried out to monitor and enforce information security policy compliance.[4] Beyond these preliminary measures, a site compliance team—including certified auditors—should define and document the frequency, scope, procedures, and results of all internal audits. In addition to the above considerations, successful practices often impose strict human resource penalties targeted at enforcing proper compliance, require cross-functional risk assessments created outside of the facility's compliance team, abide by ISO/IEC 27001:2013 and SSAE 16/ISAE 3402 standards, and arrange for third party audits and certifications.

Network vulnerability and penetration testing (VaPT) also helps with evaluating a practice's security efforts. Vulnerability testing uses assessment tools to find weaknesses and flaws in a network, while penetration tests try to exploit these vulnerabilities to find out if unauthorized users can gain access and cause harm.

The transition to a value-based healthcare system in the United States also heightens the importance of these robust security measures. As more and more providers turn to outside firms to help cut costs while still providing high-quality care, it's imperative that these information governance best practices extend to all partners.

For example, as part of a competitive bidding process, providers should engage their organizations' top compliance and IT security officers to perform information security assessments to understand the potential risk of exposure. If a candidate does

not meet the criteria, then this should play a significant role in the due diligence and selection process, since inadequate information security controls pose massive risks to the organization's business and reputation.

And once a comprehensive plan is in place, it's also important to regularly assess ongoing security and privacy challenges—for both an organization and its outside partners. While it is true that data breaches are indiscriminate and unpredictable due to new risks that emerge periodically in the world of technology, it is definitely possible to substantially limit the possibility of a breach, keep PHI safe, and increase profitability by incorporating data security best practices into a daily routine.

Notes

[1] Ponemon Institute. "Criminal Attacks Are Now Leading Cause of Data Breach in Healthcare, According to New Ponemon Study." May 7, 2015. www.ponemon.org/news-2/66.

[2] Copeland, Kenneth W. and C. Jinshong Hwang. "Electronic Data Interchange: Concepts and Effects." Internet Society. www.isoc.org/inet97/proceedings/C5/C5_1.HTM.

[3] Experian. "2015 Second Annual Data Breach Industry Forecast." 2015. www.experian.com/assets/data-breach/white-papers/2015-industry-forecast-experian.pdf.

[4] Workgroup for Electronic Data Interchange. "Perspectives on Cybersecurity in Healthcare." June 2015. www.wedi.org/docs/test/cyber-security-primer.pdf?sfvrsn=0.

References

International Organization for Standardization. "ISO/IEC 27001:2013." October 1, 2013. www.iso.org/iso/catalogue_detail?csnumber=54534.

Deloitte. "ISAE 3402 and SSAE 16 (replacing SAS 70)." 2014. www2.deloitte.com/content/dam/Deloitte/lu/Documents/risk/lu_en_isae3402-ssae16_04072014.pdf.

Devendra Saharia (devendra.saharia@agshealth.com) is chief executive officer at AGS Health, Inc.

Article citation:
Saharia, Devendra. "Information Governance for Offsite Data Security" *Journal of AHIMA* 87, no.4 (April 2016): 20-23.