Electronic Health Records: Overcoming Security, Privacy, and Data Challenges

Published: December 2015

accusoft®

Electronic Health Records: Overcoming Security, Privacy, and Data Challenges

It's been almost two years since the January 2014 deadline set forth in the Health Information Technology for Economic and Clinical Health (HITECH) Act[1], for healthcare providers to adopt electronic health records (EHR). And while it's reported that 83 percent of office-based physicians[2] and 76 percent of hospitals have adopted at least basic EHR systems[3], there are still numerous security issues and concerns being addressed by healthcare facilities across the nation.

In fact, a recent Poneman Institute benchmark study[4] states that, "For the first time, criminal attacks are the number one cause of data breaches in healthcare. Criminal attacks on healthcare organizations are up 125 percent compared to five years ago." This is a concerning statistic, especially given that a survey found nearly one-quarter of patients withhold information from their providers due to security concerns.[5]

While the shift to electronic health and medical records was meant to improve efficiency, safety, and patient care, increased security breaches and patients' reluctance to share information could reduce the EHR program's overall benefits. This paper identifies four key EHR security and data concerns, and presents ways to address and even overcome some of them.

EHR Security and Data Challenges: The Top Four

Although the potential benefits from adopting EHRs are paramount to improved patient care, it's vital that providers address growing security and data concerns. With proper preparation, controls, and technology, it's possible to minimize some of the most prominent barriers to success.

Hacking

As more healthcare practices switch to digital records, there has been an increase in data hacking. And unfortunately, the rate and size of these breaches has led many public health officials to become increasingly concerned.

At the beginning of 2015, Anthem Inc. reported a data breach that exposed personal data for nearly 80 million of its customers.[6] In this instance, hackers attacked and gained access to internal database records.

At Howard University Hospital, more than 34,000 patients' data was compromised[7] when a hospital contractor downloaded their information to a personal laptop, which was stolen. While the laptop was password protected, the data itself was unencrypted. This means anyone able to bypass the laptop password could potentially have access to vital patient data.

Adoption

Many healthcare practices across the nation report having difficulty with EHR implementation because they lack the funding to support EMR adoption. Without gaining access to grants and loans, many of these practices simply don't have the funds to make the switch.

Even practices that already have the right type of technology installed in their offices have to pay a substantial amount of money for software and support to ensure that the EHR practices implemented are both effective and compliant with government mandates on both a federal and state level.

Outdated technology

To protect EHR data from malicious activity and careless exposure, systems need to employ the right technology solutions. And as technology continues to evolve from one day to the next, it often becomes difficult to make sure the EHR technology itself is up to date with the latest safety practices.

As can be imagined, keeping up with this ever-changing technology can be both costly and difficult. Not only does the implementation of newer technology result in having to update servers and systems, but it also leads to process and workflow issues. As personnel get comfortable with one EHR system, updates may take place, requiring them to learn newer ways of performing the same tasks.

Lack of training

As mentioned above, extensive training is often needed to ensure staff members know how to properly use new systems. Lack of training leads to an increase in security concerns because staff members won't understand the best ways to keep patient data safe. For example, if a staff member doesn't understand how to log out correctly, this can lead to patient data screens staying open, which makes it simple for unauthorized users to acquire access. Poor training can also result in patient data not be entered correctly, thus causing diagnoses and treatments to be inaccurate and ineffective.

Solutions: What Can You Do?

Fortunately, there are a variety of solutions that you can implement to minimize data and security concerns. There are three primary ways to address several data and security concerns, all of which are fairly simple to enforce.

Improve administrative controls

First and foremost, all EHRs should be password protected as well as encrypted. This means that when patient data is shared, it should be shared using encryption practices to help ensure it cannot be hacked. Administrative access to all pertinent data should be limited to staff members who need to see the data and absolutely no one else. Most EHR systems have a dashboard with administrative access options, and it's important that healthcare practices take advantage of this feature.

Monitor system access

EHR system administrators should be carefully and constantly monitoring access. Doing so makes it easier to quickly pinpoint unauthorized access and address threats. It also helps determine which data should be accessible by those without permission. For example, if a multi-specialty practice grants access to patient history to all physicians but one, this is an indicator that this physician may require access to ensure relevant data is being shared with the appropriate doctors. This not only enhances the sharing process, but it leads to better patient care.

Integrate advanced document viewers

Patient records are the lifeblood that keeps healthcare practices afloat. Not only do these records document vital patient data, but they also lead to an improvement in insurance reimbursements. Unfortunately, though, many healthcare records are saved in a variety of formats, which can lead to difficulty and confusion when trying to read them, especially when sharing between practices. With a secure and efficient document viewer, it becomes possible to read and share documents such as medical and financial records, insurance forms, physician's' orders, prescriptions, X-rays and lab results, regardless of the formats they are in. The value that document viewers can bring to a healthcare practice are often overlooked, and include:

- Universal document viewing
- Improvement in EHR system functionality
- Enhanced flexibility and scalability
- Mobile web viewing
- Streamlined document processing

Conclusion

While healthcare patient data will always be a target for hackers, there are steps providers can take to minimize threats and improve EHR security. Not only will this promote compliance with the latest mandates, but it also enhances and improves patient care. Additionally, implementing the right technology tools and document management processes will boost provider efficiency and quality.

Sources

[1] http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitechenforcementifr.html

[2] http://dashboard.healthit.gov/quickstats/pages/physician-ehr-adoption-trends.php

[3] https://www.healthit.gov/sites/default/files/data-brief/2014HospitalAdoptionDataBrief.pdf

[4] https://www2.idexpertscorp.com/fifth-annual-ponemon-study-on-privacy-security-incidents-of-healthcare-data

[5] http://www.softwareadvice.com/medical/industryview/hipaa-breaches-report-2015/

[6] http://www.wsj.com/articles/health-insurer-anthem-hit-by-hackers-1423103720

[7] https://www.washingtonpost.com/national/health-science/medical-data-breaches-raise-alarms/2012/06/02/gJQAVPWt9U_story.html

To learn more, visit accusoft.com or call 800-875-7009.

About Accusoft

Accusoft provides a full spectrum of document, content and imaging solutions as fully supported, enterprise-grade, best-in-class client-server applications, mobile apps, cloud services and software development kits (SDKs). The company's HTML5 viewing technology is available to the enterprise as Prizm Content Connect, in cloud-based SaaS versions, and in a version optimized for SharePoint integration.