SecurityFirst™
Protecting Critical Data

Protecting Electronic Health Records

Accurate, Efficient, and… …Vulnerable

Medical records are among the most valuable data for sale on the dark web because they contain an abundance of both current demographic and historical personal and family information. They are among the most comprehensive collections of a person's identity data. Today Electronic Health Record (EHR) systems are in use by more than 96% of U.S. non-federal acute care hospitals, storing petabytes of electronic Protected Health Information (ePHI). This new application of information technology—driven in part by governmental incentives—occurred while cybercrime was maturing and increasingly perpetuated by professional thieves. As healthcare providers struggled to acquire and implement new systems, security controls were neither understood nor well-funded, making healthcare especially vulnerable to data losses.

The simple fact is this: accurate data, shared efficiently has led to better and more cost-efficient healthcare. When doctors, hospitals, pharmacies and the like stopped generating paper and started collecting digitized data, service efficiencies improved, processing errors decreased, and escalating costs came under control. Cybercriminals quickly discovered how lucrative attacks on healthcare providers could be. Additionally, medical organizations became a prime target for newer, ransomware attacks. Since the loss of IT operations can greatly impact patient care—most of the organizations suffering attacks have simply paid the ransom with the expectations of a full recovery.

Privacy Rules and Compliance

Despite any lack of security guidance or general skills for information technology usage, healthcare providers and insurers did have decades of experience establishing privacy practices. Complex regulations such as HIPAA (Healthcare Insurance Portability and Accountability Act of 1996) and the later HITECH (Health Information Technology for Economic and Clinical Health) Act of 2009 defined mandatory procedures for safeguarding access to Protected Health Information (PHI). Unfortunately, these compliance regulations stop short of mandating specific data protections.

Organizations that suffer a data breach of more than 500 records must report it to the Secretary of Health and Human Services (HHS), to the affected individuals, and sometimes even to the media. Fines may also be assessed based on the degree of any willful neglect or a failure to correct the situation within a 30-day period following the discovery of a breach, but only if the breach contained unsecured ePHI and the organization can produce documentation to demonstrate a low probability of compromise based on a multi-point risk assessment.

Insiders Leaks and Ransomware

The threats to healthcare data security are not just external. Verizon's 2018 Data Breach Investigations Report states that healthcare is "the only industry where the threat from inside is greater than that from outside." Of the 750 incidents occurring in 2017, 536 had confirmed data breaches and 56% of the attacks were due to insiders, accidentally or maliciously. Apart from education, little can be done to ensure that authorized users don't make catastrophic mistakes, but the implementation of advanced data access controls can limit the downside to this type of unauthorized disclosure.

While insider threats are often pictured as a rogue employee taking advantage of privileged access permissions, more often it is an accidental or uninformed action as in the cyberattack on Anthem Inc. In March of 2015, Anthem filed a breach report to the HHS Office for Civil Rights (OCR) per HIPAA guidelines. It was found upon investigation that the attack was the result of phishing emails where at least one employee made the mistake of responding. It was reported that the attackers got access to the ePHI of almost 79 million people. The HHS announced on October 15, 2018 that Anthem has agreed to pay $16 million to the OCR and take substantial corrective actions to settle potential violations of the HIPAA Privacy and Security Rules. The $16 million settlement eclipses the previous high of $5.55 million paid to OCR in 2016. This is in addition to a $115 million class action settlement related to the breach, that was approved by the courts on August 15, 2018.

Verizon's 2018 report also names ransomware as the dominant form of malware, present in 85% of all healthcare breach reporting. According to the HHS, when ePHI is "locked-up" as the result of a ransomware attack, a breach has occurred because the ePHI was acquired (i.e., unauthorized individuals have taken possession or control of the information), and therefore it is defined as a “disclosure” under the HIPAA Privacy Rule. Whether ransomware is more prevalent in healthcare is difficult to say as the statistic may just reflect the industry’s more stringent reporting requirements, but data should be more recoverable because implementing a data backup plan is a Security Rule requirement for HIPAA covered entities.

Ransomware attacks have been on the increase, especially against small to mid-size healthcare providers such as Hancock Health based in Greenfield, Indiana, who reportedly paid hackers $55,000 in bitcoins to unlock systems following a ransomware infection or the Cass Regional Medical Center in Missouri, whose attack caused trauma and stroke patients to be diverted to other facilities for over a week. Paying a ransom doesn’t always result in getting your data back, and the additional costs to manage through and after the attack can be very expensive, especially bringing security processes up to HIPAA standards.

Good Security Hygiene

There are many forms of available data protection, even some natively available in operating systems or data storage. HIPAA regulations all center around practicing good security hygiene, such as applying timely updates and patches to applications and operating systems, properly configuring firewalls, and managing how networks, servers and data are accessed. This requires leveraging identity and access management (IAM) tools and using up-to-date anti-malware software. In addition, you should make sure that your critical data assets are encrypted in transit and at rest, as well as backed up on a regular basis.

Encrypting data important because following a breach of unsecured ePHI, covered entities must inform affected individuals, the HHS Secretary, and sometimes even the media; however, notification is only required if the breach involved unsecured ePHI. Data that can only be seen in a decrypted state by authorized users is by definition secure, and therefore can minimize, even prevent having to report an unauthorized access event.

Can You Trust the Cloud with ePHI?

The cloud can be a scary place, especially for those who wear an IT hat as a job. Cloud Service Providers offer highly scalable infrastructure and object storage to healthcare providers who must maintain vast amounts of patient records for long periods of time. In addition, the cloud can be used as part of disaster or ransomware recovery contingency plan to protect business continuity.

While scalability and cost may entice many organizations to cloud services, it does mean that you are ceding the management and access to your critical data to a 3rd party. To protect health information, especially ePHI, data sent to the cloud should be rendered unreadable, undecipherable and unusable to all unauthorized recipients. Therefore, control must remain in the hands of the healthcare organization, not the cloud service provider, and data should be encrypted before sending to object storage for optimal security.

ePHI Data Protection by Design and Default

DataKeep supports covered entities in relation to data protection requirements under HIPAA and can help avoid breach notification requirements by protecting ePHI with access management, encryption and monitoring. Enterprises can quickly and easily apply this software-only solution to data within their network environments, even including datasets migrated to a cloud environment for long-term storage. Other organizations may prefer to select a managed services provider (MSP) to help with the management of data-centric protection from the broad network of SecurityFirst partners.

SecurityFirst™ delivers advanced security solutions that build a firewall around your data to protect against ever increasing threats and to aid in meeting regulatory requirements such as GDPR, HIPAA, NYCRR and many others.

DataKeep™, our flagship product, serves as your data firewall by using advanced encryption, scalable hierarchical key management, extensive policy enforcement and monitoring of unauthorized access to deliver the highest levels of availability, resiliency and time to value. Security requires a layered approach and protection of the data itself is your last line of defense.

For a product demonstration or more information contact:
sales@securityfirstcorp.com
888-884-7152
securityfirstcorp.com