

Health Services and HIPAA: Providing Internal Security and Privacy of Health Information Records

How Shalom Security Platform Protects Patient Records and Enforces HIPAA Act Compliance

Industry Focus: Healthcare providers, pharmaceutical, clearinghouses, insurance companies, and any institution that stores or transmits patient health information in electronic form

On August 21, 1996 the Health Insurance Portability and Accountability Act was signed into Federal Law as Public Law 104-191. This law impacts all areas of the health care industry and was designed to protect the privacy, confidentiality and security of health care information, and provide insurance portability to improve the efficiency of health care by standardizing the exchange of administrative and financial data. Section II of the HIPAA Act is responsible for “administrative simplification” and it has five primary parts to it:

1. Privacy of patient health records.
2. Security of patient data (from external attack and internal misuse).
3. Electronic Transaction Standards for exchange of health records.
4. Standard Code sets.
5. National Identifiers.

Patient health care is one of society's fundamental building blocks. With the move to electronic medical records, in order to improve efficiency, it is important that we secure patient information and manage it with the right care and security



In the health care industry, sensitive patient health and financial information is collected, transferred and shared electronically among health care providers. Whether in transit or in storage, it is important that patient information is safeguarded not only from external attack, but more so from possible malicious insiders who may want to divulge such sensitive data to wrongful parties. The Health Insurance Portability and Accountability Act addresses this issue of data privacy, but from an implementation perspective, very little attention is given to the security of patient records on the inside. If an intruder steals log on credentials of a legitimate healthcare IT administrator, the privacy and security of archived electronic patient records becomes at risk. Therefore, a need exists for automated insider security systems to

contain both impostors and malicious insiders.

NOWELL SHALOM SECURITY PLATFORM PROTECTS PATIENT HEALTH INFORMATION BY CATCHING BAD INSIDERS AND AUTHENTICATING INTRUDERS INSIDE THE NETWORK

In some cases, malicious insiders are responsible for the theft of electronic health records. When deployed, Shalom Security software provides a proactive inner security system to address both malicious insiders and impostors within the network.

- Software monitors, analyzes and provides a full behavior audit trail of user activity including network access, time usage, cloud application use, database server accesses, behavior profiling, and context review.
- Employs authentication to prevent identity theft; After a failed authentication, by simply denying further access to an impostor disguised as legitimate users, Shalom Security eliminates the risk of intruders accessing your sensitive health records. It also reports “phony” backdoor accounts and implanted automated scripts.
- In real time, Shalom Security authenticates malicious insiders at the very moment they behave suspiciously, reporting them and stopping them from stealing public health records.
- Optionally, software can be configured to only detect and report suspicious, high-risk behavior of information use, without any authentication or end-user disruption

Insider security safeguards must be implemented to fully protect the confidentiality, integrity and availability of electronic health information. HIPAA security rules set standards for basic safeguards to prevent unauthorized access, alteration, deletion, and transmission and must include an internal security policy, process, and technology to enforce the policy