Securing Electronic Healthcare Records (EHRs) and Protecting Patient Privacy

Patient health records are worth more on the black market than any other data — and for good reason: They contain a treasure trove of extremely sensitive personal data. In addition to personally identifiable information (PII), health records can contain the patient's blood type, allergies, medications prescribed and any adverse reactions, medical devices in use, as well as past procedures and diagnoses — some of which can be incredibly private.

The breadth of sensitive data in electronic health records (EHRs) opens a variety of opportunities for cyberattackers, from identity theft and insurance fraud, to blackmail and even bodily harm. Exposure of this data could be detrimental to a patient's livelihood and sense of well-being — even their life. The very mission of a healthcare organization is to protect the patients in their care. In today's digital age, that means protecting the patient's data as well.

The Challenge: Protecting Patient Data, New and Old

Unfortunately, protecting EHRs and patient data is no simple matter. Many healthcare organizations have multiple EHR systems, which communicate and integrate with other clinical systems, such as imaging, pharmaceutical, anesthesiology, and telehealth. EHR data can't necessarily be changed or deleted. In many cases, records must remain accessible; for example, for any patient whose bills are outstanding. Providing a complete picture of a patient's medical history is difficult due to the challenges of creating and implementing a system that can transfer health records with various providers while being secure.

While technology is available to detect violations associated with EHRs, these systems are often antiquated or incapable of monitoring patient data in real time. This presents a real challenge when it comes to meeting regulatory compliance requirements. The Health Insurance Portability and Accountability Act (HIPAA) specifies a 500-record threshold of compromised files before the organization is fined, and required to make public statements, take out advertisements, and add banners to the website, all shining a light on the fact that patient data in the organization's care was breached. As a result, HIPAA violations could all result in significant brand damage, which in turn impacts revenues. It's therefore imperative that organizations have the ability to detect and respond to attacks in a timely manner.

How to Gain Visibility and Control

Network monitoring provides the network and application visibility you need to address EHR and patient privacy risks. Whether the EHR solutions are in the cloud or on-premises, an analyst or security team must monitor the network and the services in real time from a centralized point. A security information and event management (SIEM) platform allows healthcare organizations to see the traffic flowing to and from all the systems in the IT environment, and determine who's inappropriately accessing patient records, how often they're using "break-the-glass"-type mechanisms to do so, and from where.

The LogRhythm NextGen SIEM Platform offers comprehensive, single-pane-of-glass visibility into legacy systems and cloud-based solutions, including EHR systems. LogRhythm can help bridge detection and response for security threats by correlating that with health records violations and other healthcare operational technology, such as medical devices and physical security. As a result, LogRhythm enables you to quickly respond to threats and prevent breaches of EHR data.

The NextGen SIEM Platform also monitors cloud services for alignment to compliance requirements. LogRhythm's prebuilt Health Care Compliance Automation Module provides a comprehensive security framework that helps protect your patients and improve your organization's security posture. The module features capabilities to help you comply with HIPAA and HITECH guidelines, including:

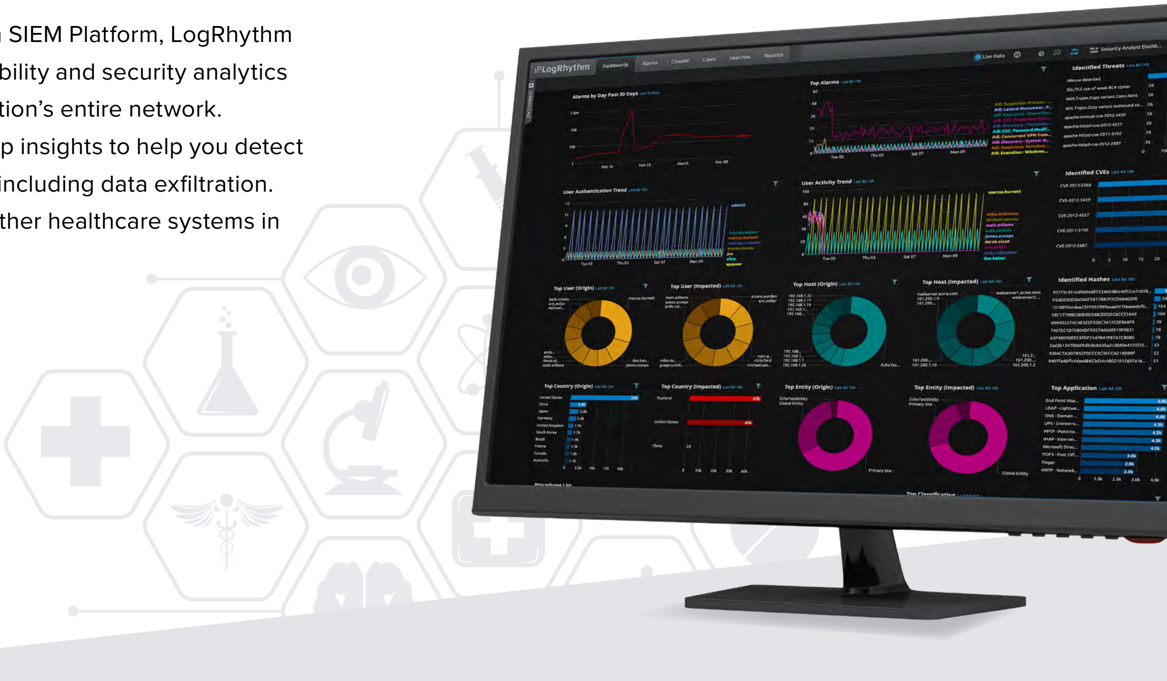
- Analysis rules built to support healthcare to monitor your environment, staff, and vendors for risks and policy violations associated with HIPAA and HITECH guidelines.
- Investigation queries designed to answer and address key questions associated with investigations and regulatory requirements.
- Prebuilt reports that directly map to HIPAA directives.

When integrated with the NextGen SIEM Platform, LogRhythm NetMon provides the real-time visibility and security analytics you need to monitor your organization's entire network. NetMon delivers rich data and deep insights to help you detect and respond to advanced threats, including data exfiltration. NetMon integrates with Epic and other healthcare systems in your IT environment.

Security orchestration, automation, and response (SOAR) from LogRhythm helps you automate workflows and accelerate threat qualification, investigation, and response. In other words, SOAR enables you to identify and stop attacks faster — reducing the risk of a data breach and reaching HIPAA's 500-record threshold. With RespondX, the LogRhythm NextGen SIEM Platform provides everything you need to incorporate SOAR technology. It easily integrates with your current and future technologies so your team can accelerate response and remediation.

LogRhythm: More Than Technology

LogRhythm knows healthcare. We have deep expertise in healthcare workflows and the nuances of security operations in a health IT environment. This is evident in our Health Care Compliance Automation Module and deep integrations with other health IT systems, which are designed to help take some of the challenges out of securing your healthcare systems and data.



To see how LogRhythm can help solve the unique challenges of protecting EHRs and patient privacy, schedule a demo today.

logrhythm.com/demo