

With healthcare organizations moving increasingly to electronic means of storing PHI, protecting that data becomes a much more important task for IT departments. Adding to the complexity of this task is the rapidly growing number of diverse technologies used for processing and storing ePHI. Each platform has its own format for recording specific activities, making it difficult for organizations to easily discover nefarious behavior.



Not only is the difficulty of securing confidential data mounting, penalties for failing to do so are becoming increasingly severe. An improperly reported breach can cost an organization tens of thousands of dollars in fines, not to mention the long term ramifications of lost confidence and revenue.

**LogRhythm provides healthcare organizations with the means to proactively protect ePHI, as well as the tools to accurately and quickly identify the culprits guilty of breaches.**

Secure the Audit Trail	Understanding User Activity	Enabling Rapid Response
<p><b>CUSTOMER CHALLENGE</b></p> <p>Healthcare organizations need to collect, securely store, and provide ready access to all ePHI-related log data for internal and external auditing and compliance. Accomplishing this with high volumes of data from a multitude of device types and formats is overly resource and infrastructure intensive for most organizations.</p>	<p>Tracking individual user behavior and understanding the relevant context of that activity has historically been a time-consuming and manual process - assuming that an organization knows where to look in the first place.</p>	<p>Organizations that experience an ePHI data breach are required to provide accurate forensic data containing all relevant details about the incident in a timely fashion. However, most IT groups are ill equipped to comply with such mandates, exposing their organizations to hefty fines and additional risks.</p>
<p><b>LOGRHYTHM SOLUTION</b></p> <p>LogRhythm automates the collection and secure archiving of all log data, regardless of the source, across the entire environment. The SecondLook™ archive restoration wizard allows administrators to immediately query against any archived data, which automatically validates the digital chain-of-custody.</p>	<p>LogRhythm provides extensive data enrichment and automatically categorizes event data into meaningful, easy-to-search categories. Additional features, such as Active Directory integration, provide meaningful user and network-related context related to an event.</p>	<p>LogRhythm provides automated alerting, to immediately notify administrators of potentially inappropriate user behavior, such as any time a high-profile record is accessed. Wizard-driven investigations and reporting tools provide immediate access to the details surrounding any potential breach.</p>
<p><b>ADDITIONAL BENEFITS</b></p> <p>LogRhythm's secure archive and rapid recovery capabilities provide compliance assurance, reduced operational burden on IT staff, and unparalleled access to longterm forensics data.</p>	<p>Users are able to alert, investigate and search on simplified, intuitive data, making it easy to pinpoint suspicious behavior and specific activity tied to a single user among thousands. One-click contextualization gives administrators immediate access to specific details about that user.</p>	<p>Administrators have real-time access to incident-related information, such as a user emailing files to a newspaper after accessing a high-profile patient's records. This allows them to respond quickly to possible breaches, avoiding fines for delayed detection and response.</p>