

ScienceLogic EM7 HIPAA Assessment Summary

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) presents a unique, enterprise-wide, compliance challenge for health care organizations. Healthcare organizations that are federally mandated to comply with the HIPAA regulations are required to implement safeguards to comply with the HIPAA security standards. These safeguards must protect the data administratively (policies), physically and technically. The HIPAA standards do not mandate the use of any specific technological solutions. However, certain devices, such as ScienceLogic's EM7, may reduce the burden of compliance for a healthcare organization.

ScienceLogic has performed a self-assessment of its EM7 tool, and has concluded that EM7 assists in compliance of numerous HIPAA requirements and can help facilitate implementation of the HIPAA standards within healthcare organizations.

Specifically, EM7 provides support in the following areas:

- 1) Risk Analysis, Risk Management & Information System Activity Review, found in Administrative Safeguards – Section 164.308(a)(1)
 - a. Risk Analysis
 - i. The EM7 System provides reporting regarding network and system configurations that can facilitate the Risk Analysis process.
 - b. Risk Management
 - i. The EM7 System provides reporting regarding changes in network and system configurations and access policies that can facilitate the Risk Management process.
 - c. Information System Activity Review
 - i. The EM7 System is capable of storing and parsing server, workstation and network device logs. Using this data, successful and failed log-in attempt can be monitored assisting in the IS Activity Review.
- 2) Protection from Malicious Software and Log-in Monitoring included in Security Awareness and Training – Section 164.308(a)(5)
 - a. Protection from Malicious Software
 - i. The EM7 System can be configured to watch for the opening of ports related to known malicious software.
 - ii. The EM7 System can be configured to watch for running processes that are known to be associated with malicious software.
 - b. Log-in Monitoring
 - i. The EM7 System includes functionality that can monitor successful and failed log-in attempts to server and workstations.
- 3) Response and Reporting part of Security Incident Procedures – Section 164.308(a)(6)

- a. The EM7 System has a fully featured monitoring component that can be used to assist in addressing the HIPAA requirement to identify suspected or known security risks.
 - b. The EM7 System has a fully featured ticketing and notification system (e-mail or IM). This system can assist organizations in addressing the HIPAA requirement to respond to suspected or known security incidents.
- 4) Asset Tracking for Disaster Recover part of Contingency Planning – Section 164.308(a)(7)
- a. The Asset Management functionality included in the EM7 System may assist organizations in developing contingency and disaster recovery plans in order to comply with the HIPAA requirement.
- 5) Evaluation – Section 164.308(a)(8)
- a. As part of the HIPAA requirements, covered healthcare organizations are required to undertake periodic evaluations of their security policies and procedures. The EM7 System can assist in these evaluations by producing reports regarding event logs, system usage, log-in attempts, etc.
- 6) Facility Access Controls – Section 164.310(a)(1)
- a. The EM7 System can interface with many physical access control systems to maintain the data gathered by these systems. This data can then be later used to generate reports to assess and assure HIPAA compliance. The collected data can include information ranging from the times that secured doors are opened and closed to information about personnel entering secure facilities by means of a badge or other scan.
- 7) Technical Access Controls – Section 164.312(a)(1)
- a. The EM7 System can gather and store data about workstation, server and network device successful and failed log-in attempts. In addition, the system can be configured to send alerts based on multiple failed log-in attempts or other access control related policies.
- 8) Audit Controls – Section 164.312(b)
- a. Under the HIPAA Security rules covered organizations are required to examine the activity of their information systems that contain protected health information. The EM7 System can generate reports that show log-in activity, activity based on server, workstation and network logs, downtime of devices, server hardware utilization and bandwidth utilization. These reports can assist in fulfilling these requirements.
- 9) Documentation – Section 164.316(b)(1)
- a. The extensive reporting capabilities of the EM7 System can be used to produce documentation to fulfill the requirement that records of activities associated with covered systems be maintained. The EM7 System includes the capability to export these reports as PDF files