




- [Solutions](#)
- [Products](#)
- [Industries](#)
- [Customers](#)
- [Partners](#)
- [Support](#)
- [Company](#)
- [Contact Us](#)



**Solutions**

[Security & Log Management](#)

[Compliance Auditing](#)

PCI DSS

**HIPAA**

Sarbanes-Oxley

NISPOM

FISMA

DCID

NERC

ISO 27002

[IT Operations & Risk Management](#)

[Business Data Intelligence](#)

**SenSage Compliance Auditing for Health Insurance Portability and Accountability Act (HIPAA) and Joint Commission Standards**

As a health care provider, health insurance plan, and even certain types of employer, you know that you are bound to the audit requirements created by the Health Insurance Portability and Accountability Act (HIPAA) enacted by Congress in 1996. Additionally, the Joint Commission has several standards relating to the issue of client privacy and confidentiality.

The Privacy sections of HIPAA outline the access restrictions of data known as Protected Health Information (PHI) which can be broadly defined as any part of a patient's medical record or payment history.

The Security Rule sections specifically outline the types of security precautions that must be followed and this includes:

- Physical Safeguards- controlling physical access to protect against inappropriate access to protected data
- Technical Safeguards - controlling access to computer systems and enabling covered entities to protect communications containing PHI transmitted electronically over open networks from being intercepted by anyone other than the intended recipient

SenSage has worked with hundreds of health care providers and plans to develop a log management solution with out of the box reports that will pass the scrutiny of internal auditors, the Joint Commission and the HHS Office of Inspector General and allow your organization to demonstrate compliance.

Examples of SenSage's out-of-the-box compliance reports for satisfying audit requirements include the following:

SenSage Compliance Report	HIPAA Audit Requirement
<b>Privileged Account Access Detailed</b>	§ 164.308 (a)(1)(ii)(B) and (D), § 164.308 (a)(4)(ii)(B), § 164.308 (a)(5)(ii)(C)
<b>Privileged Account Access Summary</b>	§ 164.308 (a)(1)(ii)(B) and (D), § 164.308 (a)(4)(ii)(B), § 164.308 (a)(5)(ii)(C)
<b>Privileged Command Summary</b>	164.308 (a)(6)(ii) and (a)(8), § 164.314 (b) and (d)
<b>Privileged Account Activity Detailed</b>	§ 164.308 (a)(3)(ii)(A), § 164.308 (a)(4)(ii)(B) and (C), § 164.308 (a)(5)(ii)(C), § 164.308 (a)(6)(ii), § 164.314 (b)

SenSage's flexible architecture works with any data source and supports all major databases and all Health Care Management Software solutions.

Further demonstrating our value in the health services market, SenSage was selected by Cerner Corporation (NASDAQ: CERN), the largest healthcare IT systems provider, as its solution provider partner for log management and HIPAA compliance.

**Resources**

**Gartner**

- Gartner 2009 SIEM Magic Quadrant
- Critical Capabilities for SIEM Technology

**Brochures**

[HIPAA](#)

**White Papers**

[Audit Trail Analysis for Safeguarding Electronic Protected Health Information \(EPHI\)](#)

**Case Studies**

[SANS Maximizing Logging RC Noridian](#)

**News**

[Button Up - Blue Cross Blue Shield on HIPAA Compliance](#)

**» Contact Us**