SAVIYNT FOR HEALTHCARE
SOD Workbench

SAVIYNT

Access Compliance and SOD Management Solutions for the Healthcare Industry

HIPAA COMPLIANCE

Regulatory Challenges

Regulatory requirements including HIPAA, HITRUST and PHI, compounded by data breaches, amplify the need for appropriate, secure user access.

Identifying high-risk SOD violations in clinical and revenue cycle modules, and defining controls for high-privileged access remains a critical issue.

> "We're using Saviynt to manage access provisioning to our Epic system, which is a very important system for Partners Healthcare. It does role management for 2,500 different levels of access and provisions and deprovisions fine-grained entitlements. It's a huge time saver: it replaces a manual process with a very well functioning automated process."
>
> — Ivan Childress, Manager, IAM
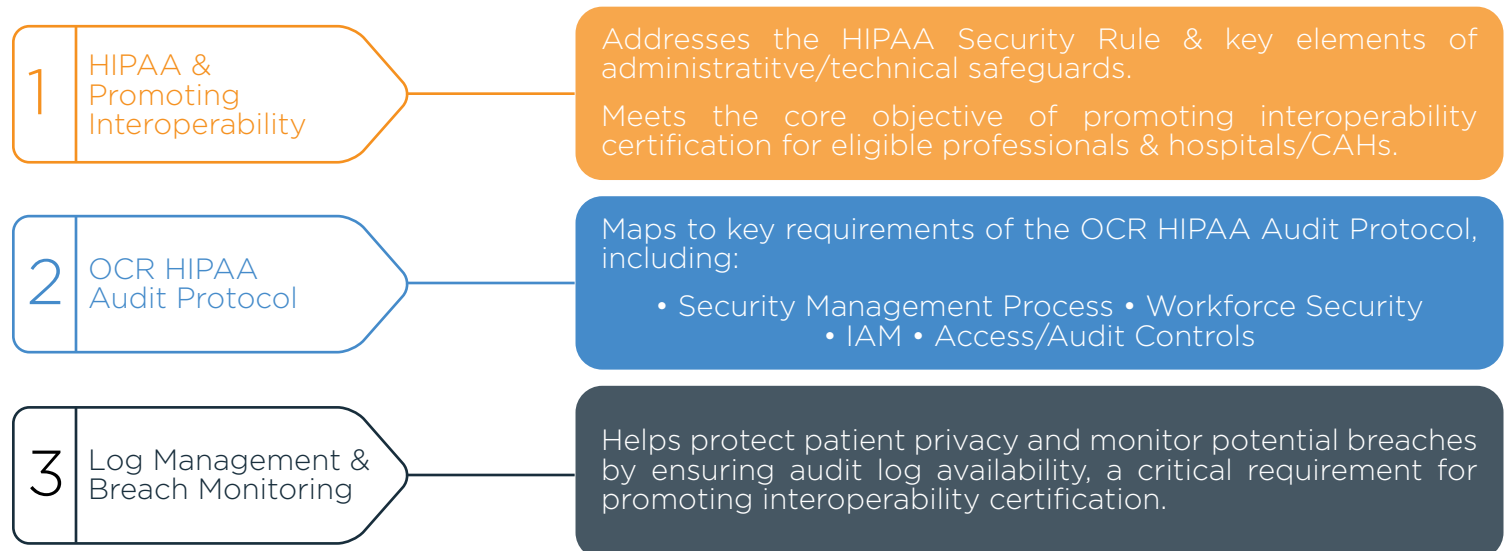> Partners Healthcare
>
> **PARTNERS HEALTHCARE**

Why Segregation of Duties (SOD)?

Healthcare organizations must comply with strict HIPAA rules and security measures to reduce risks and vulnerabilities. They must also ensure confidentiality, integrity and availability of all electronic protected health information.

Organizations often adopt the NIST Special Publication guideline to address HIPAA rules, which describes the enforcement of SOD through assigned access authorizations.
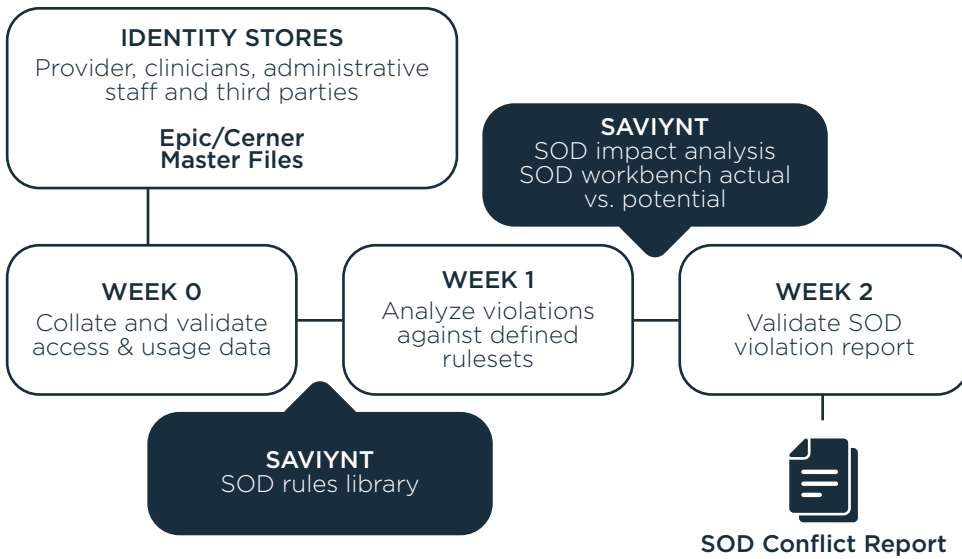
The NIST standard recommends implementing access controls on information systems to prevent users from having all of the authority to perform fraudulent activity, to help prevent collusion. For example, the same person that issues refunds shouldn't be the approver of those refunds. This ensures that no malevolent activity goes unnoticed and corrective remediation measures can be taken.

Necessary Features of a Healthcare Regulation & Compliance Solution

1 HIPAA & Promoting Interoperability

Addresses the HIPAA Security Rule & key elements of administratitve/technical safeguards.

Meets the core objective of promoting interoperability certification for eligible professionals & hospitals/CAHs.

2 OCR HIPAA Audit Protocol

Maps to key requirements of the OCR HIPAA Audit Protocol, including:

- Security Management Process • Workforce Security
- IAM • Access/Audit Controls

3 Log Management & Breach Monitoring

Helps protect patient privacy and monitor potential breaches by ensuring audit log availability, a critical requirement for promoting interoperability certification.

SOD WORKBENCH FOR HEALTHCARE

Multi-state environments including healthcare providers employ various silos to store and manage content. This creates a wide array of access needs, and the complex hierarchies of healthcare EHR platforms often hide SOD violations.

IDENTITY STORES
Provider, clinicians, administrative staff and third parties
Epic/Cerner Master Files

SAVIYNT
SOD impact analysis
SOD workbench actual vs. potential

WEEK 0
Collate and validate access & usage data

WEEK 1
Analyze violations against defined rulesets

WEEK 2
Validate SOD violation report

SAVIYNT
SOD rules library

SOD Conflict Report

AUTOMATE SOD ANALYSIS

- Identify various user access permissions causing SOD violations
- Our platform accelerates analysis of the current state of SOD conflicts in healthcare revenue cycles, based on a pre-built controls library
- The library has hundres of controls and can be customized based on user preferences
- Connectors for EMR/EHR and HR platforms include Epic, Cerner, McKesson, Meditech, Workday, PeopleSoft, SAP HR and others, further automating the extraction of access and usage data

REMEDIATE SOD VIOLATIONS

- Rank SOD violations based on criticality, severity and impact
- Remediate SOD violations by removing conflicting entitlements or roles from users
- Alternately apply and document compensating controls, e.g. additional monitoring, approval steps or risk acceptance
- Assign ownership and/or duration to revisit the SOD violation in future

PREVENTIVE SOD CONTROLS

- Maintain a SOD free environment on a continual basis by integrating preventive SOD validation during access request
- Our Intelligent Access Request System not only automates appropriate approvals, it also identifies increased risk or potential SOD violations in real-time if the request is approved
- This allows the approver to make an informed decision about whether to approve the request and assign compensating control as necessary

Intelligent Identity. Smarter Security.

The SOD remediation process relies on close coordination between various teams. Our intelligent, integrated SOD Workbench for automated remediation delivers these capabilities and benefits:

- Automatic recommendations on security class and template SOD violations
- Access remediation simulation enables impact asessment and intelligent decision-making
- Analysis of usage logs identify whether existing SODs were unknowingly exploited by users— a powerful tool for prioritizing SOD review and detecting fraud
- Mitigating control management for assignment of oversight and ownership to individuals
- Time-bound mitigating controls to enforce continuous review
- Automation remediates users to prevent conflicting templates and functions

Saviynt's IGA solution automates the burdensome policies and processes associated with healthcare access management. Robust analytics segregates duties and delivers regulatory compliance with sufficient flexibility to adapt to organizational changes.

Saviynt USA Headquarters | 1301 E. El Segundo Blvd, Suite D, Los Angeles, CA 90245 USA
Phone: 310-641-1664 | www.saviynt.com | info@saviyntsale.com

Intelligent Identity. Smarter Security.