SAVIYNT

SAVIYNT FOR EPIC

COMPREHENSIVE SOLUTION FOR ACCESS COMPLIANCE AND SOD MANAGEMENT

WHY SEGREGATION OF DUTY (SOD) CONTROL?

HIPAA rules 164.306(a) and 164.308(a)(1)(ii)(B) specify the implementation of security measures that are sufficient enough to reduce risks and vulnerabilities and to ensure confidentiality, integrity and availability of all electronic protected health information. One guideline that organizations adopt to address these HIPAA rules is NIST Special Publication 800-53 AC-5. It describes the enforcement of Segregation of Duties (SOD) through assigned access authorizations. The NIST standard recommends the implementation of access control on the information system that prevents users from having all of the necessary authority or information access to perform fraudulent activity without collusion.

SOD control is critical in order to prevent inappropriate and erroneous actions by ensuring that not ONE person is responsible for initiating transactions, reviewing/approving transactions, recording transactions, reconciling balances and handling assets. This ensures that no malevolent activity goes unnoticed and corrective remediation measures can be undertaken. For example, the same person issuing refunds and reversing transactions or payments (HB) cannot be the approver of those refunds.

Segregation of duties can sometimes be difficult to adopt (especially for smaller institutions where fewer employees perform multiple roles); it could prove cumbersome to implement and manage. In such cases where duties cannot be sufficiently segregated, compensating controls need to be implemented with a detailed and periodic supervisory review of overlapping activities. Saviynt enables organizations with the means to effectively identify, remediate and avoid SOD conflicts on a continuous basis.

1. AUTOMATE SOD ANALYSIS WITH SAVIYNT:

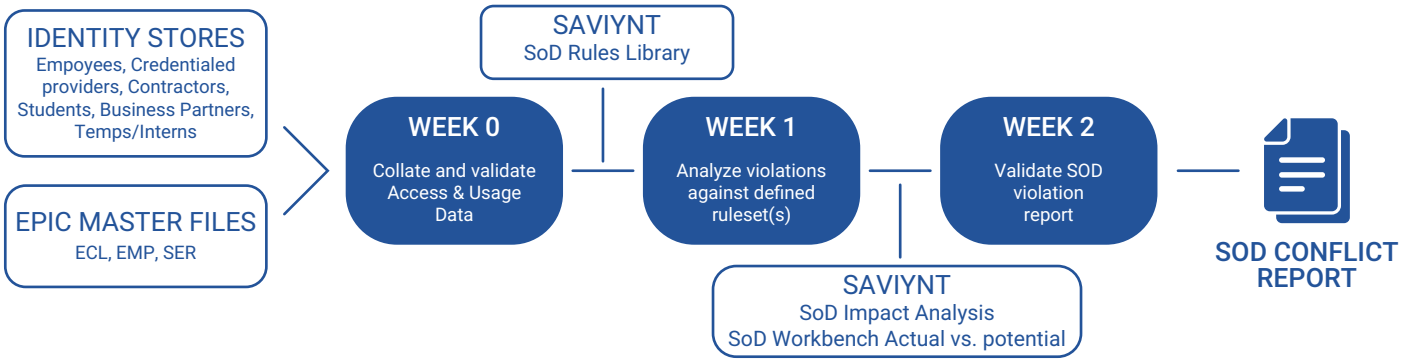
The first step in comprehensive SOD management is identifying the various user access permissions that are causing SOD violations. Saviynt provides a platform that accelerates the analysis of the current state of SOD conflicts within various functions of the healthcare revenue cycle; it is cased on the based on a pre-built controls library. The library has over 170 controls and has the ability to be extended and customized based on enterprise preferences. Saviynt has connectors for Epic and other EMR and HR platforms such as Cerner, McKesson, Meditech, Workday, PeopleSoft, SAP HR, etc. to further automate the extraction of access and usage information as part of the analysis.

2. REMEDIATE SOD VIOLATIONS:

Once existing SOD violations are verified with business and platform owners, next step is to remediate them using several techniques:

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

AUTOMATED SOD ANALYSIS APPROACH:



The SOD remediation process, as listed above, can easily become cumbersome and relies on close coordination between various teams. Saviynt has an integrated and intelligent SOD Workbench for automated remediation. The workbench offers the following capabilities and benefits:

- Automatic recommendations on inherent security class and template SOD violation remediation – doing this first enables to reduce violations counts drastically
- Automatic recommendations to remediate user to conflicting template(s)/function(s)
- Advanced simulation of access remediation enables business to assess impact and take intelligent decisions
- Analyzes usage logs to identify if existing SOD were exploited (un)/knowingly by users – a powerful tool for prioritizing SOD review and/or detect fraud
- Mitigating control management allows assignment of oversight and ownership to individuals
- Time-bound mitigating controls enforces continuous review

3. PREVENTIVE SOD CONTROLS:

After remediating existing violations, it is crucial to maintain a SOD free environment. One of the ways to ensure this on a continual basis is the integration of preventive SOD validation during access request. Saviynt's Intelligent Access Request System not only automates appropriate approvals, but it also identifies increased risk or potential SOD violations in real-time if the request is approved. This allows the approver to take an informed decision on approving the request and also assign compensating control as necessary.

Another way to ensure a SOD free environment is during (sub-)/ template design. Saviynt Access Protect module incorporates SOD simulation during template/security class definition/change. This provides the designer with the capability to stem the proliferation of potential SOD violations in the environment.

In conclusion, a well-designed SOD management framework is a powerful tool for healthcare organizations to avoid potential fraudulent acts and ensure adherence to various compliance and privacy mandates.

Saviynt USA / Headquarters, 5777 W Century Blvd
Suite 370, Los Angeles, California 90045, USA

info@saviynt.com
sales@saviynt.com

310-641-1664