

Closing the Access Governance Gap in Epic Environments

Why SoD and access risk stay hidden in EHR systems – and how continuous governance closes the gap

The Access Governance Blind Spot

- ▶ SoD risk is rarely labeled as SoD risk – audit findings show up as “access control deficiencies,” not the SOX-style language common in ERP audits.
- ▶ Clinical access monitoring runs outside the EHR itself, through separate privacy-surveillance tools layered on top of Epic.
- ▶ Access lives in silos – a person’s Epic access is invisible to SAP, Workday, or any other platform they touch, and vice versa.

Where Native Epic Security Stops

- Epic’s Security Class and Profile model governs access exceptionally well – within Epic. Two structural gaps follow directly from that scope:
- ▶ User (EMP) and Provider (SER) are separate records for the same person; security classes need dedicated Epic-certified analysts, and lagging updates create drift windows.
 - ▶ No native mechanism sees conflicts that span systems, and access reviews happen only when someone looks – not continuously.

What Audits Are Already Finding

\$2.2M

in unassigned credit balance work queues across 52,202 accounts, surfaced in an academic health system’s revenue cycle audit – which drove management action on SoD for security access and payment handling.

Source: UT System internal audit report

5

access control deficiencies found in a federal healthcare system information security inspection, including unmanaged privileged accounts and unreviewed database audit logs.

Source: VA Office of Inspector General information security inspection

4

internet-facing web applications found with authentication and validation gaps in a large hospital’s HHS OIG cybersecurity audit.

Source: HHS Office of Inspector General hospital cybersecurity audit.

How Saviynt AAG Closes the Gap

AAG capability	What it delivers
Cross-application SoD analysis	Extends SoD rules across Epic, SAP, Workday, and every connected system – catching conflicts no single platform can see alone.
Continuous access certification	Automated, ongoing certification replaces manual point-in-time reviews, surfacing risk before an auditor has to find it.
Joiner / mover / leaver automation	Ties provisioning and deprovisioning to HR events, closing the window where transferred or terminated staff keep stale access.
Privileged & emergency access oversight	Monitors break-glass usage for pattern and justification quality, independent of the system being accessed.
Healthcare-tuned SoD risk library	Prebuilt SoD rulesets mapped to healthcare workflows – no dependency on deep in-house Epic security-class expertise.
Audit-ready reporting	A continuous, exportable evidence trail built for OIG, Joint Commission, and internal audit requests.