IATRIC® systems

Enhancing Health Care IT

Security Audit Manager™

Security Audit Manager
— a PATIENT PRIVACY SOLUTION

KLAS CATEGORY LEADER
PATIENT PRIVACY MONITORING
2018

**KLAS® Category Leader
Four Consecutive Years**

ONC Certified HIT
2015 EDITION

Protecting Patient Privacy and Building Trust Since 2003

Having your hospital's name splashed across the news because of a patient privacy breach could cost your hospital for years. You can attempt to manually monitor the thousands of daily accesses to patient data, or you can discover Iatric Systems Security Audit Manager™ (SAM). SAM provides you with one solution that handles all your patient privacy auditing and incident risk management. SAM is an integrated solution that can interface with any HIS as well as export to any system. Security Audit Manager...

- Receive alerts on potential threats thus reducing insider threats, identity theft, and tax fraud

- Provides at-a-glance management from its Executive Dashboard

- Reduces Patient Privacy Breaches with automated rules that find inappropriate behavior

- Safeguard patient trust by protecting your patients' Protected Health Information no matter where it resides

- Integrates Breach Notification Risk Assessment

MUST-HAVE technology that can protect your hospital from financial penalties and damage to your reputation.

Thousands of times a day, employees access your hospital's patient data. Security Audit Manager is an advanced application that automatically monitors audit logs across your entire enterprise, sees every access, and identifies potential privacy breaches 24/7. It performs the auditing task that requires too many resources to do manually and delivers these capabilities:

- **Monitors, identifies, and alerts on potential privacy violations.** Proactively audits all access to patient records and quickly spots inappropriate activity.

- **Provides at-a-glance management from its Executive Dashboard.** Displays graphic representation of your privacy compliance program, delivering quick, real-time reporting and alerts to possible violations.

- **Correlates audit logs from any HIS.** Save time and effort with a system that automatically aggregates audit logs from across your entire enterprise, provides precise information, and alerts about events as they occur.

- **Integrates Breach Notification Risk Assessment.** Provides a pre-built, out-of-the-box solution using best-practices content and workflow. Customizable to meet your unique breach risk assessment criteria and process.

- **Advanced behavioral reporting.** Finds inappropriate behavior through pre-built reports showing changes in activity/volumes from normal, established (baseline) levels.

- **Risk-based analysis.** Auditor's Desktop, as a companion to Security Audit Manager, is the next generation solution for protecting patient privacy. By using advanced analytics, Auditor's Desktop significantly reduces the false positives, tracks user/patient audit history, and prioritizes the most probable cases of inappropriate access so you know what to focus on.

Key Advantages Include:

Security Audit Manager is certified for 2014 ONC HIT Meaningful Use. Hospitals can now stop struggling with manual audits and be confident that your organization is doing everything possible to mitigate risk and protect patient privacy. SAM is certified for Meaningful Use so Hospitals and Eligible Providers can receive ARRA dollars when you protect patient privacy.

- Proactively monitors application access 24/7

- Designed to facilitate the entire lifecycle of a potential privacy breach, from the data collection, the initial analysis, the requisite breach risk assessment, and incident response management

- Compiles audit trails from diverse software applications for a truly enterprise-wide solution

- Includes a full library of turnkey, customizable audit reports

- At-a-glance reporting of your privacy compliance program with the Executive Dashboard

- Analyze millions of records daily on an enterprise database that can be deployed on-premise or on the cloud

For more information on **Security Audit Manager**, or any other Iatric Systems products or services, please contact us using the information below.

Additional required software may include: OS, database, backup, virus protection, digital certificate, and HIS/EMR software. Additional Types of Costs may include: server and storage hardware, Microsoft licensing (OS, database, etc.), 3rd party licensing (digital certificates, backups, virus protection, etc.), and 3rd party interface/integration. For additional information please visit https://new.iatric.com/security-audit-manager-product-certification or contact Iatric Systems for more information.

Security Audit Manager, version 5.1, has been certified on April 3, 2013 as an EHR Module, for both an Hospital, certification number CC-2014-290560-1, and Eligible Provider, certification number CC-2014-290560-2. This EHR module is ONC 2014 Edition compliant and has been certified by the Certification Commission for Health Information Technology (CCHIT®), an ONC-ACB, in accordance with the applicable certification criteria adopted by the Secretary of Health and Human Services. This certification does not represent an endorsement by the U.S. Department of Health and Human Services. Security Audit Manager, version 5.1, meets the following certification criteria: 170.314(d)(1) Authentication, access control, and authorization; 170.314(d)(3) Audit report(s); 170.314(g)(4) Quality management system; and 170.314(d)(5) Automatic log off. The additional types of costs that an Eligible Provider or Hospital would pay to implement Security Audit Manager 5.1 in order to attempt to meet meaningful use objectives and measures include: MS-SQL licensing if required, data storage, initial hardware investment.

ONC CERTIFIED HIT® is a registered trademark of HHS.