IATRIC systems

Enhancing Health Care IT

Security Audit Manager™

Justifying the Cost of a Patient Privacy Monitoring Program

When Protected Health Information (PHI) is accessed inappropriately, it's a violation of the trust that patients place in their healthcare providers. Hospitals that experience a privacy breach can be subject to a huge financial hit — in fines, litigation costs, and lost revenue as patients stay away or look elsewhere for their care.

Security Audit Manager™ protects sensitive patient information while protecting the hospital from the costs of a breach. It's designed for today's strict HIPAA and HITECH rules, with technology that proactively audits all accesses of PHI across the organization, detects inappropriate behavior, and documents breach investigations automatically. It's so easy to use, and so cost-effective, that protecting PHI and complying with regulations is not only within reach, it's also good business.

This brochure examines ways to cost justify your patient privacy monitoring program. It steps you through the:

- Steep costs you will avoid by preventing a breach
- Efficiencies and day-to-day time savings for security staff, which is burdened with many other pressing tasks
- Ways breaches affect quality scores and how you could incur a reduction in Hospital Consumer Assessment of Healthcare Providers and Systems (HCAHPS) scores
- Financial savings that result from a 75% reduction in inappropriate access

KLAS CATEGORY LEADER 2015/2016

ONC Certified HIT 2014 EDITION

Justifying the Cost of a Patient Privacy Monitoring Program

Many healthcare organizations realize that they need to implement a privacy privacy monitoring and breach detection program. But they haven't been successful in finding ways to justify the cost of the software. Our customers have shared with us ways to show how costs for data breaches can be avioded and how Security Audit Manager has improved the overall process and efficiencies by decreasing inappriopriate access.

Avoiding the Costs of Data Breaches

According to the *2014 Cost of Data Breach Study: Global Analysis from Ponemon Institute*, the average cost of a data breach to a healthcare organization was $3.5 million in U.S. dollars — 15% more than in 2013. Data breach costs to healthcare organizations include fines, lost revenues, litigation costs, lower quality scores, and the cost of failing an OCR audit. A breakdown of some of these costs is provided below. (These costs don't include the human toll and impact on careers.)

Fines

The majority of fines for a data breach are outlined by the the American Recovery and Reinvestment Act (ARRA) of 2009, which established a tiered civil penalty structure for HIPAA and data breach violations. These fines include:

- Four categories of violations that reflect increasing levels of culpability (see the table below)
- Four corresponding tiers of penalties that significantly increase the minimum penalty amount for each violation
- A maximum penalty amount of $1.5 million for all violations of an identical provision

Civil Monetary Penalties for HIPAA Violations	
Violation Tier	**Penalty**
1. The covered entity or individual did not know (and by exercising reasonable diligence would not have known) the act was a HIPAA violation.	$100 - $50,000 for each violation, up to a maximum of $1.5 million for identical provisions during a calendar year
2. The HIPAA violation had a reasonable cause and was not due to willful neglect.	$1,000 - $50,000 for each violation, up to a maximum of $1.5 million for identical provisions during a calendar year
3. The HIPAA violation was due to willful neglect, but the violation was corrected within the required time period.	$10,000 - $50,000 for each violation, up to a maximum of $1.5 million for identical provisions during a calendar year
4. The HIPAA violation was due to willful neglect and was not corrected.	$50,000 or more for each violation, up to a maximum of $1.5 million for identical provisions during a calendar year

The bottom line is that HIPAA fines are not going away, and fines have increased over time. Violations can cost the healthcare organization up to $1.5M in a calendar year.

Justifying the Cost of a Patient Privacy Monitoring Program

Lost Revenue — 65% of Patients Would Leave the Hospital

The TransUnion Healthcare Data Breach Survey of 2015 revealed that nearly 7 out of 10 patients (65%) would avoid healthcare providers that experienced a data breach.

Lawsuits Due to Violation of Patient Trust

In addition to fines, penalties, and lost revenue, a PHI security breach can cost millions in settlement and litigation costs, as well as higher insurance premiums. Even if a hospital only faces one lawsuit every few years, the annual prorated costs can amount to hundreds of thousands of dollars.

Costs Associated with Quality Issues

- Patients say if the facility had experienced a breach, they would be less likely to share with their caregiver health information that the caregiver might need to provide proper care.
- Quality issues and higher 30-day readmissions could mean that hospitals could receive penalties — up to 2% of Value Based Payments (VBPs), and up to 3% hospital readmission penalties.
- Hospital Consumer Assessment of Healthcare Providers and Systems (HCAHPS) scores are very important to hospitals. High scores mean more new patients and higher reimbursements. Hospitals that experience a breach will receive lower HCAHPS scores, which means fewer new patients and lower reimbursements.

OCR Audits and Enforcement

After nearly a two-year delay, the Department of Health and Human Services' Office of Civil Rights has begun OCR HIPAA audits of healthcare organizations and their business associates. OCR is doing a good thing by making us "Eat our Vegetables." The OCR HIPAA audits are critical to protecting patients' health information, and most healthcare professionals do not take the audits seriously because of the poor state of cybersecurity in healthcare. Patient trust should be used as a competitive advantage. Good performance in an audit can become a marketing tool for healthcare organizations.

Process and Efficiency Improvements Using Security Audit Manager

As a comprehensive, automated solution for monitoring PHI access and complying with regulations, Security Audit Manager saves time daily for staff responsible for protecting patient information. It allows you to automate critical privacy monitoring tasks that you could never accomplish manually.

Greatly Reduces Inappropriate Access to Patient Records

Hospitals report that after using Security Audit Manager, they see a dramatic decrease in inappropriate access, as well as major process improvements in how access events are monitored, tracked, and reported.

"Combined with employee education, Security Audit Manager has resulted in a 75% decrease in inappropriate access to patient records. Security Audit Manager automates the auditing process, and saves staff time in other ways, too. In the past, nurses were restricted to patient records by location. Every time a nurse needed to complete documentation after the patient had been moved to another location, we had to temporarily un-restrict access for the user, and then remember to lock it down again afterward. With Security Audit Manager in place, nurses no longer need to be restricted to patient records by location."

Clinical Informatics Analyst
Campbell County

Justifying the Cost of a Patient Privacy Monitoring Program

Protects PHI Enterprise-wide

Security Audit Manager proactively monitors audit logs across your entire enterprise, sees every access, and identifies potential privacy breaches 24/7.

"Security Audit Manager brings together audit trails from many disparate systems to give us a complete view of how people are looking at our data. It is allowing us to have a view into applications that we wouldn't normally audit due to time and resource constraints."

AVP and Assistant Chief Information Officer
West Virginia United Health Care

Helps Hospitals Respond to a CMS Audit and Keep Meaningful Use Dollars

Not passing a Meaningful Use audit means having to give back the money received in incentive payments. The Security Risk Assessment is a Meaningful Use Objective, and our customers have told us that when facing a CMS audit, Security Audit Manager has helped them pass the audit. In the event of an audit, hospital staff can easily assemble the information requested in a fraction of the time needed compared to locating the information manually.

Security Audit Manager in Action

Security Audit Manager is an advanced application that automatically monitors and correlates audit logs across your entire enterprise, sees every access, and identifies and ranks potential privacy breaches 24/7. It automates auditing tasks that could never be accomplished manually and delivers these capabilities:

- Monitors application access 24/7
- Proactively identifies and alerts on potential privacy violations
- Analyzes potential privacy violations and ranks them by severity, thus increasing productivity and reducing patient privacy risks
- Manages the entire lifecycle of a potential breach, from data collection through initial analysis, risk assessment, and response management
- Compiles audit trails from diverse software applications for a truly enterprise-wide view of PHI access
- Includes a full library of turnkey, customizable audit reports
- At-a-glance visibility and reporting from the Executive Dashboard
- Ability to analyze millions of records daily
- Certified for 2014 HIT Meaningful Use

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

IATRIC systems

Ph: 978.805.4100 Fax: 978.805.4101 info@iatric.com security.iatric.com