Security Audit Manager™ Checklist

Evaluate the technology needed for effective and compliant patient privacy monitoring.

Compliments of

IATRIC systems

Patient Privacy Monitoring Technology Checklist

Having your healthcare organization's name splashed across the news because of a patient privacy breach could cost your hospital for years. You can manually monitor the thousands of daily accesses to patient data — or you can automate it with Iatric Systems Security Audit Manager™.

This single solution for patient privacy auditing and incident risk management automates what is impossible to do manually. It monitors audit logs across your entire enterprise, sees every access, and identifies potential HIPAA privacy breaches 24/7.

When you are evaluating technology to build a successful patient privacy monitoring program, use this checklist to make sure the solution you select offers these critical capabilities:

Technology needed to fully protect patient privacy.	Security Audit Manager	Other	Other
1. Centrally monitor all access to patient records. The solution should automatically aggregate audit logs from across the entire organization and provide single search queries and proactive auditing. This requires a solution that incorporates data integration to all applications that contain PHI, such as HIS, PACs, LAB, and Radiology. Integrating this data into one place should not be the hospital staff's responsibility.	✓		
2. Monitor, identify, and send alerts on potential privacy violations. It is important to proactively audit all accesses to patient records and spot inappropriate activity as it happens. This type of monitoring reduces violations, helps prevent recurring breaches, and allows you to document and share audit findings with your security team for quick resolution.	✓		
3. Track incidents and end-user workflow. The solution should be designed to facilitate the entire lifecycle of a potential privacy breach — from the data collection, the initial analysis, the requisite breach risk assessment, and the incident response management.	✓		
4. Audit and manage massive volumes of patient access records. Imagine that, on a daily basis, a 100-bed facility has an average of 52,000 patient access records. Manually monitoring and reviewing these accesses every day to find which ones are inappropriate is clearly unfeasible. Correlating this data using an enterprise database, and using virtualization to manage the massive amounts of data is essential.	✓		

5. Generate reports per state and federal guidelines. Healthcare organizations are required to report breaches. The solution should have a comprehensive, centralized environment to review documented findings and provide insight into areas requiring additional security measures and/or employee education.	✓		
6. Audit the release of medical records. With so many ways that a HIPAA violation can occur when releasing medical records, it is important that the solution document and track their release.	✓		
7. Document and account for all disclosures. The HITECH rule requires all hospitals and business associates to account for all electronic disclosures of patient health information. In addition, the accounting must produce disclosures made for three years prior to the date of the request. The accounting requirement applies only to disclosures and not to uses (which are understood to be within the covered entity). This process should be tracked and documented in a central repository.	✓		
8. Meet Meaningful Use patient privacy requirements. Under the HIPAA Security Rule, hospitals are required to implement policies and procedures to prevent, detect, contain, and correct security violations under HIPAA 45 CFR 164.308(a)(1). It is important that your solution is 2014 ONC HIT certified so when you protect patient privacy, ARRA dollars can be received.	✓		
9. Manage patient privacy from an at-a-glance Executive Dashboard. The solution should display a graphic representation of your privacy compliance program, delivering quick, real-time reporting and alerts to possible violations.	✓		
10. Prevent fraud with pre-built Medical Identity Theft reports. Ponemon Institute's study on Medical Identity Theft estimates an average of two million Americans are victims of medical identity theft yearly, with an estimated total cost to U.S. healthcare organizations of $41 billion. It is vital that your solution proactively analyze and send alerts when these violations occur.	✓		

Iatric Systems Security Audit Manager was built to help you eliminate the severe financial penalties and harm to your healthcare organization's reputation that can occur due to a patient privacy breach.

Start now.
For personal assistance developing your own organization's patient privacy strategy — contact Iatric Systems today.

978-805-4100
info@iatric.com

IATRIC systems

Iatric Systems, Inc.
27 Great Pond Drive
Boxford, MA 01921