10 Reasons Security Audit Manager is a MUST for Your Hospital

Security Audit Manager is an innovative software solution that transforms your hospital's efforts to meet the rules of the 2009 HITECH Act, helps achieve Stage 1 Meaningful Use criteria and proactively audits patient record security. Here are ten reasons that it's a MUST for your hospital.

1. **Protect your hospital's reputation**. Patients have a choice of which hospital to use. They don't choose the one featured on the 10 o'clock news for breaching patient privacy. If patients can't trust your ability to keep their health information private, they won't trust your ability to take care of their medical needs. Security Audit Manager helps your hospital be the one in your community that patients trust most and turn to with confidence.
2. **Stay compliant**. Security Audit Manager was designed specifically to help hospitals meet the many legislative requirements, including the 2009 HITECH Act and other state and federal rulings addressing patient data privacy.
3. **Centralize monitoring of employee access to patient records**. Save time and effort with a system that automatically aggregates audit logs from across the entire enterprise and provides single search queries and pro-active audit reports.
4. **Automate a function that cannot be performed manually**. Auditing takes so many resources and so much time it's impossible to do manually. Here's just one example for a 100-bed facility.
   - On an average day a typical audit file generates 73,000 rows.
   - 52,000 of those rows are patient access audits.
   - If one auditor spends five seconds per audit, reviewing 100% of the records, it would take 73 hours.
   - If one auditor spends five seconds per audit, reviewing 10% of the records, it would take 7.3 hours.
   - Even if one auditor spends a more reasonable 30 seconds per audit, reviewing 10% of the records, it would take 43.83 hours.
5. **Catch and resolve single and recurring breaches in real time**. Pro-actively audit all access to patient records and spot inappropriate activity as it happens. This comprehensive monitoring reduces violations, helps prevent recurring breaches, and allows you to document and share audit findings with your security team for quick resolution.
6. **Document breach investigations and resolutions**. As required by the 2009 HITECH Act, Security Audit Manager's comprehensive monitoring provides the information you need to properly document investigations and resolutions and fulfill notification requirements.
7. **Simplify efforts to meet reporting requirements**. Hospitals are required to report breaches. Security Audit Manager provides all the information you need to comply with this ruling. The comprehensive compliance reports allow you to review your documented findings, providing insight to the areas you need to address with additional security measures and/or targeted employee education sessions.
8. **Motivate hospital employees to honor patient privacy rules**. Because Security Audit Manager is reviewing data for you, you can better educate employees and make them aware that their access activities are monitored, preventing the potential for inappropriate access.
9. **Help meet Meaningful Use criteria**. Security Audit Manager actively monitors usage within your EMR system to help your facility meet the security risk analysis requirements under 45 CFR164.308 (a)(1).
10. **Protect your hospital's bottom line**. Security Audit Manager delivers a more efficient use of staff time and reduces the chance that your hospital could incur penalties of up to $1.5 million.

Start achieving these 10 essentials today.

For more information on **Security Audit Manager** please contact us using the information below.