

Security Audit Manager[™] Privacy Analytics and Filtering







Reduce Audits by 95% and Review Remaining in Ranked Order

With the introduction of HIPAA and HITECH, there is an increased need to identify, analyze, and monitor all information systems that contain Protected Health Information. Since 2003, Security Audit Manager™ has been protecting patient privacy and was awarded the leader in patient privacy monitoring for the last four years by KLAS.

Security Audit Manager functionality extends beyond automated monitoring with analytics and filtering capabilities to accurately identify inappropriate access. Using a combination of three methods, Security Audit Manager quickly narrows down the scope of audits, reducing audits by 95%. These remaining audits are then ranked and weighted, so the audits with the highest probability of inappropriate behavior are the ones that are reviewed.



Filters out false positives using appropriate access



Filters out known routines, users, and devices



Ranks by likelihood using privacy analytics

Security Audit Manager[™] Privacy Analytics and Filtering











At Iatric Systems, our patient privacy development team is continually investing in advanced technology to increase user productivity, automate workflow, filter out false positives, and streamline investigations with machine-learning algorithms.

The combination of these methods dynamically reduces your audits, allowing privacy auditors to review only those audits with the highest likelihood of suspicious activities, and effortlessly make quick audit determinations.

Filters out false positives using appropriate access



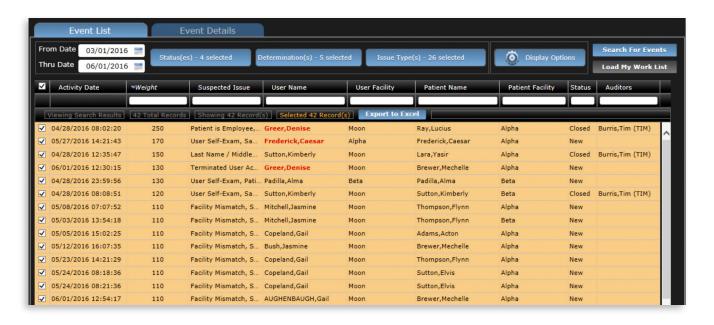
Security Audit Manager™ quickly identifies audits that are clinically justified and marks them as "Appropriate." It detects appropriate audits by analyzing a combination of user and patient information. Examples of appropriate audits include a clinician administering medication, entering a note, or documenting patient status. Security Audit Manager will then automatically update the audits in the database that match the criteria as "Appropriate" so that you can filter those audits from appearing on reports.

Filters out known routines, users, and devices

Security Audit Manager allows the auditor to use filtering to exclude known routines such as batch jobs or status board displays. You can also filter specific events to see instances where a user may have only viewed, printed, or even downloaded a patient record.

Ranks by likelihood using privacy analytics

Security Audit Manager uses analytics to find the most probable privacy violations using 30 algorithms that apply weights to the audits, and then ranks by severity. This ensures that the most likely cases of inappropriate access rise to the top.



To learn more about **Security Audit Manager** or other Iatric Systems products or services, please contact us using the information below.

Ph: 978-805-4100 Fax: 978-805-4101 <u>info@iatric.com</u> <u>iatric.com</u> (1/18)