EventTracker
Actionable Security Intelligence

HIPAA Solution Brief

HIPAA

EventTracker | 8815 Centre Park Drive, Columbia MD 21045

About EventTracker

EventTracker delivers business critical software and services that transform high-volume cryptic log data into actionable, prioritized intelligence that will fundamentally change your perception of the utility, value and organizational potential inherent in IT audit and event log files. EventTracker's award winning solutions provide capabilities to implement Security Information and Event Management (SIEM), Log Management, and real-time Threat Intelligence to help optimize IT operations, detect and deter costly security breaches, and comply with multiple regulatory mandates.

EventTracker software is designed to be implemented for organizations with 25 to 25,000 assets such as servers, firewalls, other network and security devices, workstations, applications. SIEMphonic managed services are right-sized to assist you with system administration, incident analysis and compliance activities through "self- half- or full-service" options.

HIPAA Compliance Overview

http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html

> §164.308(a)(1)(ii)(D): **Security Management Process** – Implement procedures to regularly review records of information system activity, such as ***audit logs, access reports, and security incident tracking reports.***

HHS issued HIPAA privacy requirements compel the regular organization-wide review of specified system audit logs by designated IT and security personnel. These organizations include health insurers, HMO's, managed service providers, clearing houses, benefits managers, claims processors, medical bill collection agencies, law firms practicing in the health care industry and of course health care providers, health systems, clinical laboratories and others. Compliance with HIPAA involves the management, use and sharing of medical and personal information of a particular identifiable individual. HIPAA requires health care providers and industry associates to ***develop and follow procedures that ensure the confidentiality and security of Protected Health Information (PHI),*** when it is transferred, received, shared or stored. This applies to all forms of PHI including paper, oral and electronic. And only ***the minimum required health information*** for conducting business is to be shared and used.

http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html

> §164.308(a)(6): **Security Incident Procedures** (§164.308(a)(6)(ii)) – Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.

You must monitor and review logs and access reports for this covered information and information exchange in real-time, or as soon thereafter as is practicable to avoid privacy breaches and placing your organization at risk of failing a HIPAA audit. You must also document your policies, identify and train responsible personnel and ***provide evidence of incident and log review procedures on an on-going basis.***

Audits usually are stressful, expensive and time consuming. However, you should also consider that audits serve to confirm that your HIPAA compliance activities are both understood and practiced by your organization

on a regular basis. This is good, and can help make you a safer operation – so auditor input should be viewed as "constructive criticism". Auditors do have wide discretion to determine what constitutes compliance or non-compliance and the relative severity/intent therein. By demonstrating that your organization is aware of the requirements and is serious about your operational commitment by being "audit-ready all the time" you are more likely to receive corrective guidance coming out of an audit as opposed to punitive action.

EventTracker streamlines both the ***real-time security incident detection*** and the ***compliance report review processes.*** By providing "single-click" issue flagging and report annotation on-the-fly, HIPAA audit-ready summaries are available on demand in EventTracker to help minimize the stress, foreboding and hours/days of tedious preparation often associated with HIPAA audits.

EventTracker Provides a Full View of the Entire IT Infrastructure

EventTracker improves security, helps organizations demonstrate compliance and increases operational efficiencies. EventTracker enables your organization to be more aware of potential security risks and internal/external threats. It provides you with the ability to respond to a security incident with comprehensive data and forensic tools for analysis. The time required to investigate and mitigate security incidents can be greatly reduced minimizing the potential exposure and costs.

SIEMphonic is our managed services offerings to enhance the value of EventTracker implementations. Our expert staff can assume responsibility for some or all EventTracker SIEM related tasks including system management, incident reviews, daily/weekly log reviews, configuration assessments, HIPAA audit reports annotation, and audit support. We augment your IT Security team, allowing you to focus on your priorities by leveraging our expertise, discipline and efficiency.

Scalable, Log Collection and Processing with Notifications based on Criticality

EventTracker provides automatic consolidation of thousands or even millions of audit events to meet the needs of any size organization. The inbound log data is identified by the EventTracker built-in manufacturers Knowledge Base which contains log definitions for thousands of types of log events, and ***automatically identifies which events are critical to security and HIPAA compliance.***

EventTracker provides real-time and batch aggregation of all system, event and audit logs from your firewalls, IDS/IPS, network devices, windows, linux/unix, VMWAre ESX, Citrix, databases, MS Exchange web servers, EHRs and more.

Ease of Deployment and Scalability

EventTracker is available on premise or as a highly scalable cloud-based SIEM and Log Management solution that offers several deployment options to meet the needs of organizations with a few dozen systems or those with thousands of systems spread across multiple locations. EventTracker Cloud is available as an AMI on Amazon EC2, Microsoft Azure or your cloud infrastructure provider of choice. It supports multi-tenant implementations for health care MSSP organizations serving the needs of smaller customers.

For more information on EventTracker and SIEMphonic visit www.eventtracker.com

EventTracker Statement of Compliance for HIPAA

Administrative Safeguards:

HIPAA Control Requirements	EventTracker Solution	EventTracker Reports	EventTracker Alerts
Section: 164.308(a) (1) (i) Security management process. Implement policies and procedures to prevent, detect, contain, and correct security violations.	Fully featured auditing of access, changes, and configuration of all systems creating, receiving, maintaining, and transmitting ePHI and recording of who changed what, when, and where, ensures HIPAA compliance. Centralized consolidation and archival or audit trials, using predefined and custom-built reports covering all major types of activities across the entire IT infrastructure.	Yes	Yes
Section: 164.308(a) (1) (ii) (D) Information system activity review: Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	Extensive auditing and reporting on both administrative and user activity in Active Directory, Group Policy, Exchange, the file servers, virtual environments (VMware, Microsoft), SQL Servers. Detection of who did what, when, and where with advanced rollback capabilities of unauthorized actions. Centralized consolidation and archival or audit trials with web-based reporting using predefined and custom-built reports covering all major types of activities: logins, logoffs, user account operations, file access on servers, workstations, both successful and the failed ones.	Yes	Yes
Section: 164.308(a) (3) (ii) (C) Termination procedures: Implement procedures for terminating access to electronic protected health information when the employment of workforce member ends.	Auditing of disabled accounts, automated de-provisioning of inactive user accounts. Create report of all disable account.	Yes	Yes
Section: 164.308(a) (4) (i) Information access management. Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.	Auditing of files, folders and their permissions across the entire IT infrastructure for early detection of unauthorized changes to security access settings (e.g. granting of new permissions, changes of user access rights, etc.) and ensure adequacy of technical controls.	Yes	Yes
Section: 164.308(a) (4) (ii) (A) Isolating health care clearinghouse functions: If a healthcare clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.	Complete auditing and automated change documentation for all types of access rights, privileges, and policies that control access to workstations, programs, transactions, and other systems to detect violations of HIPAA compliance security measures.	Yes	Yes
Section: 164.308(a) (4) (ii) (C) Access establishment and modification: Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.	Complete auditing and automated change documentation for all types of access rights, privileges, and policies that control access to workstations, programs, transactions, and other systems to detect violations of HIPAA compliance security measures.	Yes	Yes

HIPAA Control Requirements	EventTracker Solution	EventTracker Reports	EventTracker Alerts
Section: 164.308(a) (5) (ii) (C) Log-in Monitoring: Procedures for monitoring log-in attempts and reporting discrepancies.	Centralized consolidation and easy to use reporting of all successful and failed logon/logoff activities with extensive filtering capabilities.	Yes	Yes
Section: 164.308(a) (5) (ii) (D) Password Management: Procedures for creating, changing, and safeguarding passwords.	Auditing of all password changes. Self-service password management for end users with customizable password security settings and secure access based on user identity verification. Prevention of excessive help desk calls related to secure password policies.	Yes	Yes
Section: 164.308(a) (6) (i) Security incident procedures. Implement policies and procedures to address security incidents.	As a part of internal control implement procedure to regularly review audit trails to identify and mitigate security incidents as they occur.	Yes	Yes
Section: 164.308(a) (6) (ii) Response and Reporting: Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.	Auditing of all administrative and user activities with configurable alerts and reporting that documents all security incidents and helps with early detection and prevention of further security incidents.	Yes	Yes
Section: 164.308(a) (7) (ii) (B) Disaster recovery plan: Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence.	Investigate audit trail with changes including before/ after values for immediate data recovery. Quick rollback of unauthorized and accidental changes to Active Directory objects, including restoration of deleted objects.	Yes	Yes

Technical Safeguards:

HIPAA Control Requirements	EventTracker Solution	EventTracker Reports	EventTracker Alerts
Section: 164.312(a) (2) (i) Unique user identification. Assign a unique name and/or number for identifying and tracking user identity.	Complete auditing of user accounts and logons to analyze violations and prevent usage of the same ID by multiple persons (e.g. from different computers) Compare audit trail with HR records to validate HIPAA compliance.	Yes	Yes
Section: 164.312 (b) Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	Auditing, archiving, and reporting of access and modifications within systems containing PHI.	Yes	Yes
Section: 164.312(d) Person or entity authentication. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.	Auditing logon activities of implemented within the organization two-tiered authentication system. Additionally users can be verified by Challenge/response system to confirm their identity when they change their passwords.	Yes	Yes

Policies, Procedures and Documentation Requirements:

HIPAA Control Requirements	EventTracker Solution	EventTracker Reports	EventTracker Alerts
Section: 164.316(b) (1) (ii) If an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.	Configurations states and complete audit trail of access and changes, including who, when, where, what with before and after values. Consolidated within two-tiered (file-based and SQL database) storage solution, holding data for up to 10 years or more, with built-in archiving and reporting capabilities. Streamline HIPAA compliance with scheduled reports and real-time alerts.	Yes	Yes
Section: 164.316(b) (2) (i) Time limit. Retain the documentation required by paragraph (b) (1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.	Configurations states and complete audit trail of access and changes, including who, when, where, what with before and after values. Consolidated within two-tiered (file-based and SQL database) storage solution, holding data for up to 10 years or more, with built-in archiving and reporting capabilities. Streamline HIPAA compliance with scheduled reports and real-time alerts.	Yes	Yes
Section: 164.316(b) (2) (ii) Availability. Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.	Configurations states and complete audit trail of access and changes, including who, when, where, what with before and after values. Consolidated within two-tiered (file-based and SQL database) storage solution, holding data for up to 10 years or more, with built-in archiving and reporting capabilities. Streamline HIPAA compliance with scheduled reports and real-time alerts.	Yes	Yes

References:

http://www.hipaasurvivalguide.com/hipaa-regulations/hipaa-regulations.php

http://www.hipaasurvivalguide.com/hipaa-regulations/164-308.php

http://www.hipaasurvivalguide.com/hipaa-regulations/164-310.php

http://www.hipaasurvivalguide.com/hipaa-regulations/164-312.php