CIMCOR

SOLUTION BRIEF

Meeting HIPAA Requirements with CimTrak

AT A GLANCE

» **COMPLETE AUDIT TRAILS**
Be able to track changes in real-time and have complete documentation and evidence as to the integrity of those changes.

» **FORENSIC DETAIL OF CHANGES**
Know who made the change, when the change was made, how it changed and what process was used is critical to the triage process of incident response.

» **CONTINUITY OF OPERATIONS**
CimTrak provides the ability to roll-back and restore changes manually or automatically, keeping your critical information secure, available and accessible.

» **DISASTER RECOVERY**
CimTrak enables you to take "snapshots" of your files and configurations as change occurs and is reconciled giving an organization the ability to deploy a previous snapshot at any time.

» **COMPLETE REPORTING**
CimTrak provides a wide variety of reports on monitored systems as well as internal reporting on CimTrak users and activities.

CIMTRAK

HIPAA Requirements

Protecting and securing critical electronic health information is now more important than ever. Since the implementation of HITECH, and the Omnibus Final Rule of 2013, many of the questionable areas regarding breach standards have additional clarity, including increased scrutiny of covered entities as well as stiffer fines for violations. Ensuring the security and integrity of your IT environment is critical to maintaining HIPAA compliance.

Many tools can be implemented to assist you in becoming compliant with HIPAA but none of them compare to the features and functionality of CimTrak's comprehensive system integrity assurance framework. CimTrak's policy management capabilities enable an organization to meet the objective of HIPPA Security Rule part 164 and the integrity of your "electronic protected health information" (ePHI) on a continuous and on-going basis. CimTrak helps maintain the security and compliance of everything from servers, workstations, network devices, firewalls, container orchestration, hypervisors, cloud configurations, database schemas & configurations, active directory/LDAP, and more.

Audit Type – Security

Key Activity	Requirement	Established Performance Criteria	How CimTrak Helps
General Requirements	§164.306(a)	§164.306(a): Covered entities and business associates must do the following: (1)Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits. (2)Protect against any reasonably anticipated threats or hazards to the security or integrity of such information. (3)Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part; and (4) Ensure compliance with this subpart by its workforce.	CimTrak provides a System Integrity Assurance platform that ensures the integrity and security of the devices that handle PHI and provides the necessary evidence that the process and technologies are in place from a compliance perspective.

Key Activity	Requirement	Established Performance Criteria	How CimTrak Helps
Security Management Process	§164.308(a)	§164.308(a): A covered entity or business associate must in accordance with 164.306: (1)(i) Implement policies and procedures to prevent, detect, contain, and correct security violations.	CimTrak has the unique ability to identify, protect, detect, respond and recover from security incidents and violations by utilizing a fully integrated ticketing and workflow system to ensure the integrity and security of everything from servers, workstations, POS, network devices, container orchestration, hypervisors, cloud configurations, database schemas & configurations, active directory/LDAP, and more.

Key Activity	Requirement	Established Performance Criteria	How CimTrak Helps
Security Management Process – Risk Management	§164.308(a)(1)(ii)(B)	§164.308(a)(1)(ii)(B): Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306(a).	CimTrak's core value proposition is the reduction and elimination of IT security risk through a closed-loop change control process ensuring that only known, expected and authorized changes are being allowed to facilitated. This process is encompasses hardening, configuration management, change control, change reconciliation, roll-back and remediation, change preventing, file whitelisting, reputation services, STIX & TAXII feeds and ticketing system workflow.

Audit Type – Security (continued)

Key Activity	Requirement	Established Performance Criteria	How CimTrak Helps
Security Management Process – Information System Activity Review`	§164.308(a)(1)(ii)(D)	§164.308(a)(1)(ii)(D): Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	CimTrak enables the security management process of information activity and review in a clear and concise manner to highlight unknown, unauthorized and unexpected change to an infrastructure. If at any time change was unwanted, CimTrak can provide immediate notification and provide corrective action(s) and steps for roll-back and remediation. CimTrak also provides a compliance report that ensures the proper controls are not only in place but are operating as expected. If a compliance scan identifies a non-compliant system or device, evidence is immediately provided with steps on how to correct

Key Activity	Requirement	Established Performance Criteria	How CimTrak Helps
Security Awareness, Training, and Tools – Protection from Malicious Software	§164.308(a)(5)(ii)(B)	§164.308(a)(5)(ii)(B): Procedures for guarding against, detecting, and reporting malicious software.	CimTrak's ability to detect zero-day breaches extends well beyond just identifying malicious software. Its ability to identify, protect, detect, respond and recover from security incidents and violations is accomplished by creating a closed-loop workflow for change control of expected and authorized change. This process by default will highlight in real-time any change that was made by virtue of a circumvented process or one that was malicious in nature. CimTrak does incorporate the use of file reputation services as another data point to enforce system integrity assurance throughout the infrastructure.

Audit Type – Security (continued)

Key Activity	Requirement	Established Performance Criteria	How CimTrak Helps
Security Incident Procedures – Response and Reporting	§164.308(a)(6)(ii)	§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 or business associate; and document security incidents and their outcomes.	CimTrak's ability to detect security incidents and breaches in real-time is accomplished by the closed-loop process of change management. Establishing a trusted and hardened system by leveraging CIS Benchmarks and DISA STIGs facilitates a root of trust which is incorporated into the trusted baseline or configuration where integrity drift is then compared against in real-time over the entire life-cycle of operation. If unwanted change is identified, an immediate notification will be delivered to the appropriate individual(s) for response and resolution though a ticketing system where the applicable data and information if populated inside the ticket.

Key Activity	Requirement	Established Performance Criteria	How CimTrak Helps
Contingency Plan – Disaster Recovery Plan	§164.308(a)(7)(ii)(B)	§164.308(a)(7)(ii)(B): Establish (and implement as needed) procedures to restore any loss of data.	CimTrak is a key part of an organization's contingency plans. When a system goes down, being able to quickly recover and return to normal operations is absolutely critical, especially in the health care environment. With the ability to keep snapshots of files and configurations as they change, CimTrak has the ability to redeploy a previous snapshot at any time. This allows for quick recovery from a malicious threat or accidental mistake. What's more is that CimTrak can be configured to restore changes back instantly, thus effectively "self-healing" a system ensuring that operations are not disrupted. The CimTrak Master Repository, where files and configurations are compared for changes can be located offsite (or backed up offsite) in order to ensure the ability to recover files and configurations quickly in the event of a disaster.

Audit Type – Security (continued)

Key Activity	Requirement	Established Performance Criteria	How CimTrak Helps
Access Control	§164.312(a)(1)	§164.312(a)(1): Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).	CimTrak has a unique feature of preventing change, even if an individual has administrative privileges. This ability to prevent and grant access rights for change mitigates the risk of security breaches and incidents. With a full audit trail of who made the change, when the change was made, how it changed and what process was used enforces an organizations technical policies and procedures for electronic information systems that maintain electronic protected health information.

Key Activity	Requirement	Established Performance Criteria	How CimTrak Helps
Audit Controls	§164.312(b)	§164.312(b): Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	CimTrak provides a convenient way to track changes in your IT environment, giving you the ability to track any changes as well as provide detailed forensic detail on those changes. Additionally, CimTrak's internal logging tracks all users and administrator activity. All change and internal auditing information is stored securely within the CimTrak database and are not able to be deleted, effectively preventing an insider from covering up malicious activity.

Audit Type – Security (continued)

Key Activity	Requirement	Established Performance Criteria	How CimTrak Helps
Integrity	§164.312(c)(1)	§164.312(c)(1): Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.	When it comes to ensuring the integrity of your IT environment in order to protect critical medical information, CimTrak is simply unmatched by any other product. With the ability to protect against both internal and external threats, CimTrak differs from many other security tools that simply protect the network perimeter. CimTrak maintains systems in a known and trusted state by taking a digital snapshot of your files and configurations and then comparing them for changes. This method ensures that all changes are captured including threats that may bypass your existing network defenses such as those that are unsignatured. No other integrity and compliance tool can match these stringent safeguards to protect your information. Further, CimTrak was the first and is still the only integrity software that can immediately roll-back and remediate changes, thus effectively preventing changes that can cause a data breach or take your critical systems down.

Key Activity	Requirement	Established Performance Criteria	How CimTrak Helps
Integrity – Mechanism to Authenticate ePHI	§164.312(c)(2)	§164.312(c)(2): Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.	CimTrak's core value proposition is to provide integrity assurance and verification from a compliance perspective that nothing is altered or deleted in an unauthorized manner. If unauthorized change occurs, CimTrak and restore the necessary files, directories, configuration, etc...back to the last know trusted and correct state of operation.

Key Activity	Requirement	Established Performance Criteria	How CimTrak Helps
Transmission Security – Integrity Controls	§164.312(e)(2)(i)	§164.312(e)(2)(i): Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.	With a complete audit trail of all changes, an organization will know the moment a file is changed. With CimTrak, you can implement security measures ensuring electronic protected health information is not improperly modified.

Supported Platforms

CimTrak for Servers, Critical Workstations & POS Systems

WINDOWS: XP, Vista, 7, 8, 10, Embedded for Point of Service (WEPOS), POSReady, Windows 10 IoT Enterprise
WINDOWS SERVER: 2003, 2008, 2012, 2016, 2019
LINUX: Amazon, CentOS, ClearOS, Debian, Fedora, Oracle
SUN SOLARIS: x86, SPARC Red Hat, SUSE, Ubuntu, others
MAC: Intel, Power PC
HP-UX: Itanium, PA-RISC
AIX

Windows Parameters Monitored

FILE ADDITIONS, DELETIONS, MODIFICATIONS, AND READS
ATTRIBUTES: compressed, hidden, offline, read-only, archive, reparse point
Creation time, DACL information, Drivers, File opened/read, File Size, File type, Group security information, Installed software, Local groups, Local security policy, Modify time, Registry (keys and values), Services, User groups

UNIX Parameters Monitored

FILE ADDITIONS, DELETIONS, AND MODIFICATIONS
Access Control List, Attributes: read-only, archive, Creation time, File Size, File type, Modify time, User and Group ID

Supported Platforms CimTrak For Network Devices

Cisco, Check Point, Extreme, F5, Fortinet, HP, Juniper, Netgear, NetScreen, Palo Alto, Others

Supported Platforms CimTrak For Databases

Oracle, IBM DB2, Microsoft SQL Server
MySQL PARAMETERS MONITORED, Default rules, Full-text indexes, Functions, Groups, Index definitions, Roles, Stored procedures, Table definitions, Triggers, User defined data types, Users, Views

Supported Hypervisors

Microsoft Hyper-V, VMware ESXi 3x, 4x, 5x, 6x, 7x

Supported Cloud Platforms

Google Cloud, Amazon AWS, Microsoft Azure

Supported Container & Orchestration Integrations

Docker, Docker Enterprise, Kubernetes, Google Kubernetes Engine (GKE), Amazon Elastic Kubernetes Service (EKS)

Supported Ticketing Integrations

CA ServiceDesk, Atlassian Jira, ServiceNow, BMC Remedy

Supported SIEM Integrations

IBM QRadar, McAfee Event Security Manager, Splunk, LogRhythm, Microfocus Arcsight, and others