

CorreLog for HIPAA

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is an American federal law that requires organizations that handle personal health information (PHI) to protect it against loss or disclosure.

Organizations must protect PHI, which includes an individual's name, address, birth date, Social Security number, demographic data, physical or mental health, and payment history. Organizations must:

- Secure patient records that contain PHI so they are not readily available to those who don't need them—organizations may disclose PHI to facilitate treatment, but only the minimum information necessary
- Adopt and implement privacy procedures, train employees on requirements, and designate a responsible party for adopting and following procedures
- Notify patients of their privacy rights and how their PHI may be used

Q: Why is the HIPAA Privacy Rule needed?

A: Health care providers have a strong tradition of safeguarding private health information. However, in today's world, the system of keeping paper records in locked filing cabinets is not enough. With information broadly held and transmitted electronically, the HIPAA rules provides clear standards for the protection of personal health information.

Background facts

HIPAA was enacted in 1996.

HIPAA privacy regulations took effect April 14, 2003, although some smaller insurers had until April 14, 2004 to comply.

Companies and industries impacted

Organizations impacted by HIPAA include U.S. health care providers (hospitals, private practices), health plans (insurers), and companies that exchange patient information with the above entities, such as billing services, funds transfers and prescription-drug plans.

Penalties and fines for non-compliance

Penalties for disclosing PHI can be severe, whether the disclosure is accidental or not:

- Disclosing PHI: fines up to \$50,000 plus a year in prison
- Disclosure under false pretenses: Up to \$100,000 and five years in prison
- Disclosure with intent of commercial or personal gain or malice: Up to \$250,000 and 10 years in prison

Ship's Log: True Tales of HIPAA

1. Your agency is accused of data negligence.

- a) CorreLog provides a clear record of security violations, and supports an over-arching security policy that incorporates all types of platforms, network devices and application programs.
- b) Tamper-proof archives, with encrypted *checksums*, provide clear evidence of security breaches (or the absence of security breaches).
- c) Correlog monitors thousands of security points within your enterprise and provides a clear audit trail — demonstrating your commitment to security and data privacy.
- d) If a breach does occur, immediate assessment of the actual severity can be obtained, as opposed to your customer or client assuming the worst-case scenario.

2. A mistake permits a private disk to be exported to a public area.

- a) Correlog detects the disk changes and immediately notifies administrative personnel.
- b) CorreLog determines who may have accessed the data — and what other activities they may have done prior to and following the illegal access.
- c) CorreLog takes automatic action upon certain events, such as shutting down firewalls or public Internet access.
- d) The advanced correlation features of CorreLog greatly reduce false alarms, so that action is taken only if the problem is truly critical.

3. An agency contractor uses the password of a government employee to enter your private system.

- a) CorreLog keeps track of user activity on your system, automatically tracking when users have logged into the system and what changes they have made to critical data items.
- b) You can quickly see when a user has accessed an invalid machine, perhaps during odd hours, and be notified of suspicious behaviors, such as clearing log files, installing software, or simply running an editor or application.
- c) You are notified of the event via e-mail, pager, or some other method — so you can take immediate action to block unauthorized access.
- d) A permanent log of all activity is saved, allowing you to investigate further.

CorreLog at the Helm of HIPAA Compliance

CorreLog will guide you through HIPAA compliance. CorreLog configuration audit and control software detects every change made to the IT system, alerts when an unauthorized change is made, and assesses each change is within policy. CorreLog facilitates compliance with many NIST controls, particularly operational and technical controls. By using CorreLog, federal agencies and their associated organizations can achieve and maintain a known and trusted state across their IT infrastructure. The CorreLog system monitors thousands of security points; logging all activity on your system (in excess of ten-million events each day) and correlating this data into alerts and actionable data – more clear and detailed than any other technology today. In general, CorreLog:

- Centralizes all logs on a single system
- Provides clear, detailed visibility into logs globally
- Reduces time and resources spent demonstrating effectiveness of IT controls. CorreLog provides the empirical proof to verify compliance with a single audit trail. CorreLog provides detailed, automated reporting to compliment audits. Correlog dramatically reduces the resources required to prepare audits.
- Maintains compliance automatically – Correlog expose unauthorized changes through reconciliation with expected changes and allows IT staff to immediately identify any exceptions and trigger remediation of configurations that do not conform to policy – helping to meet the continuous monitoring requirements of HIPAA.
- Minimizes security risks – Correlog monitors and reports on every change made across the enterprise regardless of source, detecting unauthorized change and non-conforming configurations to proactively discover and manage security and compliance position.

Correlog incorporates a sophisticated, indexed search engine to furnish extremely fast, interactive searching – saving your organization man hours and reducing expertise requirements. With CorreLog, businesses can reach HIPAA compliance. Below, please find out how CorreLog addresses HIPAA regulations:

User Logon report.

HIPAA requirements (164.308 (a)(5) - log-in/log-out monitoring) clearly state that user accesses to the system be recorded and monitored for possible abuse. CorreLog provides this report.

User Logoff report.

HIPAA requirements clearly state that user accesses to the system be recorded and monitored for possible abuse. CorreLog provides this report.

Audit Logs Access report.

CorreLog provides records of information system activity such as audit logs to help meet HIPAA requirements (164.308 (a)(3) that calls for procedures to regularly review and audit access logs..

Object Access report.

CorreLog identifies when a given object (File, Directory, etc.) is accessed, the type of access (e.g. read, write, delete) and whether or not access was successful/failed, and who performed the action.

System Events report.

CorreLog identifies local system processes such as system startup and shutdown and changes to the system time or audit log.

Host Session Status report.

CorreLog indicates that someone reconnected to a disconnected terminal server session (generated on a machine with terminal services running).

Successful User Account Validation report.

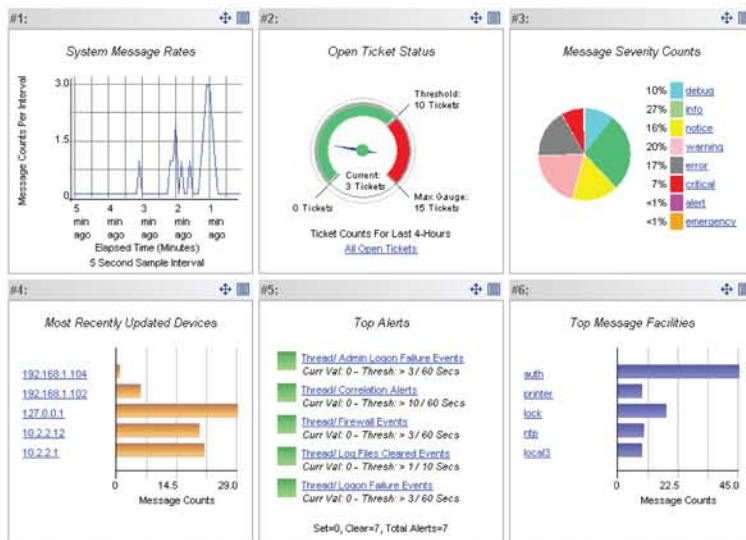
CorreLog identifies successful user account logon events, which are generated when a domain user account is authenticated on a domain controller.

Unsuccessful User Account Validation report.

CorreLog identifies unsuccessful user account logon events, which are generated when a domain user account is authenticated on a domain controller.

Restrict physical access to health care data.

CorreLog detects when systems are restarted (via a cold-start trap or via syslog messages) indicating that physical access may be breached — and systems may have been tampered with. This includes detection of USB and computer driver activity; indicating that somebody may have physical access to a restricted machine. CorreLog monitors the creation, deletion and modification of user accounts and groups so it can detect when access has been given to a user to a particular system. Additionally, CorreLog keeps track of user logins to these systems, including by time of day, so that “after hours” unauthorized access is easily detected.



Sample of CorreLog Custom Dashboard Reporting

Track and monitor all access to network resources and health care data and support audits with detailed visibility.

This is the main role of CorreLog as a security monitor. It provides visibility into who is logging into what areas of the enterprise and keeps track of what users are doing on the system. This is achieved through monitoring log messages and mapping activity back to security protocol.

Regularly test security systems and processes.

CorreLog schedules periodic tests of network integrity and verifies that certain messages are logged, indicating successful tests. CorreLog interfaces easily with common, security-test software, including port scanners, to verify that CorreLog is successfully monitoring system security. CorreLog has a self-test associated with AES encryption that permits users to verify that CorreLog encryption is working.

Maintain a policy that addresses information security.

An organization cannot claim to have a comprehensive information security policy without monitoring the security message being constantly logged on platforms within your enterprise. An enterprise that installs CorreLog, with no other action, takes a major step forward in creating and maintaining an enterprise security policy.

Develop and maintain secure systems and applications.

CorreLog furnishes ability to make Windows platforms more secure (using the CorreLog Windows agent). For UNIX and other platforms, CorreLog leverages the existing native agent (i.e. the syslog process) to make the managed system more secure. CorreLog is a substantial “development component” of an enterprise-wide security system that incorporates a standards-based, easy-to-use API to allow you to extend your security to any streaming log file or home-grown application.

Navigate Your Way to HIPAA Compliance Today

Meet several HIPAA requirements with the ability to assess security protocol configurations and detect and audit change within the IT infrastructure. CorreLog helps you achieve and maintain the integrity of all IT security configurations.

For more information about CorreLog and HIPAA compliance, visit www.correlog.com.

To learn more about how CorreLog can help, contact CorreLog toll-free in the US at 877-CorreLog or 239-514-3331.

About CorreLog, Inc.

CorreLog, Inc. delivers security information and event management (SIEM) combined with deep correlation functions. CorreLog's flagship product, the CorreLog Security Correlation Server, combines log management, Syslog, Syslog-NG, SNMP, auto-learning functions, neural network technology, proprietary semantic correlation techniques and highly interoperable ticketing and reporting functions into a unique security solution. CorreLog furnishes an essential viewpoint on the activity of users, devices, and applications to proactively meet regulatory requirements, and provide verifiable information security. CorreLog automatically identifies and responds to network attacks, suspicious behavior and policy violations by collecting, indexing and correlating user activity and event data to pinpoint security threats, allowing organizations to respond quickly to compliance violations, policy breaches, cyber attacks and insider threats. CorreLog provides auditing and forensic capabilities for organizations concerned with meeting SIEM requirements set forth by PCI/DSS, HIPAA, SOX, FISMA, GLBA, NCUA, and others. Maximize the efficiency of existing compliance tools through CorreLog's investigative prowess and detailed, automated compliance reporting. CorreLog markets its solutions directly and through partners. Visit www.correlog.com for more information.

CorreLog, Inc. • 311 Conners Ave. • Naples, Florida 34108 • 1-877-CorreLog • 239-514-3331 • info@correlog.com