



Event Log Management & Compliance Best Practices: For Government & Healthcare Industry Sectors

By Ipswitch, Inc.
Network Management Division

Table of Contents

Compliance Initiatives: Prepare for the Worst	1
HIPAA	1
HITECH ACT	2
FISMA	2
Event and Log Management Best Practices	3
Best Practice #1: Define Your Audit Policy Categories	3
Best Practice #2: Automatically Consolidate All Log Records Centrally	3
Best Practice #3: Event Monitoring—Real-Time Alerts & Notification Policies	4
Best Practice #4: Generating Reports for Key Stakeholders	5
Best Practice #5: Auditing Log Data	6
What Should an Event and Log Management Solution Provide?	6
Event and Log Management Solution Requirements	7
Conclusion	8
Introducing WhatsUp Event Log Management Suite	8

Compliance Initiatives: Prepare for the Worst

In 2010 to date, fifty-four breaches of protected health information have been reported in public sector healthcare, affecting about 449,000 individuals. And HIPAA non-compliance can be costly; recently, the Department of Veterans Affairs committed \$20 million to correct a data breach which could affect almost one million VA physicians and patients! When it comes to protected health information (PHI), the Department of Veterans Affairs has the same obligations under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) to protect patient information as does a doctors' office in Kansas or a hospital in Boston. As a result, the VA is required to provide notice and credit-monitoring services for approximately 650,000 physicians and 254,000 veterans.

In order to ensure compliance as well as protection of financial and customer data, you need to know who is accessing which systems and data and what they are doing at all times. Records of events taking place in your environment are being logged right now into event logs and Syslog files across your servers, workstations and networking devices. This log data needs to be collected, stored, analyzed and monitored to meet and report on regulatory compliance standards such as FISMA or HIPAA. Without the right log management strategy in place, your organization's exposure to security breaches, malware, loss, damage and legal liabilities is significantly increased.

A quick review of each of the relevant laws and standards below will provide you with a high-level overview to understand compliance regulations in the healthcare industry or government sector and how they can affect your log management strategy.

HIPAA

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is primarily comprised of the Privacy and Security Rules, each of which maintain specific requirements for implementation and reporting. The Rules describe the responsibilities of Covered Entities to provide records and compliance reports as well as to cooperate with, and permit access to information for, investigations and compliance audits and reviews.

According to the Centers for Medicaid and Medicare, organizations must build an IT infrastructure and strategies to protect against "threats or hazard to the security of the information" and, most importantly, prepare for investigation of potential security breaches. HIPAA requires the existence of a reliable audit trail to protect the personal data of medical patients, which must be able to provide "sufficient information to establish what events occurred, when they occurred, and who (or what) caused them."

HIPAA DEFINITIONS FOR ELECTRONIC PROTECTED HEALTH INFORMATION	
Encryption	Use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.
Access	The ability or the means necessary to read, write, modify or communicate data/information or otherwise use any system resource.
Authentication	Corroboration that a person is the one claimed.
Technical safeguards	Technology, policy, and procedures for its use that protect electronic protected health information and control access to it.
Workstation	An electronic computing device. For example, a laptop or desktop computer, and electronic media stored on its immediate environment implement the required specifications.
Workforce clearance procedure	Implementation of procedures to determine that the access of a workforce member to electronic protected health information is appropriate.

When violations of HIPAA regulations are found, the severity and type of violation will dictate whether civil or criminal penalties are appropriate. The below tables detail the potential civil and criminal penalties that can be applied. Criminal sanctions for HIPAA violations are enforced by the Department of Justice.

CIVIL PENALTIES		
Monetary Penalty	Term of Imprisonment	Offense
\$100	N/A	Single violation of a provision (can be multiple violations with a penalty of \$100 each, as long as each violation is for a different provision).
\$25,000	N/A	Multiple violations of an identical requirement or prohibition during a calendar year.

CRIMINAL PENALTIES		
Monetary Penalty	Term of Imprisonment	Offense
Up to \$50,000	Up to one year	Wrongful disclosure of individual health information.
Up to \$100,000	Up to five years	Wrongful disclosure of individual health information committed under false pretenses.
Up to \$250,000	Up to ten years	Wrongful disclosure of individual health information committed under false pretenses, with intent to sell, transfer, or use for commercial advantage, personal gain or malicious harm.

HITECH ACT

The HITECH Act of 2010 amended HIPAA to require Covered Entities to provide notification to individuals, the Office of Civil Rights (OCR) and others when certain breaches of unsecured protected health information (UPHI) occur (Section 13402(e)(3)). The implementing interim “Breach Notification For Unsecured Protected Health Information” regulations (Breach Regulation) published by OCR require Covered Entities subject to HIPAA to notify affected individuals, OCR and in some cases the media within specified periods following a “breach” of UPHI occurring on or after September 23, 2009 unless the Covered Entity can demonstrate that the breach qualified as exempt from the breach notification obligation under the Breach Regulations.

FISMA

The Federal Information Security Management Act (FISMA) is designed to protect critical information infrastructure of the United States Government. It sets minimum security standards for information and information systems and provides guidance on assessing and selecting the appropriate controls for their protection. Each Federal agency and its contractors are required to develop, document and implement policies that meet the FISMA standards.

The National Institute of Standards and Technology (NIST) has issued a Special Publication 800-53 to provide guidelines for selecting and specifying security controls for information systems supporting the executive agencies of the federal government.

All of the legal or industry standards highlighted above reflect an ongoing need to ensure the protection and integrity of PHI and other data and ensure that an audit trail is available for each transaction.

Event and Log Management (ELM) Best Practices

Healthcare entities need to address several essential areas through an event and log management strategy in order to comply with HIPAA rules. It is strongly recommended that IT and security professionals seek the input and feedback of their management and audit teams when structuring any compliance strategies. There should be complete involvement from all disciplines to ensure the integrity of the entire process from gathering of event and log data to auditing and reporting. Here are some of the best practices that will help you build an effective ELM strategy:

- Define audit policy categories (in other words, configure which events to record)
- Automatically consolidate all event records centrally
 - ✓ Use both flat format & database records
- Event monitoring- Real-time alerts & notification policies
 - ✓ Define which events should trigger an alert, and define your poll intervals
- Generating reports for key stakeholders: auditors, security or compliance officers & management teams
 - ✓ Auditing Log Data: Central Log Analysis & Ad-hoc forensics

Also, keep in mind that Windows based systems have several different event logs that should be monitored consistently. Of these logs, the most important is the Security Log. It provides key information about who is on logged onto the network and what they are doing. Besides Security Event logs, some of other Windows event logs that should be regularly monitored are:

- Application events – records application related events; application starts, failures
- System events– records system component events; driver failures and hardware issues
- Directory Services events – Domain controllers record any Active Directory changes
- File Replication service events – for File Replication service events; Sysvol changes
- DNS events – DNS servers record DNS specific events

Best Practice #1: Define Your Audit Policy Categories

The term audit policy, in the Microsoft Windows lexicon, simply refers to the types of security events you want to be recorded in the security event logs of your servers and workstations. On Microsoft Windows NT® systems, you must set the audit policy by hand on individual servers and workstations, but in Windows 2000® or Windows 2003® Active Directory® domains, with Group Policy enabled, you can associate uniform audit policy settings for groups of servers or the entire domain. For a summary of key logging categories to enable, please refer to the “Key Windows and Syslog Events to Monitor” table.

Best Practice #2: Automatically Consolidate All Log Records Centrally

By default, Windows event logs and Syslog files are decentralized, which each network device or system recording its own event log activity. To obtain a broader picture of trends going on across the network, administrators tasked with security and compliance-centric initiatives must find a way to merge those records into a central data store for complete monitoring, analysis and reporting. Log data collection and storing is critical since some compliance standards mandate data retention for 7 years or more! Automation can really help here because it will save time and ensure the log data reliability. Remember:

- 1) **When the archived log files are retrieved, it must be a reliable copy of the data—there can be no debate as to the integrity of the data itself.** As the human element is removed with automation, the level of data reliability is increased.
- 2) The number of machines, users, and administrators in the enterprise; and considerations such as bandwidth and competing resources can complicate log collection so much **that an automated solution is the only way to ensure that every event is collected.** Can you ensure that each and every event has been successfully collected through a manual process?

In a typical setup, an administrator will configure an ELM tool to gather event log records nightly (or periodically) from servers and workstations throughout their network. This process involves saving and clearing the active event log files from each system, reading log entries out of the log files into a central database (e.g. Microsoft SQL or Oracle), and finally compressing the saved log files and storing them centrally on a secure server.

BASELINE ELM STRATEGY FOR SECURITY, COMPLIANCE AND AUDIT
Key Windows and Syslog Events to Monitor
<ul style="list-style-type: none"> • Any changes to File or Folder ACLs • Registry Access – adds, changes, and deletions • User account changes that provide administrator equivalent permissions • Active Directory access and changes • Changes to Groups – adds, changes or deletions • Windows and SSH login failures and successes • System events – process start and shutdown • Application failure, start or shutdown • IDS and anti-virus logs • Interfaces for high TCP and UDP traffic • Server off-line or on-line and reboots • Access to network infrastructure • Changes to ACLs on switches, routers or firewalls • DNS changes • Web server access and permission changes • HTTP “404” errors • FTP server access and file transfers • Server and workstation logs for intrusion incidents and policy changes • Access and permission changes to Files, Folders, and Objects containing financial, customer or compliance data
Key Windows Event Logging Categories to Enable
<ul style="list-style-type: none"> • Logon Events - Success/Failure • Account Logons - Success/Failure • Object Access - Success/Failure • Process Tracking - Success • Policy Change - Success/Failure • Account Management – Success • Directory Service Access - Success/Failure • System Events - Success/Failure

Keeping your log data in two formats—as database records and as compressed flat files—offers a distinct auditing advantage. Event log data in flat files compresses extremely well, often down to 5% of the original size. Therefore, in terms of storage cost, it costs very little to keep archived log data for many years should an auditor ever need it. However, flat files are a very poor medium for analysis and reporting, so keeping an active working set of data (often 60 to 90 days) in a database allows ad hoc reporting as well as scheduled reporting to be available for recent events. **Look for an ELM tool that provides an easy mechanism for rapid re-import of older saved log files back into your database should they ever be needed.** It has been our experience that the majority of employee hours when facing an audit are dedicated to simply chasing flat files around and attempting to extract the same types of data from all of them. Having data at the ready in a central database greatly reduces the potential for lost hours when an auditor comes knocking.

Best Practice #3: Event Monitoring—Real-Time Alerts & Notification Policies

Most organizations have a heterogeneous IT environment, with a broad mix of operating systems, devices and systems. Even though your environment may trend towards Windows desktop and server OSs, you may also want the option of choosing more than just Windows event log monitoring. **Syslog support is important to have not only for routers, switches, IDS and firewalls, but also for UNIX or LINUX systems.**

Most software products require the use of agents to perform real time monitoring of log files. If any factor influences your choice of a solution, this should be the one. **If you can opt for a no-agents-required implementation of a monitoring solution, do it.** This will save a lot of headaches in the initial implementation, as your network grows, and in the ongoing maintenance of your monitoring solution.

When developing a log monitoring plan, every organization has different rules on what sorts of events they must monitor. IT departments will frequently focus on security events as the sole indicator of any issues. While monitoring the security event log is essential, other event logs can also indicate issues with applications, hardware issues or malicious software. **At a minimum all monitored events should be traceable back their origination point.**

Best Practice #4: Generating Reports for Key Stakeholders: Auditors, Security or Compliance Officers and Management Teams

Reporting is a key area because it provides you with significant data on security trends and proves compliance. Reporting can also help you substantiate the need to change security policies based on events that could result or have resulted in compromised security. **Any ELM solution that you implement needs to answer the following questions:**

- What report formats are available?
- How much of your work is already done for you in prepackaged event log reports?
- Are you tied to a particular format? Will HTML and the availability of that HTML report to multiple users play a role?
- Can customized filters be easily recalled for repeat use?
- From what data sources can reports be generated? Does it include EVT, text, Microsoft Access, and ODBC? Can you create custom reports?
- Will the solution be compatible with your event archiving solution?

In general, reporting should be robust, have broad coverage, and provide roll-up of data on a daily, weekly, monthly and yearly basis, along with the ability to define custom reports. Any compromise on reporting will negate the all the other benefits of an ELM solution. The following tables map suggested reporting requirements for security and compliance officers to specific requirements of HIPAA and FISMA:

HIPAA	
Legal Requirements	Suggested Reports
Security Rule §164.306 and Privacy Rule §164.530(c) All of the following must be addressed for logging and reporting: <ul style="list-style-type: none"> • Password Aging • Consolidated Change Logs • User Privileges • NTFS Permissions • System Privileges • Role Permissions & Membership • Remote Access • User Access • Auditing Enabled 	<ul style="list-style-type: none"> • Account Management – Success/Failure • Directory Service Access - Success/Failure • System Events - Success/Failure • Object Access Attempts – Success/Failure • Object Deletions • Group Management • Password Reset Attempts by Users • Password Reset Attempts by Administrators or Account Operators • Computer Account Management • Directory Service Access Attempts • Logon Failures – Active Directory • Logon Failures – Local Logons

FISMA	
Legal Requirements	Suggested Reports
<p>8-602. Audit Capability. Security auditing involves recognizing, recording, storing, and analyzing information related to security-relevant activities. The audit records can be used to determine which activities occurred and which user or process was responsible for them.</p> <ul style="list-style-type: none"> • Individual accountability • Enough information to determine the date and time of action the system locale of the action, the system entity that initiated or completed the action, the resources involved, and the action involved. • Successful and unsuccessful logons and logoffs. • Successful and unsuccessful accesses to security-relevant objects and directories, including creation, open, close, modification, and deletion. • Changes in user authenticators. • The blocking or blacklisting of a user ID, terminal, or access port and the reason for the action. • Denial of access resulting from an excessive number of unsuccessful logon attempts. 	<ul style="list-style-type: none"> • Directory Service Access Attempts • Directory Service Access - Success/Failure • Logon Failures – Active Directory • Logon Failures – Local Logons • Object Access Attempts – Success/Failure • Object Deletions • Password Reset Attempts by Administrators or Account Operators • Process (Program) Usage • User Activity in Auditing Categories • Computer Account Management – Success/Failure • Successful Network Logons – Workstations and Servers • Policy Change - Success/Failure • Account Management – Success/Failure • Directory Service Access - Success/Failure • System Events - Success/Failure

Best Practice #5: Auditing Log Data

Event logs contain a large amount of data; the thought of manually sifting through daily logs to find relevant information is intimidating. However, if careful steps have been taken in planning the actual log archive, auditing and then reporting from event logs becomes much easier. A solution must provide predefined and configurable search and filtering capabilities. The ability to also define custom search and filtering parameters is another invaluable feature. Furthermore, log data should be automatically grouped into related sections, with event identifier codes translated into human readable explanations.

What Should an Event and Log Management Solution Provide?

Based upon discussions with a broad spectrum of customers who are dealing with compliance regulations and industry standards on an ongoing basis, the Event and Log Management Solution Requirements table at left represent a general consensus of the most important features that a best fit solution would provide. Your industry, organizational structure, business model, IT infrastructure and policies and procedures will shape your direction and implementation of any ELM solution.

EVENT AND LOG MANAGEMENT SOLUTION REQUIREMENTS

Log Collection	Log Archiving
<ul style="list-style-type: none"> • Automated collection of log files • Supports Windows Event Logs – both .evt and .evtx formats • Supports Syslog log files • Configure to clear or not clear log files • Collects all generated events • Collects only certain types of events • Can export log data from one source to another 	<ul style="list-style-type: none"> • Compression of log data • Can provide email notification of failed archive attempts • Can automatically retry failed archive attempts • Continues from last collected event • Scheduled time • Percent full (threshold) • Opens zipped event log files (.evt) for review
Log Consolidation and Storage	Data Formats
<ul style="list-style-type: none"> • Secure log aggregation and storage for Windows Event Logs and Syslog data from devices and OSs (UNIX, Linux) • Supports SQL databases for log data • Provides log normalization • Supports automated compression 	<ul style="list-style-type: none"> • Syslog • SQL • MS Access • .evt Log Format • Comma Delimited Text File • HTML Report Format • Comma-Delimited Report Format
Monitoring	Alerts and Notifications
<ul style="list-style-type: none"> • Agentless monitoring • Real-time monitoring • Configurable polling • Servers go offline/online • System shutdowns/restarts • Detect and track changes to users/groups/computers • Detect and track unauthorized account usage • Detect and track printer activity • Detect policy changes • Detect account lockouts • Track logon activity • Track errors and warnings • Track changes/deletions on files/folders/registry keys • Ability to create custom "alarms" for log monitoring 	<ul style="list-style-type: none"> • Define alerts for events of interest • Define alert for a single event • Configurable thresholds • Provides predefined alarms • Alerts on devices and OSs supporting Syslog • Define events as either high risk, medium risk or low risk • Notification Support <ul style="list-style-type: none"> - Network pop-ups - E-mail messages - Pager - Short e-mail messages - Syslog messages - Database insertions - NetBIOS broadcast notification • Supports regulation of notifications • Sends notifications to multiple e-mail addresses
Reporting	Log Analysis and Management
<ul style="list-style-type: none"> • Provides out-of-the-box predefined reports • Provides access to log reports via browser • Can report daily, weekly, or monthly results for defined data • Ability to create custom reports • Configurable report formats • HTML based reports 	<ul style="list-style-type: none"> • Provides a tree view of events and data for analysis • Supports extensive filtering options • Create custom filters for review • Provides predefined filters • Supports choice of log type to manage including: <ul style="list-style-type: none"> - Application - Security - System - DNS Server - Directory Service - File Replication Service

Conclusion

Security and compliance are anything but easy or simple. They both require knowledge, planning and investment. In the end, the best place to start is to review the individual requirements you think apply and then take a look at some successes from other organizations. While this is in no way the complete answer to full compliance and an A+ score on an audit or security nirvana, it does represent the best information we've encountered in successful, real-world compliance efforts.

And, of course, it helps to get started on your effort more than 12 hours before the auditors arrive. We hope that this summary of best practices for both compliance and security initiatives has provided some real-world guidance, saved you valuable time and prevented any future headaches.

Introducing WhatsUp Event Log Management Suite

The WhatsUp Event Log Management Suite is a modular set of applications that can automatically collect store, analyze and report on both Windows Event and Syslog files for real-time security event detection and response, and historical compliance assurance and forensics.

- **Event Archiver:** Automate log collection, clearing, and consolidation. Great for assisting in auditing & regulatory compliance.
- **Event Alarm:** Monitor log files and receive real-time notification on key events. Real-time notifications for intrusion detection and monitoring for domain controller lock-outs, or file and folder access.
- **Event Analyst:** Analyze and report on log data and trends. Automatically distribute reports to management, security officers, auditors and other key stakeholders.
- **Event Rover:** Mine and view event data in a convenient tree-view format. Featuring exclusive patented LogHealer Technology, for resolving potentially corrupt Microsoft EVTX log files.
- **Auditing Volume Analyzer** is a freeware utility offered to assist administrators in estimating the amount of event log data being generated on a given network.

Did you know that Ipswitch's WhatsUp Event Archiver was awarded US's Army Certificate of Networthiness # 201004611? You can find out more about the WhatsUp Gold Event Log Management Suite at: <http://www.whatsupgold.com/products/event-log-management/>

About the Network Management Division of Ipswitch, Inc.

The Network Management Division of Ipswitch, Inc. is the developer of the WhatsUp Gold suite of innovative IT management software. WhatsUp Gold delivers comprehensive network, system, application and event log monitoring and management solutions for small and medium businesses and enterprises. Built on a modular, yet integrated architecture, the affordable and easy-to-use solutions scale with the size and complexity of any physical or virtual IT infrastructure. From a single console, WhatsUp Gold supports standard IT management tasks including automated discovery, mapping, real-time monitoring, alerting, troubleshooting and reporting. More than 100,000 networks worldwide use WhatsUp Gold solutions to assure the availability, health and security of their critical business infrastructure today.

Ipswitch, Inc.'s Network Management Division recently added to its product line complete, easy-to-use solutions for Windows Security Event Management (SEM) and Log Management for small businesses and enterprise-level organizations suite with the acquisition of Dorian Software Creations, Inc. WhatsUp Gold was named Network Management Product of 2010 by Network Computing Magazine and earned the Network Products Guide 2010 Product Innovation Award in Network Management. To learn more about WhatsUp Gold – the best value in IT Management software, download a free trial or to make a purchase, please visit: <http://www.whatsupgold.com/products/download/>.

All mentioned trademarks, product and company names cited herein are the property of their respective owners.