BLUE LANCE

HIPAA Compliance with LT Auditor+

An Executive White Paper

By

BLUE LANCE, Inc.

On February 20, 2003, the Department of Health and Human Services (HHS) ended many years of speculation concerning security standards that must be met by entities processing electronic protected health information. When Congress passed the Health Insurance Portability and Accountability Act (HIPAA) in 1996, the HHS Department was authorized to define a security standard to ensure the privacy of personal health information. With an update to the Code of Federal Regulations (CFR) 45 (parts 160, 162, and 164) (the "Security Rule"), the HHS Department finalized its security standards, providing guidance on the need for administrative, physical, and technical security measures. The standards include a provision that requires regulated entities to monitor information system activities as part of their security operations. Blue Lance, with its LT Auditor+ product, can help regulated entities that must comply with the HHS Security Standards achieve compliance with the activity monitoring related implementation specifications.

HIPAA Overview – Covered Entities need to protect Health Related Information

Regulated entities include all health plans, all healthcare clearinghouses, and those healthcare providers (including doctors, dentists, and pharmacists) who electronically process certain kinds of healthcare related financial or administrative transactions ("covered transactions"). Within Subtitle F – Administrative Simplification in HIPAA, Congress stated its desire to promote efficiencies and lower the costs of administering health care. Two key requirements in achieving this objective are to (1) standardize the structure and format of common types of health care transactions and (2) encourage the use of computers to transmit health care related information between entities involved in the processing of a covered transaction. Through the use of automation and the reduction of paper-based processing, lower costs can be expected as efficiencies are realized.

Types of health care transactions that are considered "covered" include:

- Health plan enrollment and disenrollment.
- Transactions that determine eligibility for participating in a health plan or receiving health plan benefits.
- Health claims and claim-related information exchanged between parties for some approved business function.
- Health care payment and remittance advice.
- Health plan premium payments.
- Health claim status.
- Doctor referral certification and authorization requests.

- Coordination of benefits.

In conjunction with a desire to achieve processing efficiencies, Congress directed the HHS Department to develop security standards that can ensure the privacy of patient health information included in the covered transactions. In a draft Security Rule issued in 1998, the HHS Department proposed protecting all electronic patient health information that is stored and processed by computers, even if the information was not transmitted between entities as part of the processing of a covered transaction. In the final Security Rule, the HHS Department reduced the scope of electronic patient health information that is to be protected to include only information processed within covered transactions, provided the transaction involves electronic transmission of the information over a network. The HHS Department further clarified in the preamble on page 8338 in the final Security Rule that electronic patient health information must be protected before, during, and after it is transmitted.

> *"Section 1173(d)(2) of the Act [HIPAA] states: Each person described in section 1172(a) who maintains or transmits health information shall maintain reasonable and appropriate administrative, technical, and physical safeguards – (A) to ensure the integrity and confidentiality of the information; (B) to protect against any reasonably anticipated – (i) threats or hazards to the security or integrity of the information; and (ii) unauthorized uses or disclosures of the information … This language draws no distinction between internal and external data movement. Therefore, this final rule covers electronic protected health information at rest (that is, in storage) as well as during transmission."*

Technically, the HHS Security Standards only have to be applied to electronic protected heath information. Health information in paper form is not subject to the HHS Security Standards, but still needs to be protected in accordance with a separate set of standards known as the "Privacy Rule." Many of the practices advocated through the security standards would be considered best security practices, with most of the practices expected to be followed by larger covered entities that already have in place a mature information security program. Even small health care providers (e.g.; a physician or dentist who has a health care practice), that store patient health information in a single computer and subsequently transmit the information as part of a covered transaction, are responsible for complying with the security standards.

If a covered entity outsources the processing of electronic protected health information to another company, the outside service provider (a.k.a.; a business associate) is also required to comply with the HHS Security Standards. So, in effect the HHS Security Standards could motivate a minimum level of security practices that can affect entities in

businesses that are not dedicated to servicing the Health Care Industry.

Most covered entities will have until April 20, 2005 to achieve full compliance with the security standards. Small health plans will have an additional year to achieve full compliance, until April 20, 2006.

The security standards include 42 separate implementation specifications, each drafted in a way to provide guidance on achieving some information security objective. 13 of the specifications are declared mandatory – they are considered basic elements in any program that strives to protect electronic protected health information. The remaining 29 implementation specifications are considered discretionary, but the process of deciding relevance is anything but arbitrary. The HHS Department refers to these discretionary specifications as "addressable" implementation specifications. The covered entity is expected to perform an analysis to determine the applicability of each "addressable" specification, document the results of the analysis, and decide if the "addressable" specification is to be implemented or if the objective of the specification can be satisfied through some other means.

The Importance of Activity Monitoring in Achieving HIPAA Compliance

Of the 13 required implementation specifications, two of the specifications can be satisfied through the use of system audit trails:

- § 164.308 (a) (1) (ii) (D) in the Security Rule requires an Information System Activity Review to be part of a security management process in order to detect security incidents. A security incident is defined in § 164.304 in the Security Rule as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. The covered entity is expected to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

- § 164.312 (b) in the Security Rule requires implementing hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

The inclusion of these two mandatory implementation specifications is consistent with direction Congress provided the HHS Department, as stated within Subtitle F, "Administrative Simplification" section 1173(d) in HIPAA:

> *"… (d) SECURITY STANDARDS FOR HEALTH INFORMATION … The Secretary shall adopt security standards that (A) take into account … (iv) the value of audit trails in computerized record systems …"*

It should also be noted that the retention period for records that can demonstrate compliance with the Security Standards is stated to be 6 years (as indicated by § 164.316 (b) (2) (i) in the Security Rule). When audit trails are used to meet the standards, archived audit trails must be retained for 6 years.

In the preamble to the security standards on page 8336 in the Security Rule, the HHS Department indicated that 13 of the implementation specifications were determined to be mandatory and were influenced by (1) expertise of Federal security experts; (2) generally accepted industry practices and (3) recommendations from the Committee on Maintaining Privacy and Security in Health Care Applications of the National Information Infrastructure, National Research Council (NRC) appearing in Chapter 6 within the 1997 report *For the Record*: Protecting Electronic Health Information. Pages 176 to 177 in the report includes a recommendation in support of comprehensive auditing, with the objective of maintaining a detailed record of all accesses to electronic protected health information. Beginning on Page 180 of the report, the NRC presents a number of recommendations designed to deal with systemic issues related to privacy and security. Included in these recommendations is a recommendation to address potential usability issues introduced by comprehensive audit trails. Specifically, the NRC acknowledged the need to produce usable audit trails by employing effective tools, as indicated in Recommendation 5.2 under the subheading Audit Tools:

> *"Audit trails are useful as a deterrent to improper access only if there is some possibility that an improper access will be recognized as such. However the collection of audit trails routinely generated enormous amounts of data that must then be analyzed. Automated tools to analyze audit trail data would enable much more frequent examination of accesses and thus serve a more effective deterrent role. For example, intelligent screening agents could be developed that would sort through audit trail data and flag some records for more thorough analysis."*

Achieving an Effective Level of Activity Monitoring

While the HHS Department does not specify exactly what system activities are to be audited, the implication is that the level of auditing should be sufficient so unauthorized access to electronic protected health care information can be recognized and acted upon. Covered entities will need to consider various ways in which information can be compromised in determining the most effective auditing policy. Opportunities may exist to record activity from a number of vantage points including: (1) the operating system's perspective (using available system level auditing capabilities); (2) the network communication's perspective (using network traffic monitoring tools); (3) a health information application's perspective (using available application transaction logging capabilities); and (4) a database management system's perspective (using available database access logging capabilities). The importance of a particular level of logging will be situational, where varying circumstances could make the information in one log important one day, but less important another day.

Although the HHS Department avoids explicitly defining an auditing baseline configuration, we need to not lose sight of the HHS Department's interpretation that Congress' intent was to maintain a high standard of protection. Within the preamble on page 8346 in the Security Rule appears the following statement:

> *"Furthermore, we believe the Congress' intent in the use of the word 'ensure' in section 1173(d) of the Act [HIPAA] was to set an exceptionally high goal for the security of electronic protected health information."*

If covered entities need further insight into what level of system auditing could be deemed satisfactory to meet this exceptionally high goal, the entity should carefully consider the aforementioned definition of security violation (under the subheading *Security Incident* within § 164.304 in the Security Rule), implying a comprehensive level of auditing, including a comprehensive level of auditing at the operating system level.

In order to design an effective auditing policy, covered entities may seek further guidance from the ISO 17799 Standard and in particular, clause 9.7 within the standard entitled "Monitoring System Access and Use." Requirement 9.7.1 within this clause specifically advocates the importance of recording exceptions and other security-relevant events. This includes records of successful/rejected system access attempts (logons, logoffs, connections) and other successful or rejected resource access attempts (including file access). The selection of the 13 minimum implementation security specifications is consistent with various statements in the ISO 17799 standard, which Information Security

Professionals generally see as a representative statement of best practices today.

The business case for comprehensive auditing at the operating system level can be further strengthened when considering scenarios that could compromise the confidentiality, integrity, or availability of electronic protected health information. Examples of such scenarios (and potential compensating monitoring practices) include the following:

- Unauthorized review of information in files containing electronic protected health information, including unauthorized access by employees possessing privileged access with the expressed purpose to administer access controls at the application, database, or operating system level.

  Compensating Monitoring Practice: Monitor use of privileged accounts and access to sensitive files.

- Ineffective access controls implemented either in error or by a security administrator that is inadequately trained, introducing an opportunity for unauthorized users to access electronic protected health information.

  Compensating Monitoring Practice: Monitor changes to access controls and compare changes to management approved access authorizations.

- Unauthorized changes to application, system software (including operating system components), or other critical control files, with the intent of changing the behavior of the system and introducing opportunities that can lead to unauthorized access to protected health information.

  Compensating Monitoring Practice: Monitor changes to executable software and critical control files.

- Unauthorized access by someone who logs into a system under the account of someone else who is authorized to access electronic protected health information.

  Compensating Monitoring Practice: Monitor suspicious patterns of activity following a successful logon.

- Attempts at systematically testing a system for weak controls, looking for unauthorized ways to enter the system and introducing opportunities to access electronic protected

health information without authorization.

Compensating Monitoring Practice: Monitor attempts at accessing resources that are rejected.

- System infiltration by a computer virus or worm that is designed to randomly grab files and e-mail the compromised files to randomly selected e-mail addresses. If through a stroke of bad luck a grabbed file contains protected health information, this type of attack could potentially lead to a violation of the HIPAA privacy requirements, given the health information was not adequately protected while it is "at rest." It may be worthwhile to note that the concept of designing a worm with file grabbing properties was experienced with the highly prevalent *Sircam.A* computer worm and is likely to be repeated with new viruses/worms programmed with similar capabilities.[1]

  Compensating Monitoring Practice: Monitor attempts at accessing sensitive files out of a normal context.

- Exploitation of a technical vulnerability in the operating system or some other system software running in a privileged mode, allowing a skilled adversary to obtain "privileged control" over the compromised system and potential unauthorized access to protected health information on the penetrated system. Statistics reported by Carnegie Mellon University's Emergency Response Team (CERT) over the last 3 years illustrate a steep increase in reported vulnerabilities, with many vulnerabilities introducing ways to get unauthorized privileged access to vulnerable systems. 7,913 vulnerabilities were reported in 2003 and 2002, compared to 5,033 vulnerabilities reported over the previous 7 years, with many vulnerabilities affecting software that is in widespread use.

  Compensating Monitoring Practice: Monitor for suspicious patterns of activity attributed to accounts that vulnerable software runs under.

In reflecting upon the above sample scenarios, it is easier to see a networked computer system as an inherently vulnerable environment. Clearly, the statistics reported by CERT demonstrate that most businesses will be faced with continuing pressure to respond to vulnerabilities that affect their computer systems. In general, operating system level

[1]Based on Virus Incident Statistics reported by Trend Micro Incorporated, as of January 28, 2004, 1,765,727 computers were infected with the Sircam.A variant of the Sircam worm.

auditing can help a business manage its vulnerabilities in two significant ways:

- By detecting the exploitation of vulnerabilities (many which may not be recognized until they are exploited).

- By monitoring systems that are known to be vulnerable and must remain vulnerable while the business waits for the opportunity to apply corrective measures. Delays in applying corrective measures can be due to delays in receiving fixes from the vulnerable software's manufacturer or delays in applying available fixes due to other reasons (e.g.; the business does not have the time to test and apply an available fix).

Vulnerabilities that are exploited can lead to other important controls and logs becoming compromised, further degrading the integrity of a penetrated environment. Maintaining a detailed record of activity from the operating system's perspective can be advantageous in validating the integrity of other important controls and logs, including logs at the application and database management system levels. Of course, this assumes that the operating system level auditing capabilities employ reasonably reliable defensive methods to protect its logs. Without a record of activity from the operating system perspective, we would not have an independent "controlled" means to ensure that other logs recording access to electronic protected health information have not been tampered with.

Some adversarial scenarios mentioned above may seem unlikely when contemplating "motive" and considering other controls in the environment. It is legitimate to question why someone would be motivated to compromise (view or alter) electronic protected health information about someone else. What can an adversary possibly gain from unauthorized access to electronic protected health information? Motive is important to consider, since it is one of the factors that determine the "risk" that an attack may occur. Other factors include technical knowledge required to subvert existing controls, access required to launch an attack, and time required to launch the attack. Potential motives that could lead to a "motivated attack" include:

- Interest in obtaining and profiting from health care information about someone who has celebrity status.

- Interest in introducing fraudulent health care records with the objective of collecting fraudulent medical claims.

- Interest in selectively altering patient health care information with the objective of adversely affecting the care provided to a patient.

- Interest in indiscriminately disrupting a health care information system in order to disrupt a health care provider's ability to care for all its patients.

- Interests in publicizing a successful attack on a covered entity in order to shake consumer confidence in the quality of implemented controls and illustrate lack of compliance with HIPAA. We can entertain the possibility of one covered entity either directly or indirectly (through hired adversaries) becoming motivated to compromise the systems of a competitor in order to obtain some competitive advantage -- clearly unethical, immoral, and criminal, but still a possible motive.

In addition to these potential motivated attacks initiated by human adversaries, there is the possibility of "automated" indiscriminant attacks that can lead to electronic protected health information becoming compromised. Such attacks could be launched through capabilities similar to what was programmed into the *Sircam.A* computer worm.

With the above in mind, it is easier to understand how the use of audit trails can have a deterrent effect in discouraging criminal behavior or can be advantageous in prosecuting or recovering from a criminal act. We can expect that Congress had these benefits in mind when they specified that the value of audit trails should be considered by the HHS Department when defining security standards to protect health information.

Leveraging LT Auditor+ Capabilities to Help Achieve Compliance with the HIPAA Security Standards

Organizations that are required to comply with the HIPAA Security Rule will be able to take advantage of a number of features in LT Auditor+:

- The ability to use monitoring agents that record system activities from the operating system perspective. A detailed record can be generated of access to any file containing electronic protected health information.

- The ability to use monitoring agents to implement an effective level of security-event monitoring, achieved through the monitoring of:

    - System access (logons, logoffs, and connections)

- Administrative activities (e.g.; account management, access control management)
- Use of privileged accounts
  - Access to files containing confidential information,
  - Changes to access controls,
  - Changes to executable software and critical control files,
  - Suspicious patterns of activity following a successful logon,
  - Rejected attempts at accessing resources,
  - Attempts at accessing sensitive files out of a normal context,
  - Suspicious patterns of activity following exploitation of vulnerable software.

- The ability to monitor systems in a transparent manner.

- The ability to monitor Windows Servers and Workstations, Netware Servers, and SYSLOG-enabled computers/applications (including Unix Servers, Network Devices, and firewall appliances).

- The ability to install a monitoring agent from a remote location onto a computer that needs to be monitored, provided the installer has privileged access to the desired computer. This remote installation capability eliminates the need to be physically present at the computer and reduces the costs in deploying an LT Auditor+ infrastructure within an organization that has many computers that need to be monitored.

- The ability to configure and deploy a monitoring configuration from a central computer functioning as a management console to computers monitored by LT Auditor+ agents. Deployed monitoring configurations can be adjusted, on demand, from the management console, giving Blue Lance Customers the ability to throttle the level of auditing in response to changing monitoring needs.

- The ability of monitoring agents to report events in a real time manner, delivering the reports either through native operating system messaging capabilities, SNMP, or e-mail agents. Real Time Alerting can give a Blue Lance Customer the ability to recognize exceptional events (including attempted security breaches) quickly, so remedial steps can be promptly taken to contain an adversary and reduce the likelihood that electronic protected health information will be further compromised. Real Time Alerting can be used to notify incident response teams of access to honey

pot files (planted files with fake protected health information), in order to more easily identify an adversary, who has managed to penetrate an organization's infrastructure and who is searching for opportunities to compromise electronic protected health information.

- The ability to use LT Auditor+ filtering methods in order to ignore extraneous data that is automatically recorded in native Windows logs, increasing the utility of the log files maintained by LT Auditor+ and avoiding unproductive information overload.

- The ability to archive native Windows logs for backup purposes and to enhance a Blue Lance customer's ability to investigate computer crime.

- The ability to protect the recorded activity in LT Auditor+ log files from being tampered with, including an ability to transfer log files to a separate log consolidation computer in order to simplify the management and protection of archived log files. Log file transferring can be configured to occur on a scheduled basis (e.g.; off hours) or can be configured to occur in response to an attempt at shutting down an LT Auditor+ agent (i.e.; a defensive transfer) or in response to certain detected events that may be indicative of an intruder (i.e.; another form of a defensive transfer).

- The ability to protect the integrity and confidentiality of communications between an LT Auditor+ agent and manager, through the use of cryptography and other control mechanisms.

- The ability to import LT Auditor+ log files into a relational database management system on the log consolidation computer, giving Blue Lance Customers a high degree of flexibility in querying activity information stored in the database using the LT Auditor+ SQL Report Generator or using other SQL oriented querying tools.

- The ability to use canned database management scripts to simplify the retention and archiving of historical data.

- The ability to audit the actions of an LT Auditor+ Administrator and to monitor the integrity of an LT Auditor+ architecture through status monitoring and transaction logging.

Conclusion

In conclusion, this paper discussed the role of system auditing in complying with the Health Insurance Portability and Accountability Act. The Health and Human Services Department has declared monitoring information system activities to be a mandatory part of any security management practice focused on protecting health information. The final security standards published on February 20, 2003 included two mandatory implementation specifications that can be satisfied with the use of system audit trails. Blue Lance Customers that are regulated by HIPAA will be able to take advantage of LT Auditor+ as a way to validate that electronic protected health information is being accessed in an authorized manner and to recognize and respond to attempted unauthorized access.