

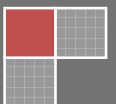
2008

HIPAA COMPLIANCE

APPROACH AT LAST PEAK

Last Peak takes pleasure in appending herewith an overview of its HIPAA implementation. While Last Peak has assumed a best practices approach in its implementation, it recognizes that industry standards are to be adhered to if it is to gain preeminence in its field of operation. In most instances Last Peak has complied with HIPAA standards, and in certain instances exceeded the same, more so when it involves risk management and data integrity.

LPD0225
LP
8/26/2008



ADMINISTRATIVE SAFEGUARDS

Administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information (EPHI) and to manage the conduct of the covered entity's workforce in relation to the protection of that information.

Security Management Process - § 164.308(a) (1)

The first standard under Administrative Safeguards section is the Security Management Process. This standard requires covered entities to:

"Implement policies and procedures to prevent, detect, contain and correct security violations."

There are four implementation specifications in the Security Management Process standard.

1. RISK ANALYSIS (C) - § 164.308(a) (1) (ii) (A)

The Risk Analysis implementation specification requires covered entities to:

"Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity."

We have listed out EPHI within the organization and the associated points of potential risk and vulnerability of the same have been identified. For each of these identified points, specific measures have been taken to minimize the overall risk.

For example:

All points from where potential data leakage can take place have been identified. These include:

- i. List of external devices that could be potentially used for copying / modifying/ deleting data from these machines
- ii. Ports on these machines to which external storage devices can be connected

- i. Networks and domains on which these machines containing EPHI data reside and their points of vulnerabilities allowing access to / from the external world
- ii. Those points of vulnerabilities from where virus or other malware can enter the eco-system
- iii. Applications like email, ftp, IM, etc through which potential data leakage can occur
- iv. The rights given to various personnel who work on the EPHI data, especially rights for data modification/ deletion – which, in turn, are closely monitored
- v. Rights to print - which are also strictly regulated and restricted only to those users who are required to print
- vi. Outlining of clear roles and responsibilities of individual operators who work on the EPHI data – with principles of Segregation of Duties (SoD) employed while outlining the same
- vii. Physical entry/exit points to premises where the EPHI data is handled from
- viii. all computers, workstation servers and laptops, along with the networks and domains, which have EPHI resident therein have been segregated and isolated within the premises.
- ix. Use of PDAs, Smart Phones, USB Memory Sticks and other external storage devices have been restricted/banned from being collocated in the premises where EPHI is being worked on or resides either on server or client environment
- x. Access to any external networks, including the Internet, is banned / restricted from these machines
- xi. No user on these machines is enabled to send mail out to any external entity from these machines.

Thus, EPHI data is protected physically by more than adequate cover against natural or manmade disasters.

2. RISK MANAGEMENT (E) - § 164.308(a)(1)(ii)(B)

Risk Management is a required implementation specification. It requires an organization to make decisions about how to address security risks and vulnerabilities. The Risk Management implementation specification states that covered entities must:

“Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).”

- EPHI is protected by a stringent security policy wherein EPHI storage is behind biometric and password pin enabled locks and all files are password protected which changes randomly every fifteen (15) days. Security policies and changes thereon are communicated every 15 days through the organization at various levels. Senior management is always involved in the decision making process and implementation.
- Having regard to the security system in place the only treat of intrusion would be via portable devices like laptops which have been separately addressed in a matrix given hereunder:

3. SANCTION POLICY (E) - § 164.308(a)(1)(ii)(C)

Another implementation specification in the Security Management Process is the Sanction Policy. It requires covered entities to:

“Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.”

- Via a generic workforce training manual, all employees are made aware of our security policies & procedures and also the consequential actions for violation of the same
- Additionally, all employees are given bimonthly training updates on changes in security policy as well as consequences for violation.
- All employees are required to sign a statement of adherence to our security policies on a quarterly basis.
- In the past, violations from adherence norms have been taken up by disciplinary procedure which has resulted in terminations. We do not distinguish on severity of transgression. All transgressions are met with dismissal

4. INFORMATION SYSTEM ACTIVITY REVIEW (E) - § 164.308(a)(1)(ii)(D)

The Security Management Process standard also includes the Information System Activity Review implementation specification. This required implementation specification states that covered entities must:

“Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.”

- We have implemented extensive audit trails through proprietary software systems to enable logging of user activity by specific machine identity and have a reporting system for all access including specific deviations by way of time outs.
- We have also restricted all anonymous access and exceptional incidents are logged contemporaneously with cause-effect reporting.
- These cause-effect reviews and reports are examined by management on a weekly basis both of exception accounting as well as for contemporaneous procedure monitoring.
- The company also has a policy whereby all reviews and audits are specifically mentioned for implementation.

Assigned Security Responsibility(C) - § 164.308(a)(2)

The second standard in the Administrative Safeguards section is Assigned Security Responsibility. There are no separate implementation specifications for this standard. The standard requires that covered entities:

“Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart [the Security Rule] for the entity.”

- We have a Chief Security Officer, who reports directly to the CEO thereby eliminating any possibility of nexus by and between the CIO and workforce administration policy breaches.

Workforce Security - § 164.308(a)(3)

The third standard is Workforce Security, which states that covered entities must:

“Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under [the Information Access Management standard], and to prevent those workforce members who do not have access under [the Information Access Management standard] from obtaining access to electronic protected health information.”

Within Workforce Security there are three addressable implementation specifications.

1. AUTHORIZATION AND/OR SUPERVISION (C) – § 164.308(a)(3)(ii)(A)

Where the Authorization and/or Supervision implementation specification is a reasonable and appropriate safeguard for a covered entity, the covered entity must:

“Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.”

- ❖ The company has implemented an authorization and access policy whereby employees at various levels are identified by access zones giving them varying levels of access to information depending on job function.
- ❖ This access is determined by managers within the organization.
- ❖ Clear Segregation of Duty (SoD) principles are employed while their individual job functions have been worked out.
- ❖ Access to paper record equivalent rank pari passu with those of EPHI

2. WORKFORCE CLEARANCE PROCEDURE (C) - § 164.308(a)(3)(ii)(B)

Covered entities need to address whether all members of the workforce with authorized access to EPHI receive appropriate clearances. Where the Workforce Clearance Procedure implementation specification is a reasonable and appropriate safeguard for a covered entity, the covered entity must:

“Implement procedures to determine that the access of a workforce

member to electronic protected health information is appropriate.”

- We have implemented procedures and practices to ensure that designated workers belonging to a particular work zone have access only to their own work zone and not to others thereby restricting information depending on level. The company also reviews access to EPHI dependant on job function periodically.

3. TERMINATION PROCEDURES (C) - § 164.308(a)(3)(ii)(C)

Where the Termination Procedures implementation specification is a reasonable and appropriate safeguard for a covered entity, the covered entity must:

“Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph(a)(3)(ii)(B) [the Workforce Clearance Procedure] of this section.”

- The company has implemented stringent termination policies and procedures for denial of access with immediate effect from when decisions of terminations are taken to ensure that physical access to work zones as well as EPHI are denied. Communications of terminations of members of the workforce are parallelly documented and communicated both by and through the CIO to ensure denial of system access as also through chain of command to deny physical access.

Information Access Management - § 164.308(a) (4)

The fourth standard in the Administrative Safeguards section is Information Access Management. Covered entities are required to:

“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 [the Privacy Rule].”

The Information Access Management standard has three implementation specifications.

1. ISOLATING HEALTH CARE CLEARINGHOUSE FUNCTIONS (C) – § 164.308(a)(4)(ii)(A)

The Isolating Health Care Clearinghouse Functions implementation specification states:

“If a health care 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.”

- ❖ Since the company performs clearing house functions, access to EPHI records are restrictive even from the larger organization and policies and procedures are in place to ensure that the larger organization's access to databases are documented, authorized and implemented consequent upon specific checks being carried out.
- ❖ Random access by the larger organization is prohibited and debarred unless an audit trail is implemented for access
- ❖ Further, these audit trails are routinely examined, as discussed earlier.

1. ACCESS AUTHORIZATION (E) - § 164.308(a)(4)(ii)(B)

In the Workforce Security standard portion of this paper, authorization was defined as the act of determining whether a particular user (or computer system) has the right, based on job function or responsibilities, to carry out a certain activity, such as reading a file or running a program. Where this implementation standard is a reasonable and appropriate safeguard for a covered entity, the covered entity must:

“Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.”

- ❖ Specific access by members of the workforce are documented in a worker-specific communication wherein rules, policies and

procedures are laid down in consonance and keeping with the guidelines of the CSO.

- ❖ Various members of the workforce are granted separate levels of access depending upon their job functions and these are worker-specific and cannot be migrated by either migrating the person or by migrating the machine.
- ❖ Security policies are in place which are both machine and individual specific in consonance and tandem whereby a member of the workforce has necessarily only to be machine specific to gain access to EPHI
- ❖ These access policies are tracked through detailed log maintenance and audit trails – which are further examined by management on a routine basis.

2. ACCESS ESTABLISHMENT AND MODIFICATION (C) -§ 164.308(a)(4)(ii)(C)

Where the Access Establishment and Modification implementation specification is a reasonable and appropriate safeguard for a covered entity, the covered entity must:

“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.”

- The company has a continual review procedure for establishing access and policies and procedures are in place to validate personnel who have access to EPHI and this is reviewed on a weekly basis.

Security Awareness and Training - § 164.308(a)(5)

Regardless of the Administrative Safeguards a covered entity implements, those safeguards will not protect the EPHI if the workforce is unaware of its role in adhering to and enforcing them. Many security risks and vulnerabilities within covered entities are internal. This is why the next standard, Security Awareness and Training, is so important. Specifically, the Security Awareness and Training standard states that covered entities must:

“Implement a security awareness and training program for all members of

its workforce (including management)."

The Security Awareness and Training standard has four implementation specifications.

1. SECURITY REMINDERS (E) - § 164.308(a)(5)(ii)(A)

Where this implementation specification is a reasonable and appropriate safeguard for a covered entity, the covered entity must implement:

"Periodic security updates."

- The company has implemented a procedure whereby, at the beginning of a shift, training and advisories are conveyed and implemented regarding security updates and policies and procedures which have been changed and which need to be advised. This is a daily ongoing function.

2. PROTECTION FROM MALICIOUS SOFTWARE (E) - § 164.308(a)(5)(ii)(B)

One important security measure that employees may need to be reminded of is security software that is used to protect against malicious software. Where this implementation specification is a reasonable and appropriate safeguard for a covered entity, the covered entity must implement:

"Procedures for guarding against, detecting, and reporting malicious software."

- The company has implemented stringent security policies both by way of hardware as well as software measures to restrict unauthorized infiltration and data access.
- This includes denial of outside mail and outside access to the internet either by way of mail or by way of access to any third party sites.
- Training is imparted on a weekly basis to make workforce aware of trends in the latest malicious content so that these are recognizable at the outset even at the very primary stage.
- Needless to say, appropriate Anti-virus and anti-malware applications have been implemented and routinely updated.

3. LOG-IN MONITORING (E) - § 164.308(a)(5)(ii)(C)

Security awareness and training should also address how users log onto systems and how they are supposed to manage their passwords. Where the Log-in Monitoring implementation specification is a reasonable and appropriate safeguard for a covered entity, the covered entity must implement:

“Procedures for monitoring log-in attempts and reporting discrepancies.”

- ❖ The company has proprietary software to track and maintain audit trails of inappropriate or attempted log ins as also using of multiple user names and passwords.
- ❖ A system whereby three incorrect logins lead to the system being locked up and access denied unless authorized by both the CIO and the CSO.
- ❖ All such reset of password and logins are reviewed on a weekly basis to ascertain cause for the same and suggest remedial measures if any.
- ❖ The company's also implemented a training module to make workforce aware of how to deal with this situation as also assign password hops

4. PASSWORD MANAGEMENT(E) - § 164.308(a)(5)(ii)(D)

The last addressable specification in this standard is Password Management. Where this implementation specification is a reasonable and appropriate safeguard for a covered entity, the covered entity must implement:

“Procedures for creating, changing, and safeguarding passwords.”

- Training is imparted to workforce to commit passwords to memory and not to use simplistic combinations for memorizing the same.
- Sharing of passwords by workforce members cannot be authenticated as our proprietary security system rejects reuse of an existing password by any other member of the workforce or the same member of the workforce after its expiry

Security Incident Procedures - § 164.308(a)(6)

The next standard is Security Incident Procedures, which states that covered entities must:

“Implement policies and procedures to address security incidents.”

There is one required implementation specification for this standard.

1. RESPONSE AND REPORTING (C) - § 164.308(a)(6)(ii)

The Response and Reporting implementation specification states that covered entities must:

“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.”

- In the unlikely event that there is a security incident, a documentation trail has been put in place to ensure that all breaches of security are recorded, documented and appropriate response to each document is recorded per policies and procedures in this regard. Incidents that are covered by documentation and procedure implementations include failure to terminate an account of an erstwhile employee, restoration of databases through external media, use of inappropriately obtained passwords and physical breakins to the facility however remote. Each one of the incidents is documented by a cause, response, and effect analysis as also an escalation matrix of who would be notified when and within what period of time of the incident.

Contingency Plan - § 164.308(a)(7)

The purpose of contingency planning is to establish strategies for recovering access to EPHI should the organization experience an emergency or other occurrence, such as a power outage and/or disruption of critical business operations. The goal is to ensure that organizations have their EPHI available when it is needed. The Contingency Plan standard requires that covered entities:

“Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.”

The Contingency Plan standard includes five implementation specifications.

1. DATA BACKUP PLAN (E) - § 164.308(a)(7)(ii)(A)

The Data Backup Plan implementation specification requires covered entities to:

“Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.”

- All data fields in the EHPI are backed up contemporaneously on secure and remote servers as well as end of cycle data dumps are taken and archived in a secure and remote location on physical media. The company has made more than appropriate arrangements for storage and implementation of back up procedures.

2. DISASTER RECOVERY PLAN (E) - § 164.308(a)(7)(ii)(B)

The Disaster Recovery Plan implementation specification requires covered entities to:

“Establish (and implement as needed) procedures to restore any loss of data.”

The company has enabled best practices to ensure that DRS's are located both physically, geographically in different locations so as to ensure that there is both time zone and seismic differential in the eventuality of natural calamities. Copies of Disaster Recovery plans and implementation of recovery are available at remote sites along with detailed manuals and documentation to ensure speedy uptime and turnaround of databases

3. EMERGENCY MODE OPERATION PLAN (C) - § 164.308(a)(7)(ii)(C)

The Emergency Mode Operation Plan implementation specification requires covered entities to:

“Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.”

Contingencies plans have been put in place to ensure that all security procedures and policies are followed even in contingency situations so that data integrity is not violated for the sake of expediency. The company has erred on the side of caution to ensure that EPHI denials are at higher levels during emergency situations than normal. Detailed procedures and policies also exist with enabling on personnel to be contacted for each scenario with telephone numbers, back ups of the same as well as contingencies for invoking third party responses so as to enable workforce attention in case members of workforce are unreachable.

4. TESTING AND REVISION PROCEDURES (C) - § 164.308(a)(7)(ii)(D)

Where the Testing and Revision Procedures implementation specification is a reasonable and appropriate safeguard for the covered entity, the covered entity must:

“Implement procedures for periodic testing and revision of contingency plans.”

- The company enforces a monthly procedure where contingency plans are invoked to ensure the veracity of the system in place as also to test the integrity of the personnel implementing the same. If there are failures in the implementation of the system appropriate audits are carried out on the failures and changes in the system implemented to provide for such shortcomings

5. APPLICATION AND DATA CRITICALITY ANALYSIS (C) - § 164.308(a)(7)(ii)(E)

The last implementation specification in the Contingency Plan standard is Application and Data Criticality Analysis. Where this implementation specification is a reasonable and appropriate safeguard for the covered entity, the covered entity must:

“Assess the relative criticality of specific applications and data in support of other contingency plan components.”

The disaster recovery manuals and procedures in place provide for a sequential enabling of events to ensure that applications and data get prioritized depending on applicability and use

Evaluation - § 164.308(a)(8)

It is important for a covered entity to know if the security plans and procedures it implements continue to adequately protect its EPHI. To accomplish this, covered entities must implement ongoing monitoring and evaluation plans. Covered entities must periodically evaluate their strategy and systems to ensure that the security requirements continue to meet their organizations' operating environments. The Evaluation standard has no separate implementation specifications. The standard requires covered entities to:

“Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operations changes affecting the security of electronic protected health information, that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart [the Security Rule].”

Business Associate Contracts and Other Arrangements - § 164.308(b)(1)

The last standard in the Administrative Safeguards section is Business Associate Contracts and Other Arrangements. The organizational requirements related to this standard are discussed in more detail in § 164.314(a) of the Rule, which is covered in paper five of this series titled “Security Standards – Organizational, Policies and Procedures and Documentation Requirements.” The Business Associate Contracts and Other Arrangements standard states that:

“A covered entity, in accordance with § 164.306 [the Security Standards: General Rules], may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory

assurances, in accordance with § 164.314(a) [the Organizational Requirements] that the business associate will appropriately safeguard the information (Emphasis added).”

The standard has one implementation specification.

1. WRITTEN CONTRACT OR OTHER ARRANGEMENT (C) – § 164.308(b)(4)

Covered entities are required to:

“Document the satisfactory assurances required by paragraph (b)(1) [the Business Associate Contracts and Other Arrangements] of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of §164.314(a) [the Organizational Requirements].”

Identification of business associates have been made depending on functionality and it has been determined that access to systems is given only to pre-identified personnel of specific vendors of hardware and software who have direct dealings or access to internal systems where EPHI may reside. Security practices and procedures have also been implemented in all cases where EPHI is exposed in any manner to any third party