

HIPAA Security Gap Analysis

Per the HIPAA Security Summit Guidelines (January 2000), “qualitative measurement criteria should be developed as a tool to evaluate the current environment for each of the security standards pursuant to identification of readiness gaps and potential vulnerabilities. The measurement criteria suggested as part of the gap analysis could include rankings of current readiness weighted against HIPAA requirements, such as:

Scale:

- | | |
|---|---|
| 0 | No identified process or control |
| 1 | Informal or partial process or control |
| 2 | Process or controls implemented for many required HIPAA elements |
| 3 | Process or controls fully implemented for all required HIPAA elements |
| 4 | Process or controls exceed required HIPAA elements |

| Number | Requirement | Control Category | Rating |
|-------------------------------------|--|--|--------|
| A. Administrative Procedures | | | |
| 1. | Certification | Management | |
| 2. | Chain of Trust Partner Agreements | Management | |
| 3. | Contingency Plan | IT | |
| | a. Applications and Criticality Analysis | | |
| | b. Data Backup Plan | | |
| | c. Disaster Recovery Plan | | |
| | d. Emergency Mode Operation Plan | | |
| | e. Testing and Revision Procedures | | |
| 4. | Formal Mechanism for Processing Records | Medical Records | |
| 5. | Information Access Control | IT, Medical Records | |
| | a. Access Authorization Policy | | |
| | b. Access Establishment Policy | | |
| | c. Access Modification Policy | | |
| 6. | Internal Audit | Medical Records, Patient Relations, HR, IT | |
| 7. | Personnel Security | Safety, Risk Mgmt, Security, IT, HR | |
| | a. Access Authorizations Record Procedure | IT | |
| | b. Access Level Authorization Procedure | Security, IT | |
| | c. Maintenance Personnel Supervision Procedure | Security, IT | |
| | d. Personnel Clearance Procedure | IT, HR | |
| 8. | Security Configuration Management | IT | |
| 9. | Security Incident Procedures | Risk Mgmt, Security, IT, HR | |
| 10. | Security Management Process | IT, HR, MR | |
| | a. Risk Analysis | | |
| | b. Risk Management Policy | | |
| | c. Sanction Policy | | |
| | d. Overall Policy Stating Commitment to Security | | |
| | e. Security Management Policies and Procedures | | |
| 11. | Termination Procedures | HR, IT | |
| | a. Changing locks | | |
| | b. Removal from access lists | | |

| | | | | |
|--|----|---|----------------------|---|
| | c. | Removal of user accounts | | |
| | d. | Turning in of keys, tokens or cards that allow access | | |
| 12. | | Training | HR, IT, Safety | |
| | a. | Awareness Education | | |
| | b. | Periodic Security Reminders | | |
| | c. | User Education regarding Virus Protection | | |
| | d. | User Education in importance of monitoring log-in success/failure and how to report discrepancies | | |
| | e. | User Education in Password Management | | |
| B. Physical Safeguards | | | | |
| 1. | | Assigned Security Responsibility | Management | |
| 2. | | Media Controls | IT | |
| 3. | | Physical Access Controls | Security, IT, Safety | |
| | a. | Physical Access and Control Policy | Security, IT | |
| | b. | Need-to-Know Procedures for Personnel Access | IT | |
| | c. | Equipment Control Security | IT | |
| | d. | Facility Security Plan | Security | |
| | e. | Access Verification | IT | |
| | f. | Limited Access Policies and Procedures | IT | |
| | g. | Sign-In Procedure for Visitors | Security | |
| 4. | | Policy/Guidelines on Workstation Use | IT | |
| 5. | | Secure Workstation Location | IT | |
| 6. | | Security Awareness Training | HR, Safety, IT | |
| C. Technical Security Services | | | | |
| 1. | | Access Controls | IT | |
| 2. | | Audit Controls | IT | |
| 3. | | Authorization Controls | IT | 2 |
| 4. | | Data Authentication | IT | |
| 5. | | Entity Authentication | IT | |
| D. Technical Security Mechanism | | | | |
| 1. | | Communication/Networking Controls | IT | |
| 2. | | Network Controls | IT | |
| E. Electronic Signature* | | | | |
| 1. | | Digital Signature | IT | |
| F. Risk Assessment | | | | |

*Electronic Signature is optional at this time. If an organization chooses to use an electronic signature as part of a particular transaction, **message integrity, non-repudiation, and user authentication** must be implemented.

HIPAA Regulations Criteria

| Number | HIPAA Regulation | Criteria |
|--------------------------|--|---|
| A. Administrative | | |
| A.1. | Certification | Pending HCFA's determination of requirements and logistic for conducting certifications by an external accrediting agency, healthcare organizations should prepare to self-certify that the appropriate security measures have been implemented. |
| A.2. | Chain of Trust Partner Agreement | Ensuring the same level of security will be maintained across the continuum of electronic transmission, chain of trust partner agreements should be instituted between healthcare organizations and those third parties with whom electronic health information is exchanged. |
| A.3. | Contingency Plan | A comprehensive contingency plan for responding to a system emergency will facilitate the assurance of continuity of key business systems and operations. |
| A.3.a. | Applications and Data Criticality Analysis | Will be used to assess sensitivity, vulnerability and security of key information assets. |
| A.3.b. | Data Backup Plan | A plan that ensures recovery of information lost or inaccessible. |
| A.3.c. | Disaster Recovery Plan | A plan to enable restoration of systems and data following a catastrophic event. |
| A.3.d | Emergency Mode Operation Plan | A plan that outlines how access to the system can be obtained in an emergency. |
| A.3.e. | Testing and Revision Procedures | Enables periodic updates and audits of all contingency plans. |
| A.4. | Formal Mechanism for Processing Records | Processes should be implemented and documented to account for the flow of health information through an organization, from time of receipt or creation through manipulation and usage, storage, dissemination and transmission, and archival or disposal. |
| A.5. | Information Access Control | Identifies how different levels of access to health care information are granted. |
| A.5.a. | Access Authorization Policy | Sets the rules for who gives authorization for access to health information, who will be granted access to health information, at what locations and times, and to what types of information. |
| A.5.b. | Access Establishment Policy | Sets the rules for determining the initial right of a person or entity to have access to your information, for example, by job title. |

| | | |
|--------|---|---|
| A.5.c. | Access Modification Policy | Sets out the reasons for changing someone's established rights of access and describes the types of changes. For example, you may modify an employee's level of access to documents if she's promoted. |
| A.6. | Internal Audit | A periodic audit should be conducted on organizational systems which process health information to assess system activity and actual or potential security incidents. This initiative assumes that adequate records and logs are maintained of such activity and that reviews are conducted routinely and thoroughly. |
| A.7. | Personnel Security | These requirements are intended to ensure that all personnel (including agents and subcontractors) who have access to health information have the required authorities and clearances as determined by the organization. |
| A.7.a. | Access Authorization Records Procedure | Ensures records are kept of everyone permitted access to your system and the level of access they may have, at which locations, and at what times. |
| A.7.b. | Access Level Authorization Procedure | Determines the level of access granted to the operating and technical maintenance personnel working on or near health information. |
| A.7.c. | Maintenance Personnel Supervision Procedure | Ensures that an authorized, knowledgeable person will supervise technical maintenance personnel when they are near health information. |
| A.7.d. | Personnel Clearance Procedure | Ensures that you clear personnel before granting access by using such methods as criminal background checks and verification of references. It should include a requirement that your I.T. and HR departments discuss the access level that a newly hired person should have and confirm that the level is actually given to that person so that he can do his job. |
| A.8 | Security Configuration Management | Ensures all security systems and applications work together to create a "perimeter of security." A standard computer virus detection system is recommended throughout the organization. The policy should ensure that routine changes to security system hardware and/or software won't cause problems to the health information system (i.e. all software updates to all desktops or servers are made simultaneously). |
| A.9. | Security Incident Procedures | A formal process should be implemented to deal with identification, reporting, and ensuing response to real or potential violations of established security policy. |
| A.10. | Security Management Process | We have a process for managing security. Policies and procedures have been created that ensure that security breaches are prevented, detected, and contained and corrected when they occur. |

| | | |
|----------------------------|---|--|
| A.10.a. | Risk Analysis | We have a written analysis that determines our health information system's vulnerabilities, any potential threats to security and the risk of costs of losing system access or data. The analysis includes a review of whether the perceived threats to security are handled in a cost-effective manner. |
| A.10.b. | Risk Management Policy | Sets procedures for managing risk on an ongoing basis and reduces risk to an acceptable level. |
| A.10.c. | Sanction Policy | Specifies disciplinary sanctions for employees, agents, and contractors. |
| A.10.d. | Overall Policy Stating Commitment to Security | We have a security policy statement of information values, protection responsibilities and organization commitment for a system. States that health information is an important asset that our organization and its employees are committed to protecting and that everyone has a responsibility to protect. |
| A.10.e. | Security Management Policies and Procedures | We have a process for managing security. Policies and procedures have been created that ensure that security breaches are prevented, detected, and contained and corrected when they occur. |
| A.11. (a.,b.,c., d.) | Termination Procedures | Covers what must be done to protect your systems when a worker's employment ends or an internal or external user's access ends. They must include: procedure for changing lock combinations, procedure for the termination or deletion of someone's access privileges (should cover how to make a decision to terminate or delete access, when to do it, and how quickly it must be done), procedure for the physical eradication of someone's access privileges (should cover how access is terminated or deleted) and a procedure for turning in of any keys, tokens or cards that allow access. |
| A.12. | Training | Details how you'll train employees in protecting the confidentiality of your health information. |
| A.12.a. | Awareness Education | How will your organization provide awareness training for all personnel, including management and maintenance personnel, about your security policies and procedures and the need to keep information confidential? |
| A.12.b. | Periodic Security Reminders | What process will be used to provide periodic security reminders such as posters, screen savers, oral reminders in meetings? |
| A.12.c.,d | User Education Log-in monitoring and Virus Protection | How will we provide education on virus protection, the importance of monitoring log-in success-failure, and how to report discrepancies? |

| | | |
|-------------------------------|--|--|
| A.12.e. | User Education in Password Management | How will we provide password management education (for example, instructing employees not to write down their passwords) |
| B. Physical Safeguards | | |
| B.1. | Assigned Security Responsibility | |
| B.2. | Media Controls | Deals with the receipt and removal of hardware and/or software from your facility. It must cover topics such as access control (who may remove software and what software can be removed), accountability (maintaining a log of what software and hardware are brought in and taken out), data backup and storage, and disposal of electronic data and/or hardware. For example, if you dispose of a computer, you would want a policy detailing how to make sure that the health information was removed. |
| B.3. | Physical Access Controls | |
| B.3.a. | Physical Access and Control Policy | Ensures that physical access to your health information is limited and only properly authorized access is allowed |
| B.3.b. | Need-to-Know Procedures for Personnel Access | Allows the user access to only the information they need to perform their particular functions. |
| B.3.c. | Equipment Control | Covers the movement of hardware and software into and out of your facility and the maintenance of a record of that movement. |
| B.3.d. | Facility Security Plan | An overall plan that safeguards both the exterior and interior of your building and the equipment inside from unauthorized physical access by both employees and outsiders. Meant to give you control over whom has physical access to your health information. It may, for example, involve placing surveillance cameras in strategic places and having a plan for controlling unauthorized access to a back door. |
| B.3.e. | Access Verification | Intended to ensure that only a person with the appropriate authorization gets into your health information system. For instance, you may require the user of passwords or some form of biometric verification. |
| B.3.f. | Limited Access Policies/Procedures | Limits physical access to your information while ensuring that properly authorized access is allowed. Should detail which people may have physical access to workstations and other areas with computers. |
| B.3.g. | Sign-in Procedure for Visitors | These cover the reception and hosting of visitors at your facility, including the provision of escorts, if appropriate. |

| | | |
|--|-------------------------------------|--|
| B.4.,5. | Workstation Use and Secure Location | Gives instructions and guidelines on the use of and location and surroundings of particular computers or types of computers, based on the sensitivity of the information that can be gotten from the computers. For example, you may have stricter guidelines for a computer with HIV information on it than for others with less sensitive information. |
| B. 6. | Security Awareness Training | Each organization is required to establish security awareness training for all employees, agents, and contractors. It should be conducted at initial orientation for new personnel as on-going training, at a minimum, on an annual basis. |
| C. Technical Security Services | | Security measures exist to protect information and control individual access to information. |
| C.1. | Access Controls | Each organization is required to maintain a mechanism for access control that would restrict access to resources and allow access only by privileged entities. Mechanism should ensure that access to health information is limited to those employees with a business need to access it. |
| C.2. | Audit Controls | Each organization is required to maintain audit control mechanisms to record and examine system activity. |
| C.3. | Authorization Controls | Each organization is required to maintain mechanism for obtaining consent for the use and disclosure of health information. These controls would be necessary to ensure that only properly authorized individuals use health information. |
| C.4. | Data Authentication | Each organization is required to provide corroboration that data in its possession has not been altered or destroyed in an unauthorized manner. |
| C.5. | Entity Authentication | Corroboration that an entity is who it claims to be exists. |
| D. Technical Security Mechanism | | Security measures put in place to guard against unauthorized access to data transmitted over a communication network. |
| D.1. | Communication Networking Controls | Each organization that uses communications or networks are required to protect communications containing health information that are transmitted electronically over open networks so that they cannot be easily intercepted and interpreted by parties other than the intended recipient, and to protect their information systems from intruders trying to access systems through external communication points. |

| | | |
|--------------------------------|-------------------|--|
| D.2. | Network Controls | When using open networks, some form of encryption should be employed. One of the following must be implemented: integrity controls, message authentication access controls or encryption. If the organization employs a network, the following features must be implemented: alarm, audit trails, entity authentication and event reporting. |
| E. Electronic Signature | | Message integrity, non-repudiation and user authentication is implemented. |
| 1. | Digital Signature | |
| F. Risk Assessment | | Evaluates the significance of the vulnerabilities in the context of the organization's operations. 2 |

¹ Draft HIPAA Security Summit Guidelines, Revised January 12, 2000, page 6.

² Health Information Compliance Insider, A Plain English guide to Privacy and Security Regulations, April 2000, pages 1-10.