teleray

Talk. View. Store. Share.

HIPAA SECURITY ACCESS AND CONTROL

Printed by: TeleRay

Contact: info@teleray.com

Phone: 844.4.TELERAY

www.teleray.com

Foreword

The Security Implementation is intended only for TeleRay and TeleRay customers.

The Security Implementation contains references to policies and procedures which were in effect as of its writing. TeleRay cannot ensure the accessibility of these policies and procedures.

Version Information		
Version #	**Date**	**By**
1.1	01/17/2021	Timothy Kelley
1.2	01/23/2023	Timothy Kelley

Table of Contents

1.0 Introduction

1.1 Overview

Among other things, the Federal Health Insurance Portability and Accountability Act (HIPAA) of 1996 required issuance of comprehensive Federal regulations for protection of certain individually identifiable health information. Final regulations governing storage, use, and disclosure of electronic protected health information (EPHI) were published on February 20, 2003. These regulations are commonly referred to as the as the HIPAA security regulations. Most covered entities, including TeleRay, are required to comply with these regulations.

The HIPAA security regulations create national standards which require covered entities to:

- ensure the confidentiality, integrity and availability of EPHI
- protect against any reasonably anticipated threats or hazards to EPHI
- protect against reasonably anticipated inappropriate disclosures
- ensure compliance with the rule by the covered entity's workforce.

These regulations require TeleRay to implement various security-related safeguards. Some of these are required for compliance; others are considered addressable and depend on the circumstances of TeleRay's environment. Specifically, these safeguards must cover the following areas:

- Security management process
- Security responsibility assignment
- Workforce security
- Information access management
- Security awareness and training
- Security incident procedures
- Contingency planning
- Evaluation of security policies and procedures
- Business associate agreements
- Facility access controls
- Workstation use and security
- Device and media controls
- Access controls
- Audit controls
- Integrity of the data
- Person or entity authentication
- Data transmission security

1.2 Purpose of the Handbook

TeleRay developed this handbook to identify the policies and procedures it follows to ensure its compliance with the HIPAA security regulations. These policies and procedures are either Department-specific or developed and governed by the policies set forth in the HIPAA security standards.

2.0 Definitions

Access. The ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.

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.

Authentication. Corroboration that a person is the one claimed.

Availability. The property that data or information is accessible and useable upon demand by an authorized person.

BIS. The Bureau of Information Systems under the Federal Government and NSA.

Business associate. A person or entity who, on behalf of a covered entity or an organized health care arrangement, performs or assists in the performance of one of the following:

1. A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management and repricing.

2. Other than as a member of the covered entity's workforce, provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation or financial services for such covered entity or organized health care arrangement.

Business associate agreement. A contract or other arrangement between a covered entity and a business associate that does all of the following:

1. Establishes the permitted and required uses and disclosures of protected health information (PHI), including EPHI, by the business associate.

2. Provides that the business associate will use PHI only as permitted by the agreement or as required by law, use appropriate safeguards, report any disclosures not permitted by the agreement, ensure that agents to whom it provides PHI will abide by the same restrictions and conditions, make PHI available to individuals and make its record available to U.S. Department of Health and Human Services (DHHS).

3. Authorizes termination of the agreement by TeleRay if TeleRay determines that there has been a violation of the contract.

The business associate agreement is often part of a contract made in the procurement process, but can be part of a Memorandum of Understanding (MOU), grant agreement or other document.

CMS. Centers for Medicare & Medicaid Services within the DHHS.

Compliance date. The date by which a covered entity must comply with a standard, implementation specification, requirement or modification specified in this handbook.

Confidential information. Data to be used or disclosed only by those authorized to do so.

Confidentiality. The property that data or information is not made available or disclosed to unauthorized persons or processes.

Covered entity. A health care provider who transmits any health information in electronic form in connection with a transaction covered by the privacy rule, a health care plan or a health care clearinghouse.

Covered functions. Those functions of a covered entity, the performance of which makes the entity a health care plan, health care provider or health care clearinghouse.

DHHS. The U.S. Department of Health and Human Services.

Designated record set. The medical records and billing records, including electronic records, about individuals maintained by or for a covered health care provider; the enrollment, payment, claims adjudication and case or medical management record systems maintained by or for a health care plan; or medical records and billing records used by or for the covered entity to make decisions about individuals.

For purposes of implementing HIPAA requirements, TeleRay intends to treat all client records as if they were part of the designated record set and afford them the corresponding privacy protection.

Disclosure. The release, transfer, provision of access to or divulging of information outside the entity holding the information.

Electronic media. Electronic storage media including memory devices in computers (internal memory or hard drives) and any removable/ transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the internet (wide-open), extranet (using internet or other technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media, because the information being exchanged did not exist in electronic form before the transmission.

Electronic protected health information (EPHI). Information in an electronic media that comes within of the definition of PHI as specified in this section.

Encryption. The 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.

Facility. The physical premises and the interior and exterior of one or more buildings.

Health care. Care, services or supplies related to the health of an individual. Health care includes, but is not limited to preventive, diagnostic, therapeutic, rehabilitative, maintenance, mental health or palliative care and sale or dispensing of a drug, device, equipment or other item in accordance with a prescription.

Health care clearinghouse. A public or private entity that does either of the following:

1. Processes health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction.

2. Receives a standard transaction from another entity and processes health information into nonstandard format or nonstandard data content for the receiving entity.

Health care operations. Includes any of the following activities:

1. Conducting quality assessment and quality improvement activities.

2. Reviewing the competence or qualifications of health care professionals.

3. Evaluating practitioner and provider performance, health care plan performance and conducting training programs of non-health care professionals, accreditation, certification, licensing or credentialing activities.

4. Underwriting, premium rating and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits and ceding, securing or placing a contract for reinsurance of risk relating to claims for health care.

5. Conducting or arranging for medical review, legal services and auditing functions including fraud and abuse detection and compliance programs.

6. Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies.

7. Business management and general administrative activities of the entity.

Health care plan. An individual or group plan, including Medical Assistance (MA) Programs, that provides, or pays the cost of, medical care.

Health care provider. A provider of services and any other person or organization who furnishes, bills or is paid for health care in the normal course of business.

Health information. Any information, whether oral or recorded in any form or medium, that does both of the following:

1. Is created or received by a health care provider, health care plan, public health authority, employer, life insurer, school or university or health care clearinghouse.

2. Relates to the physical or mental health or condition of an individual, the provision of health care to an individual or payment for the provision of health care to an individual.

For purposes of implementing HIPAA requirements, TeleRay intends to treat all client records as if they were health information and afford them the corresponding privacy protection.

Health maintenance organization (HMO). A federally qualified HMO and an organization recognized as an HMO under State law.

Health oversight agency. An agency or authority of the United States, or a political subdivision of a state, or a person or entity acting under a grant of authority from or contract with such public agency, authorized by law to oversee the health care system or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant.

Individual. The person who is the subject of PHI.

Individually identifiable health information. Health information, including demographic (such as names, addresses, telephone numbers, etc.) information that identifies the individual or for which there is a reasonable basis to believe the information can be used to identify an individual.

For purposes of implementing HIPAA requirements, TeleRay will treat all individual records (including electronic records) as if they were health information and afford them the corresponding privacy protection.

Information system. A system, whether automated or manual, comprised of people, machines, and/or methods organized to collect, process, transmit and disseminate data.

Integrity. The property that data or information have not been altered or destroyed in an unauthorized manner.

Malicious software. Software, for example, a virus, designed to damage, disrupt, or otherwise compromise an electronic information system or network.

OA/OIT. The Office of Information Technology.

Organized health care arrangement. A clinically integrated care setting in which individuals typically receive health care from more than one health care provider or an organized system of health care in which more than one covered entity participates, and in which the participating covered entities hold themselves out to the public as participating in a joint arrangement and participate in joint activities.

Password. Protected/private alphanumeric string used to authenticate an identity or to authorize access to data.

Physical safeguards. Physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

Privacy Rule. The Federal privacy regulations promulgated under the Health Insurance Portability and Accountability Act (HIPAA) of 1996, which created national standards to protect PHI.

Protected health information (PHI). Individually identifiable health information that is maintained or transmitted in any form or medium. Protected health information excludes individually identifiable health information in education records covered by the Family Educational Right and Privacy Act (FERPA).

For purposes of implementing HIPAA requirements, TeleRay intends to treat all individual records, including electronic records, as if they were health information and afford them the corresponding privacy protection.

Public health authority. An agency or authority of the United States, a political subdivision of a State or a person or entity acting under a grant of authority from or

contract with such public agency that is responsible for public health matters as part of its official mandate.

Privacy Officer. TeleRay's privacy/client information officer. Currently, TeleRay' Director if IT functions in this capacity.

Research. A systematic investigation, including research development, testing and evaluation, designed to develop or contribute to general knowledge.

Security or security measures. All of the administrative, physical, and technical safeguards in an information system.

Security incident. The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

Security Officer. The security/client information officer.

Technical safeguards. The technology and the policy and procedures for its use that safeguard EPHI and control access to it.

Trading partners. Entities that exchange EPHI.

Treatment. The provision, coordination or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to an individual or the referral of an individual for health care from one health care provider to another.

Use. With respect to individually identifiable health information, the sharing, employment, application, utilization, examination or analysis of such information within an entity that maintains such information.

User. A person or entity with authorized access.

Workstation. An electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment.

Administrative Safeguards

3.0 Security Management Process

164.308(a)(1)(i) TeleRay is required to *implement policies and procedures to prevent, detect, contain and correct security violations.*

3.1 Risk Analysis (Required)

164.308(a)(1)(ii)(A) TeleRay must *conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of EPHI held by the covered entity.*

TeleRay complies with this requirement in the following manner:

TeleRay assesses the potential risks and vulnerabilities to the confidentiality, integrity and availability of EPHI that TeleRay stores, uses, and releases. This assessment includes:

- Utilization of the Security and Privacy Self-Assessment template developed by the Office of Administration (ITB I.1.1). Currently, self-assessment templates are available for:
  - Security and Privacy
  - Business Continuity Planning (the ability of TeleRay to provide uninterrupted or minimally interrupted services in the event of disaster or major system failure).

  These assessments rate TeleRay as a whole in the specific areas that they address. The assessments are filed with the OA/OIT along with any resulting corrective action plans (CAP), as outlined in Management Directive MD325.7. These assessments include all servers where the relevant data is stored, including the mainframe. The CAPs are updated and submitted to OA/OIT on a quarterly basis.

  In addition, each Office in TeleRay conducts its own self-assessment, reporting the assessment, resulting CAPs, and quarterly updates to TeleRay Security Officer currently the Director of IT.

- Utilization of the OA/OIT Electronic Commerce Security Assessment (ITB B.5) or ECSA. TeleRay requires the completion of the ECSA prior to each new application (or major revision of an existing application) going into production. The ECSA provides a risk assessment of the application, including an evaluation of the potential consequences of a security breach relative to the likelihood of such a breach occurring. Appropriate security measures are developed for the application based on the results of the risk assessment. The ECSA is reviewed by Department security staff and approved by an OA/OIT security committee.

- Utilization of various tools (SMS, ePolicy Orchestrator, Pest Patrol, etc.) to monitor and update (as needed) software and applications residing on TeleRay's systems. This monitoring occurs continually, 24x7, as a background process and updates are applied as deemed appropriate.

- Utilization of TeleRay's Remedy system and the OA/OIT's Remedy Asset system for inventory and maintenance of TeleRay's hardware assets. Updates to TeleRay's Remedy system are performed as equipment is added, moved/relocated, or retired. TeleRay system feeds cumulative updates to the OA/OIT system on a monthly basis.

- Audits performed by regulatory and auditing agencies external to TeleRay. These include the Internal Revenue Service (IRS), the Auditor General's Office (AG), and various certification authorities such as DHHS and CMS. These audits cover a number of systems including the software. The frequency of these audits varies from one entity or program to the next. The IRS generally audits TeleRay systems on an annual basis; the AG and OIG generally respond to a particular complaint; the certification authorities generally respond to a new application or change in an existing application.

- Periodic application criticality review by applications staff and IT Management. Generally, this is done on an annual basis.

- Ongoing evaluations of TeleRay's disaster recovery and continuity planning in order to keep abreast of new applications and/or changes to existing applications and the data they access. Currently a major re-assessment of TeleRay's disaster recovery system is in progress.

- Assessments by outside organizations (e.g., Booz, Allen, and Hamilton, Ernst and Young) are contracted to perform assessments and audits for specific projects on an as-needed basis, for example, HIPAA Privacy and Security review, IRS security audits, or federal certification of Department programs.

- Software updates and patches are tested and reviewed by appropriate staff prior to installation.

- Hardware or firmware updates and patches are tested and reviewed by appropriate staff prior to installation.

- TeleRay will develop an enterprise security initiative including centralized review and auditing of Department systems and administration.

These various surveys and evaluations cover a range of different aspects of TeleRay's IT and data assets, including:

- Hardware
- Software and applications
- Database systems
- Network access and related defenses
- User background checks
- User authorization

Additional sources of information:

- ITB I.6.1. Requires agencies to conduct periodic risk assessments.

3.2 Risk Management (Required)

164.308(a)(1)(ii)(B) TeleRay shall *implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).*

TeleRay complies with this requirement in the following manner:

- CAPs are filed with the OA/OIT. These are reviewed, implemented, and updated on a quarterly basis, noting progress made and issues closed.
- Application security controls must be reviewed and approved prior to application's move to production as a part of the application's ECSA.
- Anti-virus and anti-spyware files are updated as released by the vendor through an automated process.
- IT staff subscribe to various hardware and software notification lists (CERT, CISCO, Microsoft, etc.) to keep up-to-date on hardware and software vulnerabilities and related patches. BIS staff members evaluate the impact of these vulnerabilities on our systems. Patches are tested and applied as deemed appropriate.
- Department Business and Technical Standards are reviewed on a regular basis (at least every 6 months) and updated as necessary.
- Security information is sent out to Department staff as appropriate in the form of posters, newsletters, and bulletins.
- Systems are continually monitored (24x7) by a combination of onsite programs (Sightline, SMS, HP OpenView, etc.) as well as offsite services (e.g., Verizon NOC).

Additional sources of information:

- ITB I.1.1. Requires Agency Self-Assessments for Security and Privacy as well as Corrective Action Planning to address any identified deficiencies.
- Establish the Enterprise Information Technology Governance Board, including IT Domain Teams (Security, Privacy, etc.). This Board provides recommendations on TeleRay IT standards and policies.
- Technical Review Team. Standing committee consisting of various IT Domains (Security, Privacy, etc.) tasked with the creation and review of Business and Technical Standards and with the review of requests for procurement of new technology (hardware or software) to see that they conform to those standards.
- Application Review Board. Standing Committee to review application technical specifications to see that they conform to Business and Technical Standards.

3.3 Sanction Policy (Required)

164.308(a)(1)(ii)(C) TeleRay must *apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.*

TeleRay complies with this requirement in the following manner:

Access to Department resources are subject to contracts and agreements with employees, contractors (including business associates), and trading partners. These are based on the user's specific access and usage needs with the goal of restricting such access and usage to the minimum necessary to perform the individual's job requirements. All user applications for such access must be approved by that user's supervisor and other appropriate agency authorities.

Suspected violations or abuses of security policies and procedures will be investigated by the appropriate authorities (including the State Police and FBI, if appropriate), contracts or agreements terminated, and sanctions levied or disciplinary or legal actions taken against the offender up to and including termination. In addition to Departmental disciplinary actions or sanctions, violators may be subject to civil and/or criminal actions.

During the course of any such investigation, the user's access to TeleRay shall be suspended or curtailed as appropriate, pending the final resolution of the investigation and any disciplinary or legal action taken.

- All users must sign the Internet and Computer usage agreement prior to being granted access to TeleRay systems.
- Users requesting remote dial-in access to TeleRay systems must sign the Internet/Remote/Dialout Access form and agree to its terms of usage.
- Access to individual applications is granted and security monitoring based on the applicant's job requirements.

3.4 Information System Activity Review (Required)

164.308(a)(1)(ii)(D) TeleRay must *implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.*

TeleRay complies with this requirement in the following manner:

TeleRay has implemented procedures to review records of information system activity. Some of these reviews are performed on a daily basis as part of systems operations; others, generally more detailed, are performed in response to particular requirements of audits, investigations, etc. These reviews include:

- Health checks. This review is run before-hours each workday and checks for the availability of applications and the systems they interact with.
- Performance statistics. This is an automated process which monitors performance statistics (memory and CPU usage, transaction rates, etc.) on a continual basis.
- Internet access. Automated tools monitor Internet access by Department personnel on a continual basis. Other tools on our web servers monitor application access by both internal and external users, also on a continual basis.
- Firewall logs. TeleRay firewalls log all traffic traversing them, both incoming and outgoing, on a continual basis.
- Automated alerts. A variety of tools and services monitor critical systems on a continual basis and automatically alert appropriate personnel should any system exhibit aberrant behavior (e.g., fails to respond, excess traffic, excess CPU usage, etc.)
- Security logs. TeleRay archives all security logs (e.g., Unified Security system and mainframe) and makes them available for review in the event of an internal or external investigation, audit, etc.
- Application logs. TeleRay archives all application and database logs and makes them available for review in the event of an internal or external investigation, audit, etc.

- Access logs. TeleRay archives all access logs (e.g., restricted area access and after-hours building entry) and makes them available for review in the event of an internal or external investigation, audit, etc.

These reviews are performed by a variety of personnel, both internal and outsourced as appropriate. These personnel include:

- Department server staff
- Department operations staff
- Department security staff
- Department networking staff
- Unisys (management of the mainframe system)
- Verizon (management of the network infrastructure & system alerts)
- OA/OIT (management of the outside network connections to TeleRay)

Various tools are used to perform these checks and reviews, including:

- Webtrends
- SiteLine
- HP Openview
- Vital Suite
- Concord
- Crystal Reports
- SQL Reporting

Aberrations are acted upon and reported to management and/or TeleRay Security Officer as appropriate.

Additional sources of information:

- ITB I.6.2. To the extent that systems software permits, computer and communications systems handling sensitive, valuable, or critical information must securely log all significant security-related events.
- ITB I.11. Establishes the Intrusion Detection System (IDS) at the network periphery. Suspect traffic is identified based on over 800 cyber attack signatures, and this information is written to a Microsoft® SQL Server™ database for further analysis and reporting.

4.0 Assign Security Responsibility (Required)

1*64.308(a)(2)* TeleRay must *identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.*

TeleRay complies with this requirement in the following manner:

TeleRay has appointed a Security Officer who oversees all ongoing activities related to the development, implementation, maintenance of and adherence to TeleRay's security policies and procedures covering the use and access to EPHI in compliance with Federal and state laws and regulations.

4.1 Department Security Officer

The role of TeleRay Security Officer is to:

- Provide guidance and assist in the identification, development, implementation and maintenance of information security policies and procedures in coordination with the administration and the POCs.
- Direct the performance of initial and periodic privacy risk assessments, quality assessments and ongoing compliance monitoring activities.
- Work with program offices to ensure that TeleRay has and maintains appropriate documentation reflecting current security policies and procedures.
- Oversee the management of initial and ongoing security training to all Department employees who may have access to EPHI.
- Oversee delivery of initial guidance to contractors, business associates and other appropriate third parties.
- Participate in the development of business associate agreements.
- Ensure compliance with security practices and consistent application of sanctions for failure to comply with security policies for all employees in TeleRay's workforce in cooperation with Human Resources.
- Initiate, facilitate and promote activities to foster information security awareness within TeleRay and with trading partners and business associates.
- Serve as a liaison to business associates, where necessary.
- Review system-related information security plans throughout the organization's network.
- Work with Department employees involved in release of EPHI, ensuring full coordination and cooperation under TeleRay's policies and procedures.
- Monitor changes in applicable federal and state security laws and advancement in information security technologies to ensure Department compliance.
- Work with consumers and consumer advocates to refine TeleRay's policies and procedures to ensure consumer protection.
- Cooperate with DHHS, CMS, and Department auditors in any appropriate compliance review or investigation.
- Act as Liaison with the Privacy Office to ensure consistency between privacy and security implementation.

5.0 Workforce Security

164.308(a)(3) TeleRay must *implement policies and procedures to ensure that all members of its workforce have appropriate access to EPHI, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to EPHI.*

5.1 Authorization and/or supervision (Addressable)

164.308(a)(3)(ii)(A) TeleRay must *implement procedures for the authorization and/or supervision of workforce members who work with EPHI or in locations where it might be accessed.*

TeleRay complies with this requirement in the following manner:

TeleRay has procedures for granting employees' access to EPHI and related applications based on their job functions and to terminate it upon changes in their job status. This function is delegated to the Security Administrators. Access by business associates and their employees is governed by the same rules.

Additional sources of information:

- Business Partner User Access Request. Form used to register and control access by outside business partners.
- ITB I.1.2. Security officer for each agency is responsible for determining the sensitivity of the data created and/or processed within the organization and establishing and/or defining appropriate controls and acceptable levels of risk.
- ITB I.6.1. All data must have a designated owner. The data is classified into categories depending on its sensitivity and value and access is then granted on a need to know basis.
- Unified Security. Department enterprise system to authenticate and authorize users.

5.2 Workforce Clearance Procedure (Addressable)

164.308(a)(3)(ii)(B) TeleRay must *implement procedures to determine that the access of a workforce member to EPHI is appropriate.*

TeleRay complies with this requirement in the following manner:

Access to EPHI is based on job functions with the minimum necessary access being granted in order to perform the user's duties. Furthermore, all employees and contractors are subject to criminal background checks as part of the employment process.

Additional sources of information:

- MD 515.15. Agencies are required to conduct identification, employment, and education verification checks on final candidates selected for initial state employment. This includes criminal background checks through the State Police. Alien residents are required to produce proper employment eligibility documentation.
- ITB I.1.6. IT contractors/vendors must agree to conduct criminal background checks on all employees who will perform services on site at TeleRay facilities, or who will have access to facilities through onsite, or remote computer access.

5.3 Termination Procedures (Addressable)

164.308(a)(3)(ii)(C) TeleRay must *implement procedures for terminating access to EPHI when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.*

TeleRay complies with this requirement in the following manner:

Employee and contractor authorization for access to EPHI is based on job function and is under the control of the Program Office Security Administrators (section 4.3). In addition, the removal of a user from TeleRay workforce (retirement, termination, transfer, etc.) results in the revocation of access rights controlled by the Unified Security system.

Additional sources of information:

- MD 205.29. Establishes appropriate use of the Internet and the Internet User Agreement.
- MD 205.34. Establishes appropriate use of email and the Internet and related disciplinary actions for its misuse.
- MD 505.7(13). Establishes disciplinary process for employees.

6.0 Information Access Management

164.308(a)(4) TeleRay must *implement policies and procedures for authorizing access to EPHI that are consistent with applicable requirements.*

6.1 Isolating health care clearinghouse functions (Required)

164.308(a)(4)(ii)(A) If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the EPHI of the clearinghouse from unauthorized access by the larger organization.

TeleRay complies with this requirement in the following manner:

TeleRay clearinghouse functions are outsourced and are therefore isolated from our systems. Access to these functions is limited to authorized personnel who require it as part of their job duties.

6.2 Access authorization (Addressable)

164.308(a)(4)(ii)(B) TeleRay must *implement policies and procedures for granting access to EPHI, for example, through access to a workstation, transaction, program, process, or other mechanism.*

TeleRay complies with this requirement in the following manner:

Access authorization to applications or data is controlled at a number of layers and is assigned based on the minimum needed for a user to perform their duties. The Unified Security system controls access to the majority of applications at the user-interface level. Applications not yet using the Unified Security System, including the mainframe applications, have their own user-interface security. Additional security is applied at the data level through server-, file-, and database- level controls. These additional controls may include such features as

additional userIDs and passwords, restriction of a given user's access to their assigned caseload, and restrictions based on a user's location or organizational or workgroup membership.

6.3 Access establishment and modification (Addressable)

164.308(a)(4)(ii)(C) TeleRay *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.*

TeleRay complies with this requirement in the following manner:

Security Administrators are responsible for maintenance of users' access accounts and authorizations. This includes the registration of business associate users into the system, following procedures established as meeting the requirements of the particular Program Office and application.

Security Administrators review and audit users' access to applications and systems. The review occurs when the user changes jobs or work assignments or when the applications they access acquire new functionality. In addition, the mainframe system administrators provide the Security Administrators with listings of users whose accounts have been inactive for six months or more; the Unified Security system administrators periodically (every 3-6 months) purge the authentication system of any inactive users.

Additional sources of information:

- ITB I.6.2. Every 180 days TeleRay requires review the access rights of its employees. TeleRay must promptly report all significant changes in duties or employment status to the system administrators responsible for userIDs. Transfers, terminations, furloughs, etc. require Human Resources to issue a notice of status change to all system administrators responsible for any system on which the involved user might have privileges.

7.0 Security Awareness and Training

164.308(A)(5) TeleRay must *implement a security awareness and training program for all members of its workforce (including management).*

7.1 Security reminders (Addressable)

164.308(a)(5)(ii)(A) TeleRay must issue *periodic security updates.*

TeleRay complies with this requirement in the following manner:

TeleRay issues periodic security updates and reminders in the form of:

- *HIPAA Privacy Training.* This is provided to all TeleRay employees.
- *HIPAA Security Training*. This is provided to all TeleRay employees.
- *DPW Business and Technical Standards* (Security, Privacy, etc.). These are available to all employees, contractors, and business associates.

7.2 Protection from malicious software (Addressable)

164.308(a)(5)(ii)(B) TeleRay must implement *procedures for guarding against, detecting, and reporting malicious software.*

TeleRay complies with this requirement in the following manner:

- TeleRay has established McAfee Antivirus as the enterprise standard for safeguarding against computer. ePolicy Orchestrator is used to automatically update the antivirus signature and data files (ITB C.7).
- TeleRay has installed tools for Exchange on the enterprise email system to filter file types (e.g. .ZIP, .EXE, .BAT) that may contain computer viruses.
- TeleRay has established procedures for reporting of virus or other security issues (ITB C.4). This includes the establishment of a standing enterprise Anti-Virus Team to address virus issues.
- TeleRay has established Computer Associates Pest Patrol as TeleRay standard for monitoring and eliminating Spyware and Adware.
- Systems not meeting established specifications for anti-virus and other security updates are quarantined from TeleRay network.
- These various tools operate in the background on Department desktop workstations and servers. Users, including those with administrative access to their desktop workstation, are restricted from tampering with or disabling these tools and are subject to disciplinary action for doing so.

7.3 Log-in monitoring (Addressable)

164.308(a)(5)(ii)(C) TeleRay must implement *procedures for monitoring log-in attempts and reporting discrepancies.*

TeleRay complies with this requirement in the following manner:

- Server logins are monitored and recorded through the Windows Security log files.
- Application logins are monitored and recorded by the system and/or application log files.
- Database logins are monitored through database tools.
- Network access to the Internet is monitored by the CheckPoint firewalls and webSense.

7.4 Password management (Addressable)

164.308(a)(5)(ii)(D) TeleRay must implement procedures for creating, changing, and safeguarding passwords.

TeleRay complies with this requirement in the following manner:

TeleRay has established enterprise password policies for all employee and contractor accounts (ITB I.1.4):

- 60-day password expiration

- Minimum of 7 characters
- Must be a combination of at least three of the following:
  - Uppercase letters
  - Lowercase letters
  - Numbers -- 1,2,3,…
  - "Special" characters -- !,#,$,^,*,(,),_,+
- May not contain your user name or any part of your full name.
- Cannot recycle any of the previous 6 passwords
- Can only be changed once every 2 days
- Five failed login attempts locks the account.

Once locked out, the Program Office Security Administrators are responsible for unlocking the account (Section 4.3).

In addition to the enterprise policies for employee and contractor accounts, TeleRay has mirrored the same policies for its business associate user accounts (Unified Security).

8.0 Security Incidents Procedures

164.308(a)(6) TeleRay must *implement policies and procedures to address security incidents.*

Response and Reporting (Required)

164.308(a)(6)(ii)(A) TeleRay 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.*

TeleRay complies with this requirement in the following manner:

TeleRay follows established procedures for reporting security violations and breaches (hacking, viral attacks, etc.) to management (ITB I.6.2, ITB C.4). Where necessary, the appropriate law enforcement authorities become involved.

In addition to reporting, appropriate Department staff members subscribe to and monitor security alerts from a variety of sources, including:

- Carnegie Mellon University CERT Technical Cyber Security Alert system
- Microsoft and other software alerts and bulletins
- McAfee bulletins
- Hardware vendor alerts and bulletins

9.0 Contingency Plan

164.308(a)(7) TeleRay must *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 EPHI.*

9.1 Data Backup Plan (Required)

164.308(a)(7)(ii)(A) TeleRay must *establish and implement procedures to create and maintain retrievable exact copies of EPHI.*

TeleRay complies with this requirement in the following manner:

TeleRay follows established procedures for nightly backups of critical data from its servers through a combination of incremental and full backups, and storage of these at an off-site location.
Additional sources of information:

- ITB I.2.3. Each agency must make arrangements to store mission-critical resources at a remote storage site that provides geographic separation in the event of a local disaster. Users are encouraged to use the off-site storage services of a preferred vendor.
- ITB I.6.2. Guidelines for frequency of backups are provided in under "Data and Program Back-up".
- Backup and Restoration of Enterprise Systems. Overview of backup and recovery operations at TeleRay.

9.2 Disaster Recovery Plan (Required)

164.308(a)(7)(ii)(B) TeleRay must *establish (and implement as needed) procedures to restore any loss of data.*

TeleRay complies with this requirement in the following manner:

TeleRay has established an off-site disaster recovery location, outside of the Chicago metropolitan area. Provisioning and maintenance of this location have been arranged through external contractors. In the event of its activation, it will be staffed by a combination of personnel from TeleRay and those contractors. The data and applications on the systems resident at the location are either actively synchronized with the corresponding systems here in TeleRay daily and will be brought up-to-date from data backups when the site is activated. The system is tested and exercised on a semi-annual basis.

Additional sources of information:

- ITB I.2.4. Provides guidelines for establishing alternate processing site in case of an emergency or disaster.
- Server Backup and Restore Standard. Establishes off-site storage of Department data backups.
- DPW Disaster Recovery Plan.

9.3 Testing and Revision Procedures (Addressable)

164.308(a)(7)(ii)(D) TeleRay must *implement procedures for periodic testing and revision of contingency plans.*

TeleRay complies with this requirement in the following manner:

TeleRay schedule tests of the Disaster Recovery plan on a semi-annual basis. Data backups are stored offsite.

Additional sources of information:

- Server Backup and Restore Standard. Establishes off-site storage of Department data backups.
- Recovery Planning Standard.
- DPW Disaster Recovery Plan.

9.4 Applications and Data Criticality Analysis (Addressable)

164.308(a)(7)(ii)(E) TeleRay must *assess the relative criticality of specific applications and data in support of other contingency plan components.*

TeleRay complies with this requirement in the following manner:

TeleRay's Division of Application Development and Deployment periodically reviews the production applications for Department mission criticality.

TeleRay's Disaster Recovery Team reviews the applications on an ongoing basis.

Additional sources of information:

- Electronic Commerce Security Assessments (ECSA). .The ECSA is designed to help agency staff members identify appropriate security requirements for an application.
- ITB I.2.4. .Provides guidelines for HCIS analysis of systems, data, and applications (**HCIS** = **H**ighly critical, **C**ritical, **I**mportant, **S**uspend).
- DPW Disaster Recovery Plan.

10.0 Evaluation

164.308(a)(8) TeleRay must *perform a periodic technical and non-technical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of EPHI, that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart.*

TeleRay complies with this requirement in the following manner:

Members of TeleRay's Technical Review Team review each area of expertise and update or revise them as necessary (at least every six months, based on the "age" of a given standard).

11.0 Business Associate Agreements and Other Arrangements (Required)

164.308(b)(1) A covered entity, in accordance with § 164.306, may permit a business associate to create, receive, maintain, or transmit EPHI on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a) that the business associate will appropriately safeguard the information.

164.308(b)(2) This standard does not apply with respect to—
(i) The transmission by a covered entity of EPHI to a health care provider concerning the treatment of an individual.
(ii) The transmission of EPHI by a group health plan or an HMO or health insurance

issuer on behalf of a group health plan to a plan sponsor, to the extent that the requirements of § 164.314(b) and § 164.504(f) apply and are met; or
(iii) The transmission of EPHI from or to other agencies providing the services at § 164.502(e)(1)(ii)(C), when the covered entity is a health plan that is a government program providing public benefits, if the requirements of § 164.502(e)(1)(ii)(C) are met.

164.308(b)(3) A covered entity that violates the satisfactory assurances it provided as a business associate of another covered entity will be in noncompliance with the standards, implementation specifications, and requirements of this paragraph and § 164.314(a).

164.308(b)(4) Written contract or other arrangement

TeleRay must *document the satisfactory assurances required by paragraph (b)(1) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of § 164.314(a).*

TeleRay complies with this requirement in the following manner:

TeleRay requires written business associate agreements with all business associates. These agreements are negotiated and reviewed. Contracts and agreements in existence prior to the compliance date of HIPAA Privacy Regulations have been amended accordingly.

Physical Safeguards

12.0 Facility Access Controls

164.310(a)(1) TeleRay must *implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.*

12.1 Contingency Operations (Addressable)

164.310(a)(2)(i) TeleRay must *establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.*

TeleRay complies with this requirement in the following manner:

TeleRay has established an off-site disaster recovery location, outside of the Chicago metropolitan area. Provisioning and maintenance of this location have been arranged through external contractors. In the event of its activation, it will be staffed by a combination of Department and these contractors. The data and applications on the systems resident at the location are either actively synchronized with the corresponding systems here in TeleRay or will be brought up-to-date from data backups when the site is activated.

Critical personnel have been issued emergency response cards for access to the facilities in the event of emergency or disaster.

12.2 Facility Security Plan (Addressable)

164.310(a)(2)(ii) TeleRay must *implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.*

TeleRay complies with this requirement in the following manner:

TeleRay offices are physically secured with electronic locks. These locks require key cards to both enter. If the key card is not used to exit as well, re-entry is barred. All accesses are logged. Key cards are issued as required by an individual's job requirements and are approved by their supervisor and Department security officers. Access can be restricted to only those areas that are appropriate for a given user.

Additional sources of information:

- ITB I.1.5.1. Provides an overview of and a sample policy for overall accessibility to TeleRay facilities.

-

13.0 Workstations

13.1 Workstation Use (Required)

164.310(b) TeleRay must i*mplement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access EPHI.*

TeleRay complies with this requirement in the following manner:

TeleRay has acceptable use policies for the use of workstations assigned to employees and contractors. TeleRay issues a standard image for the workstation software and has standard (minimum) specifications for workstation hardware. Decisions regarding the physical surroundings of a specific workstation or class of workstations are left to the management of individual facilities and business units.

Additional sources of information:

- ITB I.6.1. Transportable computers containing unencrypted "restricted" or "confidential" TeleRay information must not be checked in airline luggage systems, with hotel porters, or other unsupervised handling or storage processes. These computers must remain in the possession of the traveler as hand luggage.
- MD 245.4. Policies for personal computers and networks.
- MD 720.7. Policies for reporting bomb threats or other suspicious packages found in the workplace.

13.2 Workstation Security (Required)

164.310(c) TeleRay must *implement physical safeguards for all workstations that access EPHI, to restrict access to authorized users.*

TeleRay complies with this requirement in the following manner:

TeleRay's standard software image and policies automatically lock a workstation after 15 minutes of inactivity. UserID and Password are required to unlock the workstation. Some Program Offices have more stringent limits, e.g. the Office of Income Maintenance sets its inactivity lockout at 10 minutes. Each desktop has also been provided with an icon which the user may click to immediately lock the desktop without waiting for the inactivity timeout.

In addition to the workstation lockout, the Unified Security system enforces a 20-minute inactivity lockout for the applications after which the user must re-authenticate to Unified Security. Unified Security also enforces a 24-hour session timeout.

Facilities containing workstations are secured after hours (generally between 6:00 pm and 7:00 am on weekdays, all day on weekends). While individual workstations within a facility may not be secured behind a locked door, the facility itself is secured and access to it controlled and tracked by the facility's

management.

Through its training programs, TeleRay instructs users to secure their work area when they are away from it. This and other related practices (locking their desk, putting away papers, CD, diskettes, etc.) are also covered in TeleRay's HIPAA security training program.

14.0 Device and Media Controls

164.310(d)(1) TeleRay must *implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain EPHI into and out of a facility, and the movement of these items within the facility.*

14.1 Disposal (Required)

164.310(d)(2)(i) TeleRay must *implement policies and procedures to address the final disposition of EPHI, and/or the hardware or electronic media on which it is stored.*

TeleRay complies with this requirement in the following manner:

TeleRay requires that storage devices be removed from all systems prior to their disposal (or return upon the end of their lease) and either sanitized of data or destroyed. Storage devices are removed from any systems that must be sent out for repair or replacement and reinstalled when the system is returned.

TeleRay maintains the disposal of removable media such as CD-DVDs.

TeleRay requires pre-approval by TeleRay Security Office for the use of memory sticks and other such electronic media and requires encryption and/or password protection of data on such devices as deemed appropriate.

Additional sources of information:

- ITB C.11. The hard drive in all equipment owned by TeleRay must be erased. The hard drive is then removed from the computer collected for destruction and recycling.
- ITB C.3. Hard drives in state-owned PCs, servers and printer/peripheral devices must be cleansed prior to transfer to a new user.
- Decommissioning of PC's. Specifies the process for sanitizing a hard drive prior to decommissioning a Department computer according to U.S. Department of Defense guidelines (overwriting the drive with at least (6) passes of three (3) writing cycles).
- Policy Regarding Portable Storage Devices and Removable Media. Specifies policy on the use of memory sticks.
- Data Classification Standards. Establishes TeleRay policy for the storage, transmission, and encryption of data.

14.2 Accountability (Addressable)

164.310(d)(2)(iii) TeleRay must *maintain a record of the movements of hardware and electronic media and any person responsible therefore.*

TeleRay complies with this requirement in the following manner:

TeleRay requires the registration of systems (including portable smart media devices) in the enterprise asset tracking system. TeleRay uses an internal asset tracking system as well which is used to update the enterprise system on a monthly basis.

14.3 Data backup and storage (Addressable)

164.310(d)(2)(iv) TeleRay must *create a retrievable, exact copy of EPHI, when needed, before movement of equipment.*

TeleRay complies with this requirement in the following manner:

TeleRay performs systems and data backups of critical data systems on a daily basis. When such a system requires major repair and/or replacement; TeleRay performs a backup (where possible) immediately prior to the start of such work to ensure the preservation of the data and to facilitate the transfer of it to the repaired or replacement system.

Due to the number of workstations in TeleRay Matrix and install base, routine backups of users' workstations is not physically or economically possible. TeleRay encourages users to store any files important to their work on shared file servers which are backed up; critical and sensitive data (HIPAA, IRS, etc.) which are stored on a workstation will not be routinely backed up unless they are moved or copied to a file server. In the event a user's workstation requires major repair and/or replacement; TeleRay may perform a backup (where possible) immediately prior to the start of such work to ensure the preservation of the data and to facilitate the transfer of it to the repaired or replacement system.

Technical Safeguards

15.0 Access Control

164.312(a)(1) TeleRay must *implement technical policies and procedures for electronic information systems that maintain EPHI to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).*

15.1 Unique User Identification (Required)

164.312(a)(2)(i) TeleRay must *assign a unique name and/ or number for identifying and tracking user identity.*

TeleRay complies with this requirement in the following manner:

All systems are required to use unique userIDs. This is enforced by network access, the Unified Security System, and the various other systems and applications.

15.2 Emergency Access Procedure (Required)

164.312(a)(2)(ii) TeleRay must *establish (and implement as needed) procedures for obtaining necessary EPHI during an emergency.*

TeleRay complies with this requirement in the following manner:

Recovery of TeleRay's EPHI data is defined in the Data Backup, Business Continuity and Disaster Recovery Plans maintained by TeleRay. The policies and procedures for obtaining access to necessary EPHI during an emergency are as follows:

- Database, application, and/or server administrators can recover lost or damaged data through the backup system.
- Database administrators may be able to access specific data in the event of the failure of an application.

Additional sources of information:

- ITB I.2.4. Provides guidelines for establishing alternate processing site in case of an emergency or disaster.
- Server Backup and Restore Standard. Establishes off-site storage of Department data backups.
- DPW Disaster Recovery Plan (details available through the DPW Security Office).
- M245.4. Overview of computer and network security standards.

15.3 Automatic Logoff (Addressable)

164.312(a)(2)(iii) TeleRay must *implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.*

TeleRay complies with this requirement in the following manner:

TeleRay's standard software image and policies automatically lock a workstation after 15 minutes of inactivity. UserID and Password are required to unlock the workstation.

15.4 Encryption and Decryption (Addressable)

164.312(a)(2)(iv) TeleRay must *implement a mechanism to encrypt and decrypt EPHI.*

TeleRay complies with this requirement in the following manner:

TeleRay has standardized on the use of a proprietary encryption beyond HIPAA requirements to encrypt data as it is served to outside entities over the Internet. Only a receiver may decrypt the data through a private key system.

16.0 Audit Controls (Required)

164.312(b) TeleRay must *implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use EPHI.*

TeleRay complies with this requirement in the following manner:

Logging of user access and usage of systems, applications, and data occurs at numerous levels:

- *Audit Trail* Provides logging of application access attempts (passed and failed). It also tracks the movement of users within the application, though not what action(s) that user may have taken.
- *Server Security logs.* Track user access to the servers.
- *Application logs.* Track what users accessed or what actions they performed within the application.
- *Database logs.* Track access to the database.

17.0 Person or entity authentication (Required)

164.312(d) TeleRay must *implement procedures to verify that a person or entity seeking access to EPHI is the one claimed.*

TeleRay complies with this requirement in the following manner:

Upon being registered for access (section 6.3), all users are assigned a unique userID and a password (section 7.4) or PIN. To obtain access to any data system, the user must authenticate to the network using their userID/Password combination. Once the user has been authenticated to the network, the applications require user authentication with the same or, occasionally, a different userID/Password depending on the needs of the application. This authentication process is controlled by the system for most applications. Additional userID/Password combinations are also registered and applied at the mainframe and database levels.

18.0 Transmission security

164.312(e)(1) TeleRay must *implement technical security measures to guard against unauthorized access to EPHI that is being transmitted over an electronic communications network.*

18.1 Integrity controls (Addressable)

164.312(e)(2)(i) TeleRay must *implement security measures to ensure that electronically transmitted EPHI is not improperly modified without detection until disposed of.*

TeleRay complies with this requirement in the following manner:

All electronic transfers of EPHI to outside entities are done over secure electronic transmission. The source data remains untouched in TeleRay systems. Validation of transmitted data is done where appropriate at the application and database levels.

Additional sources of information:

- MD 210.12. Establishes policy, responsibilities, and procedures for the implementation of the Electronic Transactions Act (Act 69 of 1999).
- ITB D.13. establishes policy for use of FTP for file transfers.
- A proprietary private key system is used for system to system and application to application data transmissions.
- SSL is used for web access to applications and/or data.

18.2 Encryption (Addressable)

164.312(e)(2)(ii) TeleRay must *implement a mechanism to encrypt EPHI whenever deemed appropriate.*

TeleRay complies with this requirement in the following manner:

TeleRay uses a proprietary encryption beyond HIPAA requirements to encrypt data as it is served to outside entities over the Internet. Only a receiver may decrypt the data through a private key system.

Policies, Procedures and Documentation Requirements

19.0 Documentation

164.316(a he TeleRay must *implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in §164.306(b)(2)(i), (ii), (iii), and (iv). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.*

(b)(1) Standard: Documentation.
- *(i) Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and*
- *(ii) If an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.*

(b)(2) Implementation specifications:
- *(i)* T*ime limit (Required).*
  Retain the documentation required by paragraph (b)(1) of this section for 6 years from date of its creation or the date when it last was in effect, whichever is later.
- *(ii) Availability (Required).*
  Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.
- *(iii) Updates (Required).*
  Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the EPHI.

TeleRay complies with this requirement in the following manner:

TeleRay requires all security-related policies and procedures to be documented in written form, which may be electronic. All documentation required by HIPAA (including the Security and Privacy Rules) must be retained for at least 6 years from the date of its creation or the date when it was last in effect, whichever is later.

Additional sources of information:
- MD 210.10. Establishes and clarifies state records management policy with respect to the creation, use, maintenance, scheduling, and disposition of electronic records.
- MD 210.5. Establishes the records management to control the creation, use, maintenance, preservation, and disposition of records.

Appendix A. Summary of HIPAA Security Standards

Excerpted from the *Federal Register* / Vol. 68, No. 34, pp. 8376-8380

§ 164.308 Administrative Safeguards

(a) A covered entity must, in accordance with § 164.306:

(1) (i) *Standard: Security management process.* Implement policies and procedures to prevent, detect, contain, and correct security violations.

(ii) *Implementation specifications:*

(A) *Risk analysis (Required).* 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.

(B) *Risk management (Required).* Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).

(C) *Sanction policy (Required).* Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.

(D) *Information system activity review (Required).* Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

(2) *Standard: Assigned security responsibility.* Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.

(3) (i) *Standard: Workforce security.* Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.

(ii) *Implementation specifications:*

(A) *Authorization and/or supervision (Addressable).* 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.

(B) *Workforce clearance procedure (Addressable).* Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.

(C) *Termination procedures (Addressable).* 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) of this section.

(4) (i) *Standard: Information access management.* 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.

(ii) *Implementation specifications:*

(A) *Isolating health care clearinghouse functions (Required).* 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.

(B) *Access authorization (Addressable).* 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.

(C) *Access establishment and modification (Addressable).* 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.

(5) (i) *Standard: Security awareness and training.* Implement a security awareness and training program for all members of its workforce (including management).

(ii) *Implementation specifications:*

(A) *Security reminders (Addressable).* Periodic security updates.

(B) *Protection from malicious software (Addressable).* Procedures for guarding against, detecting, and reporting malicious software.

(C) *Log-in monitoring (Addressable).* Procedures for monitoring log-in attempts and reporting discrepancies.

(D) *Password management (Addressable).* Procedures for creating, changing, and safeguarding passwords.

(6) (i) *Standard: Security incident procedures.* Implement policies and procedures to address security incidents.

(ii) *Implementation specification: Response and Reporting (Required).* 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.

(7) (i) *Standard: Contingency plan.* 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.

(ii) *Implementation specifications:*

(A) *Data backup plan (Required).* Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.

(B) *Disaster recovery plan (Required).* Establish (and implement as needed) procedures to restore any loss of data.

(C) *Emergency mode operation plan (Required).* 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.

(D) *Testing and revision procedures (Addressable).* Implement procedures for periodic testing and revision of contingency plans.

(E) *Applications and data criticality analysis (Addressable).* Assess the relative criticality of specific applications and data in support of other contingency plan components.

(8) *Standard: Evaluation.* Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational 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.

(b) (1) *Standard: Business associate contracts and other arrangements.* A covered entity, in accordance with § 164.306, 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) that the business associate will appropriately safeguard the information.

(2) *This standard does not apply with respect to—*

(i) The transmission by a covered entity of electronic protected health information to a health care provider concerning the treatment of an individual.

(ii) The transmission of electronic protected health information by a group health plan or an HMO or health insurance issuer on behalf of a group health plan to a plan sponsor, to the extent that the requirements of § 164.314(b) and § 164.504(f) apply and are met; or

(iii) The transmission of electronic protected health information from or to other agencies

providing the services at § 164.502(e)(1)(ii)(C), when the covered entity is a health plan that is a government program providing public benefits, if the requirements of § 164.502(e)(1)(ii)(C) are met.

(3) A covered entity that violates the satisfactory assurances it provided as a business associate of another covered entity will be in noncompliance with the standards, implementation specifications, and requirements of this paragraph and § 164.314(a).

(4) *Implementation specifications:* Written contract or other arrangement (Required). Document the satisfactory assurances required by paragraph (b)(1) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of § 164.314(a).

§ 164.310 Physical Safeguards

A covered entity must, in accordance with § 164.306:

(a) (1) *Standard:* Facility access controls. Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

(2) *Implementation specifications:*

(i) *Contingency operations (Addressable).* Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.

(ii) *Facility security plan (Addressable).* Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

(iii) *Access control and validation procedures (Addressable).* Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.

(iv) *Maintenance records (Addressable).* Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).

(b) *Standard: Workstation use*. Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.

(c) *Standard: Workstation security.* Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.

(d) (1) *Standard: Device and media controls.* Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.

(2) Implementation specifications:

(i) *Disposal (Required).* Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.

(ii) *Media re-use (Required).* Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.

(iii) *Accountability (Addressable).* Maintain a record of the movements of hardware and electronic media and any person responsible therefore.

(iv) *Data backup and storage (Addressable).* Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.

§ 164.312 Technical Safeguards.

A covered entity must, in accordance with § 164.306:

(a) (1) *Standard: Access control.* Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).

(2) *Implementation specifications:*

(i) *Unique user identification (Required).* Assign a unique name and/ or number for identifying and tracking user identity.

(ii) *Emergency access procedure (Required).* Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.

(iii) *Automatic logoff (Addressable).* Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

(iv) *Encryption and decryption (Addressable).* Implement a mechanism to encrypt and decrypt electronic protected health information.

(b) *Standard: Audit controls.* Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

(c) (1) *Standard: Integrity*. Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

(2) *Implementation specification:* Mechanism to authenticate electronic protected health information (Addressable). Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.

(d) *Standard: Person or entity authentication.* Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

(e) (1) *Standard: Transmission security.* Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

(2) *Implementation specifications:*

(i) *Integrity controls (Addressable).* Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.

(ii) *Encryption (Addressable).* Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

§ 164.316 Policies and procedures and documentation requirements.

A covered entity must, in accordance with § 164.306:

(a) *Standard: Policies and procedures*. Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in § 164.306(b)(2)(i), (ii), (iii), and (iv). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.

(b) (1) *Standard: Documentation.*

(i) Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and

(ii) If an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.

(2) *Implementation specifications:*

(i) *Time limit (Required).* Retain the documentation required by paragraph (b)(1) of this

section for 6 years from date of its creation or the date when it last was in effect, whichever is later.

(ii) *Availability (Required).* Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.

(iii) *Updates (Required).* Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.

TeleRay is in accordance with the HiTech Act of 2009-

http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/hitechact.pdf

Appendix B. HIPAA Security Standards Matrix

Excerpted from the *Federal Register* / Vol. 68, No. 34, p. 8380

Standards	Sections	Implementation Specifications
Administrative Safeguards		
Security Management Process	164.308(a)(1)	Risk Analysis (R)
		Risk Management (R)
		Sanction Policy (R)
		Information System Activity Review (R)
Assigned Security Responsibility	164.308(a)(2)	(R)
Workforce Security	164.308(a)(3)	Authorization and/or Supervision (A)
		Workforce Clearance Procedure
		Termination Procedures (A)
Information Access Management	164.308(a)(4)	Isolating Health care Clearinghouse Function (R)
		Access Authorization (A)
		Access Establishment and Modification (A)
Security Awareness and Training	164.308(a)(5)	Security Reminders (A)
		Protection from Malicious Software (A)
		Log-in Monitoring (A)
		Password Management (A)
Security Incident Procedures	164.308(a)(6)	Response and Reporting (R)
Contingency Plan	164.308(a)(7)	Data Backup Plan (R)
		Disaster Recovery Plan (R)
		Emergency Mode Operation Plan (R)
		Testing and Revision Procedure (A)
		Applications and Data Criticality Analysis (A)
Evaluation	164.308(a)(8)	(R)
Business Associate Contracts and Other Arrangement	164.308(b)(1)	Written Contract or Other Arrangement (R)
Physical Safeguards		
Facility Access Controls	164.310(a)(1)	Contingency Operations (A)
		Facility Security Plan (A)
		Access Control and Validation Procedures (A)
		Maintenance Records (A)
Workstation Use	164.310(b)	(R)
Workstation Security	164.310(c)	(R)
Device and Media Controls	164.310(d)(1)	Disposal (R)
		Media Re-use (R)
		Accountability (A)
		Data Backup and Storage (A)
Technical Safeguards		
Access Control	164.312(a)(1)	Unique User Identification (R)
		Emergency Access Procedure (R)
		Automatic Logoff (A)
		Encryption and Decryption (A)
Audit Controls	164.312(b)	(R)
Integrity	164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information (A)
Person or Entity Authentication	164.312(d)	(R)
Transmission Security	164.312(e)(1)	Integrity Controls (A)
		Encryption (A)
Documentation		
Documentaton	164.316(b)(2)(i)	Time limit (R)
	164.316(b)(2)(ii)	Availability (R)
	164.316(b)(2)(iii)	Updates (R)

(R) – Required
(A) -- Addressable