

HIPAA SECURITY STANDARDS CHECKLIST

By

Larry Grudzien

Attorney at Law

INTRODUCTION

Most covered entities (health plans, health care clearinghouses, and health care providers that transmit health information electronically) must comply with the new security standards by April 21, 2005 (2006 for health plans with annual receipts of \$5 million or less).

There are two different types of security standards; “Required” compliance standards and “Addressable” compliance standards. Required standards are designated with a (R) on the following checklist and Addressable standards are designated with an (A) on the checklist. All covered entities must comply with the Required standards. With respect to the Addressable standards, every covered entity must: (1) assess whether the standard is reasonable and appropriate in its particular environment, when analyzed with the likely contributions protecting the entity’s electronic protected information; and (2) implement the standard if it is reasonable and appropriate; or (a) document why it would not be reasonable and appropriate to implement the standard; and (b) implement an equivalent alternative measure if one is reasonable and appropriate.

ADMINISTRATIVE SAFEGUARDS (§ 164.308(a))

□ SECURITY MANAGEMENT PROCESS

- Risk Analysis (R). Conduct an *accurate and thorough* assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (“e-PHI”) held by the covered entity. § 164.308(a)(1)(ii)(A).
- Risk Management (R). Implement security measures that reduce risk and vulnerabilities to a “reasonable and appropriate level.” § 164.308(a)(1)(ii)(B).
- Sanction Policy (R). “Apply appropriate sanctions” against workforce members who fail to comply with its security policies and procedures. § 164.308(a)(1)(ii)(C).
- Information System Activity Review (R). Implement procedures to regularly review records of information system activity, such as audit logs, access reports and security incidence tracking reports. § 164.308(a)(1)(ii)(D).

□ ASSIGN SECURITY OFFICIAL (R)

Identify a “security official” who is responsible for the development and implementation of necessary security policies and procedures.
§ 164.308(a)(2).

- **WORKFORCE SECURITY**
 - Authorization/Supervision Procedures (A) Implement procedures to provide for the authorization and supervision of workforce members who work with e-PHI information or who work in locations where it might be accessed. § 164.308(a)(3)(ii)(A).
 - Workforce Clearance Procedures (A). Implement procedures to determine whether the access of a workforce member to electronic health information is appropriate. § 164.308(a)(3)(ii)(B).
 - Access Termination Procedures (A). Implement procedures to terminate an individual's access to electronic protected health information when necessary or appropriate. § 164.308(a)(3)(ii)(C).

- **INFORMATION ACCESS MANAGEMENT**
 - Isolating Health Care Clearinghouse Functions (R). If a health care clearinghouse is part of a larger organization, that clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. § 164.308(a)(4)(ii)(A).
 - Access Authorization (A). Implement policies and procedures for granting access to e-PHI (e.g., through access to a workstation or other source). § 164.308(a)(4)(ii)(B).
 - Access Establishment and Modification (A). Implement policies and procedures that establish, document, review and modify a user's right to access a workstation or other similar location. § 164.308(a)(4)(ii)(C).

- **SECURITY AWARENESS AND TRAINING**
 - Security Reminders (A). Provide periodic security updates to all members of its workforce. § 164.308(a)(5)(ii)(A).
 - Software Protection (A). Implement procedures to detect and guard against viruses and other malicious software. § 164.308(a)(5)(ii)(B).
 - Log-In Monitoring (A). Implement procedures to monitor attempts to log-in to any system that holds electronic health information and to report discrepancies in attempted log-ins. § 164.308(a)(5)(ii)(C).

- Password Management (A). Implement procedures to create, change and safeguard passwords. § 164.308(a)(5)(ii)(D).
- **SECURITY INCIDENT PROCEDURES**
 - Identify and Respond to Security Incidents (R). Implement policies and procedures to identify and respond to suspected or known security incidents and document security incidents and their outcomes. § 164.308(a)(6)(ii).
 - Mitigate Known Security Incidents (R). Implement policies and procedures to mitigate, to the extent practicable, harmful effects of any security breach or incident that is known to the covered entity. § 164.308(a)(6)(ii).
 - Document Security Incidents (R). Implement policies and procedures that will document each security incident and its outcome. § 164.308(a)(6)(ii).
- **CONTINGENCY PLAN**
 - Data Backup Plan (R). Implement policies and procedures to create and maintain retrievable “exact” copies of e-PHI. § 164.308(a)(7)(ii)(A).
 - Disaster Recovery Plan (R). Establish and implement any necessary procedures to restore lost data. § 164.308(a)(7)(ii)(B).
 - Emergency Operation Plan (R). Establish and implement any necessary procedures to enable the continuation of critical business processes needed to protect the security of e-PHI while operating in an emergency mode. § 164.308(a)(7)(ii)(C).
 - Testing and Revision Procedures (A). Implement procedures that allow for the periodic testing and revision of contingency plans. § 164.308(a)(7)(ii)(D).
 - Applications and Data Criticality Analysis (A). Assess the relative importance of specific applications and data in support of other contingency plan components. § 164.308(a)(7)(ii)(E).
- **EVALUATION (R).**

Perform technical and non-technical evaluations of the entity’s security policies and procedures and in response to environmental or operational changes affecting the security of e-PHI that establishes the extent to

which an entity's security policies and procedures meet the requirements of the regulations § 164.308(a)(7).

BUSINESS ASSOCIATE CONTRACTS AND OTHER AGREEMENTS (§§ 164.308(b) and 164.314)

□ BUSINESS ASSOCIATE CONTRACTS (R).

A covered entity may generally permit a business associate to create, receive, maintain or transmit e-PHI on its behalf only if it enters into an appropriate business associate contract or arrangement with that business associate. The business associate contract or arrangement must provide that the business associate will:

- Implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the e-PHI that it creates, receives, maintains or transmits on behalf of the covered entity. § 164.314(a)(2)(i)(A).
- Ensure that any agent, including a sub-contractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect the e-PHI. § 164.314(a)(2)(i)(B).
- Report to the covered entity any security incidents of which it becomes aware. § 164.314(a)(2)(i)(C).
- Authorize the termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract, unless this requirement is inconsistent with the statutory obligations of the covered entity or the business associate. § 164.314(a)(2)(i)(D)

□ GROUP HEALTH PLANS (R).

In most instances, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard e-PHI created, received, maintained or transmitted to or by the plan sponsor. Accordingly, the plan documents of the group's health plan must be amended to incorporate the following provisions to require the plan sponsor to:

- Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity

and availability of e-PHI that the plan sponsor creates, receives, maintains or transmits on behalf of the group health plan.
§ 164.314(b)(2)(i).

- Ensure that there is an adequate separation (or fire wall) between the information that is received from the group health plan and other employment information and decisions and this separation is supported by reasonable and appropriate security measures.
§ 164.314(b)(2)(ii).
- Ensure that any agent, including a sub-contractor, to whom the plan sponsor provides this information, agrees to implement reasonable and appropriate security measures to protect the information.
§ 164.314(b)(2)(iii).
- Report to the group health plan any security incident of which the plan sponsor becomes aware of § 164.314(b)(2)(iv).

PHYSICAL SAFEGUARDS (§ 164.310)

- **FACILITY ACCESS CONTROLS**
 - Contingency Operations (A). Establish and implement any necessary procedures to allow access to the facility to support the restoration of lost data under a disaster recovery plan and an emergency mode operations plan. § 164.310(a)(2)(i).
 - Facility Security Plan (A). Implement policies and procedures to safeguard the facility and equipment from unauthorized physical access, tampering and theft. § 164.3109(a)(2)(ii).
 - Access Control and Validation Procedures (A). Implement procedures to control and validate a person's access to facilities based upon their role or function (including visitor control) and to control access to software programs for testing and revision.
§ 164.310(a)(2)(iii).
 - Maintenance Records (A). Implement policies and procedures to document any repairs or modifications to the physical components of a facility which are related to its security (hardware, walls, doors, and locks). § 164.310(a)(2)(iv).

WORKSTATION USE (R).

Implement policies and procedures specific to the functions that are to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of the specific workstation or class of workstation that can access e-PHI. § 164.310(b).

WORKSTATION SECURITY (R).

Implement physical safeguards restricting unauthorized access to authorized users-only information for all workstations that have the ability to access e-PHI. § 164.310(c).

DEVICE AND MEDIA CONTROLS

Disposal (R). Implement policies and procedures to address the final disposition of e-PHI and/or the hardware or electronic media

Disposal (R). Implement policies and procedures to address the final disposition of e-PHI and/or the hardware or electronic media on which e-PHI has been stored. § 164.310(d)(2)(i).

Media Re-Use (R). Implement procedures for removal of e-PHI from electronic media before the media is made available for re-use. § 164.310(d)(2)(ii).

Accountability (A). Maintain a record of the movements of hardware and electronic media and any person responsible for such movements. § 164.310(d)(2)(iii).

Data Backup and Storage (A). Create a retrievable, exact copy of e-PHI when needed, before movement or transfer of hardware or other electronic media. § 164.310(d)(2)(iv).

TECHNICAL SAFEGUARDS (§ 164.312)

ACCESS CONTROL

Unique User Identification (R). Implement policies and procedures that assign a unique name and/or user number to identify and track user identity. § 164.312(a)(2)(i).

- Emergency Access Procedure (R). Establish and implement necessary procedures to obtain necessary e-PHI in an emergency. § 164.312(a)(2)(ii).
- Automatic Log-Off (A). Implement electronic procedures that terminate an electronic session after a pre-determined period of inactivity. § 164.312(a)(2)(iii).
- Encryption and Decryption (A). Implement a mechanism to encrypt and decrypt e-PHI. § 164.312(a)(2)(iv).
- **AUDIT CONTROLS (R).**
Implement hardware, software, and/or procedural mechanisms that record and examine activity on information systems that contain or use e-PHI. § 164.312(b).
- **INTEGRITY (A).**
Implement electronic mechanisms to corroborate that e-PHI has not been altered or destroyed in an unauthorized manner. § 164.312(c)(2).
- **USER AUTHENTICATION (R).**
Implement procedures to verify that a person or entity seeking to access e-PHI is the person or entity claimed. § 164.312(d).
- **TRANSMISSION SECURITY**
 - Integrity Controls (A). Implement security measures to ensure that electronically transmitted e-PHI is not improperly modified without detection until the e-PHI is disposed of. § 164.312(e)(2)(i).
 - Encryption (A). Implement a mechanism to encrypt e-PHI whenever it is deemed appropriate. § 164.312(e)(2)(ii)

POLICIES AND PROCEDURES AND DOCUMENTATION REQUIREMENTS (§ 164.316)

- **POLICIES AND PROCEDURES (R).**
Implement reasonable and appropriate policies and procedures to comply with the security standards. Covered entities may change their policies

and procedures at any time, provided that the changes are documented and implemented in accordance with the security regulations.
§ 164.316(a)

□ **DOCUMENTATION.**

- Document Policies and Procedures (R). Maintain written (which may be electronic) policies and procedures that are implemented to comply with the security regulations. § 164.316(b)(1)(i).
- Document Action, Activities and Assessments (R). Maintain a written (which may be electronic) record of any action, activity or assessment required under the security regulations.
§ 164.316(b)(1)(ii).
- Time Limits (R). Retain all documentation required for six years from the date of its creation or the date when it was last in effect, whichever is later. § 164.316(b)(2)(i).
- Availability (R). Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains. § 164.316(b)(2)(ii).
- Updates (R). Review documentation periodically and update that information as necessary to respond to environmental or operational changes that affect the security of e-PHI. § 164.316(b)(2)(iii).