

# Health Insurance Portability and Accountability Act of 1996 (HIPAA)

## Security Rule

### March, 2004

This document was developed to assist the state agencies of Ohio in understanding the obligations imposed by the Health Insurance Portability and Accountability Act (HIPAA). The State of Ohio provides no guarantee of accuracy or warranties of any kind. Utilization of this information is at the sole risk of the user. As with any matter of law, independent legal counsel should be consulted regarding compliance with the requirements of the HIPAA.

Effective Date: The Rule must be implemented by April 20, 2005 except small health plans who must implement no later than April 20, 2006.

### **Purpose**

The proposed security regulations require the following:

- The ability to control access to protected health information (PHI).
- The ability to protect PHI from the accidental or intentional disclosure to unauthorized individuals.
- The ability to protect PHI from alteration, destruction, or loss.

**Structure of Rule** The Rule is organized by the topic areas as listed below. Within the each topic area, the rule specifies standards and corresponding implementation specifications that are required, or addressable. If a implementation specification is addressable, the covered entity is required to assess whether the specification is reasonable and appropriate to implement. If it is, the covered entity is required to implement the specification. If is not, the covered entity must document why it is not, and implement an equivalent alternative if reasonable and appropriate. However, the rule provides for “flexibility of approach” which allows a covered entity to reasonably and appropriately implement the standards and specifications.

#### *I. Administrative Procedures to Guard Data Integrity, Confidentiality, and Availability*

These include documented, formal practices to manage the selection and execution of security measures to protect data, and to manage the conduct of personnel in relation to the protection of data. The standard includes the following specifications:

- Security management process - implement polices and procedures to prevent, detect, contain, and correct security violations.
- Assigned security responsibility-security responsibility must be assigned to a specific individual or group.
- Workforce security -policy and procedures must be implemented to ensure that the workforce has appropriate access to e-PHI.
- Information access management- implement policies and procedures to isolate the health care clearinghouse function and establishing access authorization and modification.
- Security awareness and training-implement a security awareness and training program for all members of the workforce.
- Security incident procedures-implement polices and procedures to address security incidents.
- Contingency plan-establish polices and procedures for responding to an emergency or other occurrence. Establish a disaster recovery plan.

- Evaluation-perform technical and non-technical evaluation initially based on the standards in the rule, and subsequently in response to environmental or operational changes affecting the security of e-PHI.
- Business associate contracts and other arrangements-Obtain satisfactory assurances from business associates that e-PHI is appropriately safeguarded.

### II. Physical Safeguards to Guard Data Integrity, Confidentiality, and Availability

These include limiting access to, and the protection of, physical computer systems and related buildings and equipment from fire and other natural and environmental hazards, as well as from intrusion. They cover the use administrative measures used to control access to computer systems and facilities. This standard includes the following implementation specifications:

- Facility access controls-implement policies and procedures to limit physical access to electronic information systems and the facility(s) where they are housed while insuring proper authorized access.
- Workstation use-implement policies and procedures to insure the proper function and physical surroundings of workstations or class of workstations that access e-PHI
- Workstation security-physical access safeguards must be developed and maintained for all workstations that access e-PHI..
- Device and media control- implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain e-PHI, including media re-use, accountability and data backup and storage.

### III. Technical Safeguards to Guard Data Integrity, Confidentiality, and Availability

These include the processes to protect information and to control individual access or software access to e-PHI. This standard includes the following specifications:

- Access control-implement technical policies and procedures for systems that contain e-PHI to allow access to only to those persons or software programs that have been granted access rights as specified in the Security Rule.
- Audit controls-implement hardware, software or procedures that record and examine activity in information systems that contain or use e-PHI.
- Integrity-implement policies and procedures that protect e-PHI from improper alteration or destruction.
- Person or entity authentication-implement procedures to verify the identity of a person or entity asking for access to e-PHI.
- Transmission security-implement technical security measures to guard against unauthorized access to e-PHI that is transmitted over an electronic communications network.

IV. Organizational Requirements

This includes requirements for business associate contracts and group health plans.

- Business associate contracts-the business associate contract must meet the requirements of section 164.308 of the Security Rule.
- Requirements for group health plans-with certain exceptions, 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 on behalf of the group health plan.

V. Policy and Procedures

This includes requirements for the development, retention, availability and revision of policies and procedures and other documentation requirements.

- Policies and procedures-a covered entity must implement reasonable and appropriate policies and procedures to comply with the Security Rule.
- Documentation-a covered entity must maintain written policies and procedures implemented to comply with the Security Rule, and a written record of any action, activity or assessment required by the Rule.

**Appendix A Security Rule, 42 CFR Parts 160, 162, and 164**

Appendix A below is reproduced is reproduced directly from the federal Security Rule, 42 CFR Parts 160, 162, and 164. It provides an outline of the standards and corresponding specifications with notation of whether they are required or addressable.

## Appendix A to Subpart C of Part 164—Security Standards: Matrix (1)

Standards	Sections	Implementation Specifications (R)=Required, (A)=Addressable
<b>Administrative Safeguards</b>		
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** (see § 164.312)

---

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)