

HIPAA SECURITY REGULATIONS

ADMINISTRATIVE SAFEGUARDS

<i>Standards</i>	<i>Sections</i>	<i>Implementation Specifications</i> <i>(R)=Required, (A)=Addressable</i>
Security Management Process (Policies and procedures to prevent/detect/contain and correct security violations.)	164.308(a)(1)	
		Risk Analysis (R) (Assess risks and vulnerabilities to electronic PHI)
		Risk Management (R) (Implement security measures to reduce risk and vulnerabilities to a reasonable level)
		Sanction Policy (R) (Apply appropriate sanctions against workforce members who fail to comply with policies and procedures.)
		Information System Activity Review (R) (Procedures to regularly review info system activity, i.e. audit logs, access reports, security incident tracking.)
Assigned Security Responsibility (Identify the security official responsible for compliance with Security Regs.)	164.308(a)(2)	(R)
Workforce Security (Policies and procedures to ensure members of workforce have appropriate access to electronic PHI, and to prevent those workforce members not entitled to access from obtaining access to electronic PHI.)	164.308(a)(3)	
		Authorization and/or Supervision (A) (Adopt procedures for authorization or supervision of workforce members with permitted access to electronic PHI.)
		Workforce Clearance Procedure (A) (Adopt procedures to ensure appropriate access to electronic PHI by workforce.)
		Termination Procedures (A) (To ensure termination of access to electronic PHI at end of employment.)
Information Access Management (Adopt procedures regarding authorized access to electronic PHI.)	164.308(a)(4)	
		Isolating Health care Clearinghouse Function (R) (Applicable to Clearinghouse functions of larger organization. N/A Purdue.)
		Access Authorization (A) (Procedures to control access to electronic PHI, via workstation, transaction, program, other mechanism.)
		Access Establishment and Modification (A) (Establish, document, review, and modify user's right to access, a workstation, transaction, program, etc.)

<p>Security Awareness and Training (Train all members of workforce, including management.)</p>	<p>164.308(a)(5)</p>	<p>Security Reminders (Periodic security updates.)</p> <p>Protection from Malicious Software (Guard, detect, and report malicious software.)</p> <p>Log-in Monitoring (Monitor log-in attempts and report discrepancies)</p> <p>Password Management (Procedures re creation, changes and safeguarding of passwords.)</p>	<p>(A)</p> <p>(A)</p> <p>(A)</p> <p>(A)</p>
<p>Security Incident Procedures</p>	<p>164.308(a)(6)</p>	<p>Response and Reporting (Identify and respond to suspected or known security incidents; mitigate damages, and document incidents and outcome.)</p>	<p>(R)</p>
<p>Contingency Plan (To respond to emergencies, vandals, system failure and natural disasters.)</p>	<p>164.308(a)(7)</p>	<p>Data Backup Plan (Procedures to create and maintain exact copies of electronic PHI.)</p> <p>Disaster Recovery Plan (Procedures to restore any loss of data.)</p> <p>Emergency Mode Operation Plan (Procedures to continue critical business process to ensure the security of electronic PHI while operating in emergency mode.)</p> <p>Testing and Revision Procedure (Periodic testing and revision of Contingency Plans.)</p> <p>Applications and Data Criticality Analysis (Assess relative criticality of applications and data in support of other contingency plan components.)</p>	<p>(R)</p> <p>(R)</p> <p>(R)</p> <p>(A)</p> <p>(A)</p>
<p>Evaluation (Periodic technical and non-technical evaluation considering environmental or operational changes affecting the security of electronic PHI.)</p>	<p>164.308(a)(8)</p>		<p>(R)</p>
<p>Business Associate Contracts and Other Arrangement (Specific contractual requirements for BA's, similar to privacy regulations, aimed at protecting security of electronic PHI.)</p>	<p>164.308(b)(1)</p>	<p>Written Contract or Other Arrangement (Document assurances of BA in written agreement.)</p>	<p>(R)</p>

PHYSICAL SAFEGUARDS

<i>Standards</i>	<i>Sections</i>	<i>Implementation Specifications</i> (R)=Required, (A)=Addressable
Facility Access Controls (Policies and procedures to limit physical access to electronic info systems and the facilities housing them.)	164.310(a)(1)	Contingency Operations (A) (Procedures to allow facility access in support of restoration of lost data under disaster recovery plan and emergency mode operations.)
		Facility Security Plan (A) (Safeguard facility and equipment from unauthorized access.)
		Access Control and Validation (A) (Validate a person's access to facilities based on their role or function, including visitor control, and control during testing and revision.)
		Maintenance Records (A) (Document repairs and modifications to the physical components of a facility related to security, such as hardware, walls, doors, locks.)
Workstation Use	164.310(b)	(R) (Policies and procedures to specify the proper functions to be performed, the manner of performance, physical attributes of the surroundings of workstations that can access electronic PHI.)
Workstation Security	164.310(c)	(R) (Implement physical safeguards for all workstations with access to electronic PHI to prevent unauthorized access.)
Device and Media Controls (Policies and procedures to govern the receipt and removal of hardware and electronic media containing PHI into and out of facility and movement within the facility.)	164.310(d)(1)	Disposal (R) (Address the final disposition of electronic PHI, and hardware or media on which it is stored.)
		Media Re-use (R) (Procedures to remove electronic PHI from electronic media before re-use.)
		Accountability (A) (Maintain a record of movements of hardware and electronic media and identify responsible persons.)
		Data Backup and Storage (A) (Create retrievable, exact copy of electronic PHI, when needed, before moving equipment.)

TECHNICAL SAFEGUARDS (SEE §164.312)

<i>Standards</i>	<i>Sections</i>	<i>Implementation Specifications</i> <i>(R)=Required, (A)= Addressable</i>
Access Control (Technical policies and procedures for electronic info systems that maintain PHI to allow access only to those persons or software programs that have been granted access rights.)	164.312(a)(1)	
	Unique User Identification (Unique name or number to identify and track identity.)	(R)
	Emergency Access Procedure (Procedures to ensure emergency access of PHI.)	(R)
	Automatic Logoff (Electronic procedures to terminate electronic session after predetermined period of inactivity.)	(A)
	Encryption and Decryption (Implement a mechanism to encrypt and decrypt electronic PHI.)	(A)
Audit Controls (Hardware, software, and/or procedural mechanisms to record and examine activity in info systems that contain PHI.)	164.312(b)	(R)
Integrity (Implement procedure to protect electronic PHI from unauthorized alteration or destruction.)	164.312(c)(1)	
	Mechanism to Authenticate Electronic Protected Health Information (Implement mechanisms to corroborate that electronic PHI has not been altered or destroyed without proper authorization.)	(A)
Person or Entity Authentication (Procedures to verify that a person or entity seeking access to electronic PHI is the one claimed.)	164.312(d)	(R)
Transmission Security (Implement technical measure to guard against unauthorized access to electronic PHI transmitted over an electronic communications network.)	164.312(e)(1)	
	Integrity Controls (Adopt security measures to ensure that electronically transmitted PHI is not improperly modified without detection.)	(A)
	Encryption (Create mechanism to encrypt electronic PHI whenever deemed appropriate.)	(A)