HIPAA SECURITY RULE

QUICK REFERENCE CARD

HIPAA™ Academy

www.ecfirst.com

Standard	Section	Implementation Specification (R)=Required, (A)=Addressable
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) Data Backup Plan (R)
Contingency Plan	§164.308(a)(7)	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)

Standard	Section	Implementation Specification (R)=Required, (A)=Addressable
Workstation Use	§164.310(b)	(R)
Workstation Security	§164.310(c)	(R)
Device and Media Controls	§164.310(d)	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) (R)
Person or Entity Authentication	§164.312(d)	Integrity Controls (A)
Transmission Security	§164.312(e)(1)	Encryption (A)

Figure 1: Summary Table of HIPAA Security Rule

In this section we summarize information on all standards and implementation specifications defined in the HIPAA Security Rule.

ADMINISTRATIVE SAFEGUARDS		
Security Management Process Standard	*164.308(a)(1)(i)*	Implement policies and procedures to prevent, detect, contain, and correct security violations
Risk Analysis Impl. Spec.	*164.308(a)(1)(ii)(A)*	*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.*
Risk Management Impl. Spec.	*164.308(a)(1)(ii)(B)*	*Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with 164.306(a).*
Sanction Policy Impl. Spec.	*164.308(a)(1)(ii)(C)*	*Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.*
Information System Activity Review Impl. Spec.	*164.308(a)(1)(ii)(D)*	*Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.*
Assigned Security Responsibility Standard	164.308(a)(2)	Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.
Workforce Security Standard	164.308(a)(3)(i)	Implement policies and procedures to ensure that all members of its workforce have appropriate access to EPHI, and to prevent those workforce members who do not have access to EPHI.
Authorization and/or Supervision Impl. Spec.	*164.308(a)(3)(ii)(A)*	*Implement procedures for the authorization and/or supervision of workforce members who work with EPHI or in locations where it might be accessed.*
Workforce Clearance Procedure Impl. Spec.	*164.308(a)(3)(ii)(B)*	*Implement procedures to determine that the access of a workforce member to EPHI is appropriate.*
Termination Procedures Impl. Spec.	*164.308(a)(3)(ii)(C)*	*Implement procedures for terminating access to EPHI when the employment of a workforce member ends.*
Information Access Management Standard	164.308(a)(4)(i)	Implement policies and procedures for authorizing access to EPHI.

ADMINISTRATIVE SAFEGUARDS		
Isolation Healthcare Clearinghouse Function Impl. Spec.	*164.308(a)(4)(ii)(A)*	*If a healthcare 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.*
Access Authorization Impl. Spec.	*164.308(a)(4)(ii)(B)*	*Implement policies and procedures for granting access to EPHI, for example, through access to a workstation, transaction, program, process, or other mechanism.*
Access Establishment and Modification Impl. Spec.	*164.308(a)(4)(ii)(C)*	*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.*
Security Awareness and Training Standard	164.308(a)(5)(i)	Implement a security awareness and training program for all members of its workforce (including management).
Security Reminders Impl. Spec.	*164.308(a)(5)(ii)(A)*	*Periodic security updates.*
Protection from Malicious Software Impl. Spec.	*164.308(a)(5)(ii)(B)*	*Procedures for guarding against, detecting, and reporting malicious software.*
Log-in Monitoring Impl. Spec.	*164.308(a)(5)(ii)(C)*	*Procedures for monitoring log-in attempts and reporting discrepancies.*
Password Management Impl. Spec.	*164.308(a)(5)(ii)(D)*	*Procedures for creating, changing, and safeguarding passwords.*
Security Incident Procedures Standard	164.308(a)(6)(i)	Implement policies and procedures to address security incidents.
Response and Reporting Impl. Spec.	*164.308(a)(6)(ii)*	*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.*
Contingency Plan Standard	164.308(a)(7)(i)	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.

ADMINISTRATIVE SAFEGUARDS		
Data Backup Plan Impl. Spec.	*164.308(a)(7)(ii)(A)*	*Establish and implement procedures to create and maintain retrievable exact copies of EPHI.*
Disaster Recovery Plan Impl. Spec.	*164.308(a)(7)(ii)(B)*	*Establish (and implement as needed) procedures to restore any loss of data.*
Emergency Mode Operation Plan Impl. Spec.	*164.308(a)(7)(ii)(C)*	*Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of EPHI while operating in emergency mode.*
Testing and Revision Procedure Impl. Spec.	*164.308(a)(7)(ii)(D)*	*Implement procedures for periodic testing and revision of contingency plans.*
Applications and Data Criticality Analysis Impl. Spec.	*164.308(a)(7)(ii)(E)*	*Assess the relative criticality of specific applications and data in support of other contingency plan components.*
Evaluation Standard	164.308(a)(8)	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 EPHI that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart.
Business Associate Contracts and Other Arrangement Standard	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.
Written Contract or Other Arrangement Impl. Spec.	*164.308(b)(4)*	*Document the satisfactory assurances through a written contract or other arrangement with the business associate that meets with applicable requirements of 164.314(a).*

Figure 2: Summary HIPAA Security Rule Administrative Safeguards.

PHYSICAL SAFEGUARDS		
Facility Access Controls Standard	164.310(a)(1)	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.
Contingency Operations Impl. Spec.	*164.310(a)(2)(i)*	*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.*
Facility Security Plan Impl. Spec.	*164.310(a)(2)(ii)*	*Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering and theft.*
Access Control and Validation Impl. Spec.	*164.310(a)(2)(iii)*	*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.*
Maintenance Records Impl. Spec.	*164.310(a)(2)(iv)*	*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).*
Workstation Use Standard	164.310(b)	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 EPHI.
Workstation Security Standard	164.310(c)	Implement Physical Safeguards for all workstations that access EPHI, to restrict access to authorized users.
Device and Media Controls Standard	164.310(d)(1)	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.
Disposal Impl. Spec.	*164.310(d)(2)(i)*	*Implement policies and procedures to address the final disposition of EPHI, and/or the hardware or electronic media on which it is stored.*

PHYSICAL SAFEGUARDS		
Media Re-use Impl. Spec.	*164.310(d)(2)(ii)*	*Implement procedures for removal of EPHI from electronic media before the media are made available for re-use.*
Accountability Impl. Spec.	*164.310(d)(2)(iii)*	*Maintain a record of the movements of hardware and electronic media and any person responsible therefore.*
Data Backup and Storage Impl. Spec.	*164.310(d)(2)(iv)*	*Create a retrievable, exact copy of EPHI, when needed, before movement of equipment.*

Figure 3: Summary HIPAA Security Rule Physical Safeguards.

TECHNICAL SAFEGUARDS		
Access Control Standard	164.312(a)(1)	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).
Unique User Identification Impl. Spec.	*164.312(a)(2)(i)*	*Assign a unique name and/or number for identifying and tracking user identity.*
Emergency Access Procedures Impl. Spec.	*164.312(a)(2)(ii)*	*Establish (and implement as needed) procedures for obtaining necessary EPHI during an emergency.*
Automatic Logoff Impl. Spec.	*164.312(a)(2)(iii)*	*Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.*
Encryption and Decryption Impl. Spec.	*164.312(a)(2)(iv)*	*Implement a mechanism to encrypt and decrypt EPHI.*
Audit Controls Standard	164.312(b)	Implement hardware, software, and/or procedural mechanism that record and examine activity in information systems that contain or use EPHI.
Integrity Standard	164.312(c)(1)	Implement policies and procedures to protect EPHI from improper alteration or destruction.
Mechanism to Authenticate Electronic Protected Health Information Impl. Spec.	*164.312(c)(2)*	*Implement electronic mechanisms to corroborate that EPHI has not been altered or destroyed in an unauthorized manner.*
Person or Entity Authentication Standard	164.312(d)	Implement procedures to verify that a person or entity seeking access to EPHI is the one claimed.
Transmission Security Impl. Spec.	*164.312(e)(1)*	*Implement technical security measures to guard against unauthorized access to EPHI that is being transmitted over an electronic communications network.*
Integrity Controls Impl. Spec.	*164.312(e)(2)(i)*	*Implement security measures to ensure that electronically transmitted EPHI is not improperly modified without detection until disposed of.*
Encryption Impl. Spec.	*164.312(e)(2)(ii)*	*Implement a mechanism to encrypt EPHI whenever deemed appropriate.*

Figure 4: Summary HIPAA Security Rule Technical Safeguards.

About Us

Devoted to our Clients. Delivering with Passion.

ecfirst with rich hands-on experience delivers world-class services in the areas of:

- Security regulatory compliance solutions (HIPAA, HITECH Act, MARS-E, PCI DSS, NIST and ISO 27000, State Regulations)
  - ► Risk analysis, technical vulnerability assessment
  - ► Business Impact Analysis & Development of Disaster Recovery Plans
- Security, compliance training and certification
- On-Demand or Managed Compliance
  - ► HITECH data breach and incident response management
  - ► Deployment and implementation of security technologies (including remediation)
  - ► Policy development (privacy and security)
  - ► Encryption implementation (policy, product selection, implementation)
- E-Discovery services
- Software license assessment
- Professional staffing, including project management, security officer, HL7, HIPAA, ICD 9/10 and more

Regulatory Compliance Practice

The ecfirst Regulatory Compliance Practice delivers deep expertise with its full suite of services that include; ISO 27000 readiness and training, HIPAA Privacy Gap Analysis, Meaningful Use Risk Analysis, HITECH Data Breach, Technical Vulnerability Assessment, Policy and Procedure Development, Disaster Recovery Planning, On Demand Consulting, as well as our Managed Compliance Services Program (MCSP).

Compliance and Training Certification

ecfirst, home of the HIPAA Academy, offers the gold standard in compliance training and certification. The HIPAA CHA™, CHP and CSCS™ certifications are the only certifications recognized in the Industry. The ecfirst Certified Security Compliance Specialist™ (CSCS™) Program is the first and only information security program that addresses all major compliance regulations from a security perspective.

ecfirst delivers world-class information security and regulatory compliance solutions. With over 2,100 + clients, ecfirst was recognized as an Inc. 500 business – America's Top 500 Fastest Growing Privately Held Business in 2004 – our first year of eligibility. ecfirst serves a Who's Who client list that includes technology firms, numerous hospitals, state and county governments, and hundreds of businesses across the United States and abroad. A partial list of clients includes Microsoft, Symantec, HP, McKesson, EMC, IBM, Kaiser, Principal Financial, U.S. Army, U.S. Dept. of Homeland Security, U.S. Dept. of Veterans Affairs and many others.

ecfirst Differentiators

ecfirst combines state of the art tools, the highest credentialed staff, and reporting that maximizes value, efficiency, and information for our clients to deliver the industry's best technical vulnerability assessments. Critical ecfirst differentiators include:

- ISO 27000 suite of consulting and training services easily tailored to your requirements
- Home of The HIPAA Academy – First in the healthcare and information technology industry with the CHP and CSCS™ programs
- Highly credentialed professional consulting team with expertise in information security, HL7, ICD-9/10, HIPAA, HITECH, Meaningful Use
- E-Discovery Services
- Breach notification and incident response services
- Security technology deployment and implementation On Demand or Managed Compliance services
- On Demand Encryption Services to enable implementation of encryption capabilities in your environment (product selection, deployment on all portables/media, policy & more)
- Deep experience in the healthcare and information technology industries
- Compliance based technical vulnerability assessments (external, internal, wireless, firewall systems/DMZ)
- Executive dashboards that may be tailored for senior management to highlight critical findings

Contact ecfirst

Talk to ecfirst and you will find an organization that is passionate about the services we deliver and exceptionally devoted to its clients.

We deliver value with intensity and are paranoid about our performance for your organization. For more information, please call **+1.515.987.4044 x17** or visit www.ecfirst.com.