TriageLogic®

WHEN PATIENTS CALL, WE'RE YOUR ANSWER

Instant HIPAA Policy Mapped to the HIPAA Security Rule

Administrative Safeguards

Security Management Process (164.308(a)(1))
HIPAA Standard: Implement policies and procedures to prevent, detect, contain, and correct security violations.
Key Activities:

1. Identify Relevant Information Systems
    - ✓ Covered by Confidential Data Policy, section 4.1 Data Classification
    - ✓ Covered by Confidential Data Policy, section 4.3 Inventory
2. Conduct Risk Assessment
    - ✓ Covered by Incident Response Policy, section 4.7.1 Risk Assessment
3. Implement Risk Management Program
    - ✓ Covered by Incident Response Policy, section 4.7.2 Risk Management Program
4. Acquire IT Systems and Services
    - ✓ Covered by Introduction, section Implementation
    - ✓ Covered by Confidential Data Policy, section 4.4 Treatment of Confidential Data
5. Create and Deploy Policies and Procedures
    - ✓ Covered by Introduction, section Implementation
6. Develop and Implement a Sanction Policy
    - ✓ Covered by Sanction Policy (whole)
7. Develop and Deploy the Information System Activity Review Process
    - ✓ Covered by Network Security Policy, section 4.2 Logging
    - ✓ Covered by Network Security Policy, section 4.3 Audit Trails
8. Develop Appropriate Standard Operating Procedures
    - ✓ Covered by Network Security Policy, section 4.3.3 Audit Trails
9. Implement the Information System Activity Review and Audit Process
    - ✓ Covered by Network Security Policy, section 4.2 Logging
    - ✓ Covered by Network Security Policy, section 4.2 Audit Trails

Assigned Security Responsibility (164.308 (a)(2))
HIPAA Standard: Identify the official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.
Key Activities:

1. Select a Security Official to be Assigned Responsibility for HIPAA Security
    - ✓ Covered by Network Security Policy, section 4.21.1 Information Security Manager
2. Assign and Document the Individual's Responsibility
    - ✓ Covered by Network Security Policy, section 4.21.1 Information Security Manager

Workforce Security (164.308(a)(3))
HIPAA Standard: 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.
Key Activities:

1. Implement Policies and Procedures for Authorization and/or supervision
   - ✓ Covered by Workforce Security Policy, section 4.1 Roles and Responsibilities
2. Establish Clear Job Descriptions and Responsibilities
   - ✓ Covered by Workforce Security Policy, section 4.1 Roles and Responsibilities
3. Establish Criteria and Procedures for Hiring and Assigning Tasks
   - ✓ Covered by Workforce Security Policy, section 4.2 Hiring and Task Assignment
4. Establish a Workforce Clearance Procedure
   - ✓ Covered by Workforce Security Policy, section 4.3 Workforce Clearance
5. Establish Termination Procedures
   - ✓ Covered by Workforce Security Policy, section 4.3.2 Granting Access and Terminating Access
   - ✓ Covered by Workforce Security Policy, section 4.4 Employment Termination

Information Access Management (164.308(a)(4))
HIPAA Standard: 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.
Key Activities:

1. Isolate Healthcare Clearinghouse Functions
   - ✓ Covered by Confidential Data Policy, section 4.7 Security Controls for Confidential Data
   - ✓ Covered by Network Security Policy, section 4.11 Network Compartmentalization
2. Implement Policies and Procedures for Authorizing Access
   - ✓ Covered by Confidential Data Policy, section 4.6 Sharing Confidential Data
   - ✓ Covered by Network Access and Authentication Policy, section 4.2 Account Setup
   - ✓ Covered by Network Access and Authentication Policy, section 4.3 Account Access Levels
3. Implement Policies and Procedures for Access Establishment and Modification
   - ✓ Covered by Network Access and Authentication Policy, section 4.2 Account Setup
   - ✓ Covered by Network Access and Authentication Policy, section 4.3 Account Access Levels
4. Evaluate Existing Security Measures Related to Access Controls
   - ✓ Covered by Network Access and Authentication Policy, section 4.3 Account Access Levels

Security Awareness and Training (164.308(a)(5))
HIPAA Standard: Implement a security awareness and training program for all members of its workforce (including management).
Key Activities:

1. Conduct a Training Needs Assessment
   - ✓ Covered by Network Security Policy, section 4.21.2 Security Awareness Training
2. Develop and Approve a Training Strategy and Plan
   - ✓ Covered by Network Security Policy, section 4.21.2 Security Awareness Training

3. Protection from Malicious Software; Log-in Monitoring; and Password Management
   - ✓ Covered by Acceptable Use Policy, section 4.6 Reporting of a Security Incident
   - ✓ Covered by Password Policy, section 4.2 Confidentiality
   - ✓ Covered by Password Policy, section 4.4 Incident Reporting
   - ✓ Covered by Network Security Policy, section 4.21.2 Security Awareness Training
4. Develop Appropriate Awareness and Training Content, Materials, and Method
   - ✓ Covered by Network Security Policy, section 4.21.2 Security Awareness Training
5. Implement the Training
   - ✓ Covered by Network Security Policy, section 4.21.2 Security Awareness Training
6. Implement the Security Reminders
   - ✓ Covered by Network Security Policy, section 4.21.2 Security Awareness Training
7. Monitor and Evaluate Training Plan
   - ✓ Covered by Network Security Policy, section 4.21.2 Security Awareness Training

Security Incident Procedures (164.308(a)(6))

HIPAA Standard: Implement policies and procedures to address security incidents.

Key Activities:

1. Determine Goals of Incident Response
   - ✓ Covered by Incident Response Policy, section 4.1 Types of Incidents
   - ✓ Covered by Incident Response Policy, section 4.4 Electronic Incidents
   - ✓ Covered by Incident Response Policy, section 4.5 Physical Incidents
2. Develop and Deploy an Incident Response Team or Other Reasonable and Appropriate Response Mechanism
   - ✓ Covered by Incident Response Policy, section 4.2 Preparation
3. Develop and Implement Procedures to Respond to and Report Security Incidents
   - ✓ Covered by Incident Response Policy (whole)
4. Incorporate Post-Incident Analysis into Updates and Revisions
   - ✓ Covered by Incident Response Policy, section 4.4 Electronic Incidents
   - ✓ Covered by Incident Response Policy, section 4.5 Physical Incidents

Contingency Plan (164.308(a)(7))

HIPAA Standard: Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence that damages systems that contain electronic protected health information.

Key Activities:

1. Develop Contingency Planning Policy
   - ✓ Covered by Contingency Planning Policy (whole)
2. Conduct Applications and Data Criticality Analysis
   - ✓ Covered by Contingency Planning Policy, section 4.1 Business Impact Analysis
   - ✓ Covered by Contingency Planning Policy, section 4.2 Prioritization
3. Identify Preventive Measures
   - ✓ Covered by Contingency Planning Policy, section 4.3 Preventive Measures
4. Develop Recovery Strategy
   - ✓ Covered by Contingency Planning Policy, section 4.4 Develop Recovery Strategies
5. Data Backup Plan and Disaster Recovery Plan
   - ✓ Covered by Backup Policy (whole)
   - ✓ Covered by Contingency Planning Policy, section 4.6 Data Backup and Disaster Recovery
6. Develop and Implement an Emergency Mode Operation Plan

   - ✓ Covered by Contingency Planning Policy, section 4.7 Emergency Mode Operation
7. Testing and Revision Procedure
   - ✓ Covered by Contingency Planning Policy, section 4.8 Review, Testing, and Maintenance

Evaluation (164.308(a)(8))
HIPAA Standard: Implement policies and procedures to 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, which establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart.
Key Activities:

1. Determine Whether Internal or External Evaluation is Most Appropriate
   - ✓ Covered by Network Security Policy, section 4.9 Security Review
2. Develop Standards and Measurements for Reviewing All Standards and Implementation Specifications of the Security Rule
   - ✓ Covered by Network Security Policy, section 4.9 Security Review
3. Conduct Evaluation
   - ✓ Covered by Network Security Policy, section 4.9 Security Review
4. Document Results
   - ✓ Covered by Network Security Policy, section 4.9.3 Documentation of Evaluation Results
5. Repeat Evaluations Periodically
   - ✓ Covered by Network Security Policy, section 4.9 Security Review

Business Associate Contracts and Other Arrangements (164.308(b)(1))
HIPAA Standard: A covered entity 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 that the business associate will appropriately safeguard the information.
Key Activities:

1. Identify Entities that are Business Associates under the HIPAA Security Rule
   - ✓ Covered by Business Associate Policy, section 4.1 Business Associates
2. Written Contract or Other Arrangement
   - ✓ Covered by Business Associate Policy, section 4.4 Business Associate Agreements
3. Establish Process for Measuring Contract Performance and Terminating the Contract if Security Requirements are not Being Met
   - ✓ Covered by Business Associate Policy, section 4.4 Business Associate Agreements
4. Implement an Arrangement Other than a Business Associate Contract if Reasonable and Appropriate
   - ✓ Covered by Business Associate Policy, section 4.4 Business Associate Agreements

Physical Safeguards

Facility Access Controls (164.310(a)(1)

HIPAA Standard: 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.

Key Activities:

1. Conduct an Analysis of Existing Physical Security Vulnerabilities
   - ✓ Covered by Physical Security Policy, section 4.1 Physical Risk Assessment
2. Identify Corrective Measures
   - ✓ Covered by Physical Security Policy, section 4.1 Physical Risk Assessment
3. Develop Facility Security Plan
   - ✓ Covered by Physical Security Policy (whole)
4. Develop Access Control and Validation Procedures
   - ✓ Covered by Network Access and Authentication Policy (whole)
   - ✓ Covered by Physical Security Policy, section 4.7 Entry Security
5. Establish Contingency Operations Procedures
   - ✓ Covered by Contingency Planning Policy, section 4.4 Develop Recovery Strategies
   - ✓ Covered by Contingency Planning Policy, section 4.7 Emergency Mode Operation
6. Maintain Maintenance Records
   - ✓ Covered by Physical Security Policy, section 4.1 Physical Risk Assessment

Workstation Use (164.310(b))

HIPAA Standard: 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.

Key Activities:

1. Identify Workstation Types and Functions or Uses
   - ✓ Covered by Physical Security Policy, section 4.4 Workstation Security Policy
2. Identify Expected Performance of Each Type of Workstation
   - ✓ Covered by Physical Security Policy, section 4.4 Workstation Security Policy
3. Analyze Physical Surroundings for Physical Attributes
   - ✓ Covered by Network Access and Authentication Policy, section 4.9 Screensaver Passwords
   - ✓ Covered by Physical Security Policy, section 4.4 Workstation Security Policy

Workstation Security (164.310(c))

HIPAA Standard: Implement physical safeguards for all workstations that access ePHI, to restrict access to authorized users.

Key Activities:

1. Identify All Methods of Physical Access to Workstations
   - ✓ Covered by Physical Security Policy, section 4.4 Workstation Security Policy
2. Analyze the Risk Associated with Each Type of Access
   - ✓ Covered by Physical Security Policy, section 4.4 Workstation Security Policy
3. Identify and Implement Safeguards for Workstations
   - ✓ Covered by Physical Security Policy, section 4.5 Physical System Security

Device and Media Controls (164.310(d)(1))

HIPAA Standard: 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.

Key Activities

1. Implement Methods for Final Disposal of ePHI
   - ✓ Covered by Confidential Data Policy, section 4.4.3 Destruction
   - ✓ Covered by Network Security Policy, section 4.10 Disposal of Information Technology Assets
2. Develop and Implement Procedures for Reuse of Electronic Media
   - ✓ Covered by Mobile Device Policy, section 4.2.3 Removable Media
3. Maintain Accountability for Hardware and Electronic Media
   - ✓ Covered by Confidential Data Policy, section 4.6 Sharing Confidential Data
4. Develop Data Backup and Storage Procedures
   - ✓ Covered by Backup Policy (whole)

Technical Safeguards

Access Control (164.312(a)(1))
HIPAA Standard: 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).
Key Activities:

1. Analyze Workloads and Operations to Identify the Access Needs of all Users
    - ✓ Covered by Network Access and Authentication Policy, section 4.3 Account Access Levels
2. Identify Technical Access Control Capabilities
    - ✓ Covered by Network Access and Authentication Policy, section 4.3 Account Access Levels
3. Ensure that All System Users Have Been Assigned a Unique Identifier
    - ✓ Covered by Network Access and Authentication Policy, section 4.1 Access Control
4. Develop Access Control Policy
    - ✓ Covered by Network Access and Authentication Policy (whole)
5. Implement access Control Procedures Using Selected Hardware and Software
    - ✓ Covered by Network Access and Authentication Policy, section 4.3 Account Access Levels
6. Review and Update User Access
    - ✓ Covered by Network Access and Authentication Policy, section 4.5 Account Changes
7. Establish an Emergency Access Procedure
    - ✓ Covered by Contingency Planning Policy, section 4.7 Emergency Mode Operation
8. Automatic Logoff and Encryption and Decryptions
    - ✓ Covered by Network Access and Authentication Policy, section 4.7 Authentication
    - ✓ Covered by Encryption Policy, section 4.1 Applicability of Encryption
9. Terminate Access if it is No Longer Required
    - ✓ Covered by Network Access and Authentication Policy, section 4.6 Account Termination

Audit Controls (164.312(b))
HIPAA Standard: Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.
Key Activities:

1. Determine Activities that Will Be Tracked or Audited
    - ✓ Covered by Network Security Policy, section 4.3.1 Audit Trail Process
    - ✓ Covered by Network Security Policy, section 4.3.2 What to Record
2. Selected the Tools that Will Be Deployed for Auditing and System Activity Reviews
    - ✓ Covered by Network Security Policy, section 4.3.1 Audit Trail Process
3. Develop and Deploy the Information System Activity Review/Audit Policy
    - ✓ Covered by Network Security Policy, section 4.3 Audit Trails
4. Develop Appropriate Standard Operating Procedures
    - ✓ Covered by Network Security Policy, section 4.2 Logging
    - ✓ Covered by Network Security Policy, section 4.3 Audit Trails
    - ✓ Covered by Network Security Policy, section 4.3.3 Security of Audit Trails
5. Implement the Audit/System Activity Review Process
    - ✓ Covered by Network Security Policy, section 4.2 Logging

- ✓ Covered by Network Security Policy, section 4.3 Audit Trails

Integrity (164.312(c)(1)

HIPAA Standard: Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

Key Activities:

1. Identify All users Who Have Been Authorized to Access ePHI
   - ✓ Covered by Network Access and Authentication Policy, section 4.3 Account Access Levels
2. Identify Any Possible Unauthorized Sources that May Be Able to Intercept the Information and Modify it
   - ✓ Covered by Incident Response Policy, section 4.7.1 Risk Assessment
3. Develop the Integrity Policy and Requirements
   - ✓ Covered by Network Security Policy, section 4.8 File Integrity Monitoring
4. Implement Procedures to Address These Requirements
   - ✓ Covered by Network Security Policy, section 4.8 File Integrity Monitoring
5. Implement Mechanism to Authenticate ePHI
   - ✓ Covered by Network Security Policy, section 4.8 File Integrity Monitoring
6. Establish a Monitoring Process to Assess How the Implemented Process is Working
   - ✓ Covered by Network Security Policy, section 4.8 File Integrity Monitoring

Person or Entity Authentication (164.312(d))

HIPAA Standard: Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed.

Key Activities:

1. Determine Authentication Applicability to Current Systems/Applications
   - ✓ Covered by Network Access and Authentication Policy, section 4.7 Authentication
2. Evaluate Authentication Options Available
   - ✓ Covered by Network Access and Authentication Policy, section 4.7 Authentication
3. Select and Implement Authentication Option
   - ✓ Covered by Network Access and Authentication Policy, section 4.7 Authentication

Transmission Security (164.312(e)(1))

HIPAA Standard: Implement technical security policies and procedures measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network.

Key Activities:

1. Identify Any Possible Unauthorized Sources that may Be Able to Intercept and/or Modify the Information
   - ✓ Covered by Confidential Data Policy, section 4.4.2 Transmission
2. Develop and Implement Transmission Security Policy and Procedures
   - ✓ Covered by Confidential Data Policy, section 4.4.2 Transmission
3. Implement Integrity Controls
   - ✓ Covered by Confidential Data Policy, section 4.4.2 Transmission
4. Implement Encryption
   - ✓ Covered by Confidential Data Policy, section 4.4.2 Transmission

Organizational Requirements

Business Associate Contracts or Other Arrangements (164.314(a)(1))
HIPAA Standard: (i) The contract or other arrangement between the covered entity and its business associate required by § 164.308(b) must meet the requirements of paragraph (a)(2)(i) or (a)(2)(ii) of this section, as applicable. (ii) A covered entity is not in compliance with the standards in § 164.502(e) and paragraph (a) of this section if the covered entity knew of a pattern of an activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful—(A) Terminated the contract or arrangement, if feasible; or (B) If termination is not feasible, reported the problem to the Secretary.
Key Activities:

1. Contract Must Provide that Business Associates Adequately Protect ePHI
   - ✓ Covered by Business Associate Policy, section 4.4 Business Associate Agreements
2. Contract Must Provide that Business Associate's Agents Adequately Protect ePHI
   - ✓ Covered by Business Associate Policy, section 4.4 Business Associate Agreements
3. Contract Must Provide that Business Associates will Report Security Incidents
   - ✓ Covered by Business Associate Policy, section 4.4 Business Associate Agreements
4. Contract Must Provide that Business Associate Will Authorize Termination of the Contract if it has been Materially Breached
   - ✓ Covered by Business Associate Policy, section 4.4 Business Associate Agreements
5. Government Entities May Satisfy Business Associate Contract Requirements through Other Arrangements
   - ✓ Covered by Business Associate Policy, section 4.4 Business Associate Agreements
6. Other Arrangements for Covered Entities and Business Associates
   - ✓ Covered by Business Associate Policy, section 4.4 Business Associate Agreements

Requirements for Group Health Plans (164.314(b)(1)
HIPAA Standard: Except when the only electronic protected health information disclosed to a plan sponsor is disclosed pursuant to §164.504(f)(1)(ii) or (iii), or as authorized under § 164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electronic protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan.
Key Activities:

1. Amend Plan Documents of Group Health Plan to Address Plan Sponsor's Security of ePHI
   - ✓ Covered by Business Associate Policy, section 4.5 Group Health Plans
2. Amend Plan Documents of Group Health Plan to Address Adequate Separation
   - ✓ Covered by Business Associate Policy, section 4.5 Group Health Plans
3. Amend Plan Documents of Group Health Plan to Address Security of ePHI Supplied to Plan Sponsors' Agents and Subcontractors
   - ✓ Covered by Business Associate Policy, section 4.5 Group Health Plans
4. Amend Plan Documents of Group Health Plans to Address Reporting of Security Incidents
   - ✓ Covered by Business Associate Policy, section 4.5 Group Health Plans

Policies and Procedures and Documentation Requirements

Policies and Procedures (164.316(a))
HIPAA Standard: 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.
Key Activities:

1. Create and Deploy Policies and Procedures
   - ✓ Covered by Network Security Policy, section 4.21 Security Policy Management
   - ✓ Covered by Network Security Policy, section 4.21.3 Security Policy Review
2. Update Documentation of Policy and Procedures
   - ✓ Covered by Network Security Policy, section 4.21.3 Security Policy Review

Documentation (164.316(b)(1))
HIPAA Standard: (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.
Key Activities:

1. Draft, Maintain and Update Required Documentation
   - ✓ Covered by Network Security Policy, section 4.22 Documentation
2. Retain Documentation for at Least Six years
   - ✓ Covered by Network Security Policy, section 4.22 Documentation
3. Assure that Documentation is Available to those Responsible for Implementation
   - ✓ Covered by Network Security Policy, section 4.22 Documentation
4. Update Documentation as Required
   - ✓ Covered by Network Security Policy, section 4.22 Documentation

Please note: The information contained in this policy map is based on interpretation by an experienced policy professional and is believed to be correct. Please note, however, that InstantSecurityPolicy.com is not in the business in dispensing legal advice and thus any policies purchased should be reviewed for applicability to your specific situation.