Component of HIPAA Security Policy and Procedures Templates (Updated for HITECH)

Total Cost: $495

Buy Now

Our HIPAA Security policy and procedures template suite have 71 policies and will save you at least 400 work hours and are everything you need for rapid development and implementation of HIPAA Security policies. Our templates are created based on HIPAA requirements, updates from HITECH act, Omnibus rule, NIST standards and security best practices. The key objectives in formulating the policies were to ensure that they are congruent with the HIPAA Security regulations, integrate industry-established best practices for security, and are tailored to the healthcare provider environment.

Our HIPAA Security policy and procedures templates are ideally suited for following categories of organizations: covered entities and business associates.

The 71 HIPAA Security policies in the template suite (updated in May 2013 for Omnibus rule) are organized into following five major categories:

Category of HIPAA Policies & Procedures	Total HIPAA Policies and Procedures
Administrative Safeguards	31
Physical Safeguards	13
Technical Safeguards	12
Organizational Requirements	04
Supplemental Polices to required policy	11

I. HIPAA SECURITY POLICIES ON THE STANDARDS FOR ADMINISTRATIVE SAFEGUARDS		
Sr. No	**Policy**	**Description**
1	Breach Notification Policy	The purpose of this policy is to define how Covered Entity will respond to security and/or privacy incidents or suspected privacy and/or security incidents that result in a breach of protected health information (PHI).
2	Security Management Process	(Standard.) Describes processes the organization implements to prevent, detect, contain, and correct security violations relative to its ePHI.

3	Risk Analysis	Discusses what the organization should do to identify, define, and prioritize risks to the confidentiality, integrity, and availability of its ePHI. (Required Implementation Specification for the Security Management Process standard.)
4	Risk Management	Defines what the organization should do to reduce the risks to its ePHI to reasonable and appropriate levels. (Required Implementation Specification for the Security Management Process standard.)
5	Sanction Policy	Indicates actions that are to be taken against employees who do not comply with organizational security policies and procedures. (Required Implementation Specification for the Security Management Process standard.)
6	Information System Activity Review	Describes processes for regular organizational review of activity on its information systems containing ePHI. (Required Implementation Specification for the Security Management Process standard.)
7	Assigned Security Responsibility	(Standard.) Describes the requirements for the responsibilities of the Information Security Officer.
8	Workforce Security	(Standard.) Describes what the organization should do to ensure ePHI access occurs only by employees who have been appropriately authorized.
9	Authorization and/or Supervision	Identifies what the organization should do to ensure that all employees who can access its ePHI are appropriately authorized or supervised. (Required Implementation Specification for the Workforce Security standard.)
10	Workforce Clearance Procedure	Reviews what the organization should do to ensure that employee access to its ePHI is appropriate. (Addressable Implementation Specification for Workforce Security standard.)
11	Termination Procedures	Defines what the organization should do to prevent unauthorized access to its ePHI by former employees. (Addressable Implementation Specification for Workforce Security standard.)
12	Information Access Management	(Standard.) Indicates what the organization should do to ensure that only appropriate and authorized access is made to its ePHI.
13	Access Authorization	defines how the organization provides authorized access to its ePHI. (Addressable Implementation Specification for Information Access Management standard.)
14	Access Establishment and Modification	Discusses what the organization should do to establish, document, review, and modify access to its ePHI. (Addressable Implementation Specification for Information Access Management standard.)
15	Security Awareness & Training	(Standard.) Describes elements of the organizational program for regularly providing appropriate security training and awareness to its employees.

16	Security Reminders	Defines what the organization should do to provide ongoing security information and awareness to its employees. (Addressable Implementation Specification for Security Awareness & Training standard.)
17	Protection from Malicious Software	Indicates what the organization should do to provide regular training and awareness to its employees about its process for guarding against, detecting, and reporting malicious software. (Addressable Implementation Specification for Security Awareness & Training standard.)
18	Log-in Monitoring	Discusses what the organization should do to inform employees about its process for monitoring log-in attempts and reporting discrepancies. (Addressable Implementation Specification for Security Awareness & Training standard.)
19	Password Management	Describes what the organization should do to maintain an effective process for appropriately creating, changing, and safeguarding passwords. (Addressable Implementation Specification for Security Awareness & Training standard.)
20	Security Incident Procedures	(Standard.) Discusses what the organization should do to maintain a system for addressing security incidents that may impact the confidentiality, integrity, or availability of its ePHI.
21	Response and Reporting	Defines what the organization should do to be able to effectively respond to security incidents involving its ePHI. (Required Implementation Specification for Security Incident Procedures standard.)
22	Contingency Plan	(Standard.) Identifies what the organization should do to be able to effectively respond to emergencies or disasters that impact its ePHI.
23	Data Backup Plan	Discusses organizational processes to regularly back up and securely store ePHI. (Required Implementation Specification for Contingency Plan standard.)
24	Disaster Recovery Plan	Indicates what the organization should do to create a disaster recovery plan to recover ePHI that was impacted by a disaster. (Required Implementation Specification for Contingency Plan standard.)
25	Emergency Mode Operation Plan	Discusses what the organization should do to establish a formal, documented emergency mode operations plan to enable the continuance of crucial business processes that protect the security of its ePHI during and immediately after a crisis situation. (Required Implementation Specification for Contingency Plan standard.)
26	Testing and Revision Procedure	Describes what the organization should do to conduct regular testing of its disaster recovery plan to ensure that it is up-to-date and effective. (Addressable Implementation Specification for Contingency Plan standard.)

27	Applications and Data Criticality Analysis	Reviews what the organization should do to have a formal process for defining and identifying the criticality of its information systems. (Addressable Implementation Specification for Contingency Plan standard.)
28	Evaluation	(Standard.) Describes what the organization should do to regularly conduct a technical and non-technical evaluation of its security controls and processes in order to document compliance with its own security policies and the HIPAA Security Rule.
29	Business Associate Contracts and Other Arrangements	(Standard.) Describes how to establish agreements that should exist between the organization and its various business associates that create, receive, maintain, or transmit ePHI on its behalf.
30	Business Associate Agreement	(Standard.) Describes how to establish agreements that should exist between the organization and its various business associates that create, receive, maintain, or transmit ePHI on its behalf.
31	Execution of Business Associate Agreements with Contracts	Provide guidance to Covered Entity regarding execution of business associate contracts.
II. HIPAA SECURITY POLICIES ON THE STANDARDS FOR PHYSICAL SAFEGUARDS		
32	Facility Access Controls	(Standard.) Describes what the organization should do to appropriately limit physical access to the information systems contained within its facilities, while ensuring that properly authorized employees can physically access such systems.
33	Contingency Operations	Identifies what the organization should do to have formal, documented procedures for allowing authorized employees to enter its facility to take necessary actions as defined in its disaster recovery and emergency mode operations plans. (Addressable Implementation Specification for Facility Access Controls standard.)
34	Facility Security Plan	Discusses what the organization should do to establish a facility security plan to protect its facilities and the equipment therein. (Addressable Implementation Specification for Facility Access Controls standard.)
35	Access Control and Validation Procedures	Discusses what the organization should do to appropriately control and validate physical access to its facilities containing information systems having ePHI or software programs that can access ePHI. (Addressable Implementation Specification for Facility Access Controls standard.)
36	Maintenance Records	Defines what the organization should do to document repairs and modifications to the physical components of its facilities related to the protection of its ePHI. (Addressable Implementation Specification for Facility Access Controls standard.)
37	Workstation Use	(Standard.) Indicates what the organization should do to appropriately protect its workstations.

38	Workstation Security	(Standard.) Reviews what the organization should do to prevent unauthorized physical access to workstations that can access ePHI while ensuring that authorized employees have appropriate access.
39	Device and Media Controls	(Standard.) Discusses what the organization should do to appropriately protect information systems and electronic media containing PHI that are moved to various organizational locations.
40	Disposal	Describes what the organization should do to appropriately dispose of information systems and electronic media containing ePHI when it is no longer needed. (Required Implementation Specification for Device and Media Controls standard.)
41	Media Re-use	Discusses what the organization should do to erase ePHI from electronic media before re-using the media. (Required Implementation Specification for Device and Media Controls standard.)
42	Mobile Device Policy	Discusses what the organization should do specifically addressing mobile device security in support of the Device and Media Controls Standard.)
43	Accountability	Defines what the organization should do to appropriately track and log all movement of information systems and electronic media containing ePHI to various organizational locations. (Addressable Implementation Specification for Device and Media Controls standard.)
44	Data Backup and Storage	Discusses what the organization should do to backup and securely store ePHI on its information systems and electronic media. (Addressable Implementation Specification for Device and Media Controls standard.)
III. HIPAA SECURITY POLICIES ON THE STANDARDS FOR TECHNICAL SAFEGUARDS		
45	Access Control	(Standard.) Indicates what the organization should do to purchase and implement information systems that comply with its information access management policies.
46	Unique User Identification	Discusses what the organization should do to assign a unique identifier for each of its employees who access its ePHI for the purpose of tracking and monitoring use of information systems. (Required Implementation Specification for Access Control standard.)
47	Emergency Access Procedure	Discusses what the organization should do to have a formal, documented emergency access procedure enabling authorized employees to obtain required ePHI during the emergency. (Required Implementation Specification for Access Control standard.)

48	Automatic Logoff	Discusses what the organization should do to develop and implement procedures for terminating users' sessions after a certain period of inactivity on systems that contain or have the ability to access ePHI. (Addressable Implementation Specification for Access Control standard.)
49	Encryption and Decryption	Discusses what the organization should do to appropriately use encryption to protect the confidentiality, integrity, and availability of its ePHI. (Addressable Implementation Specification for Access Control standard.)
50	Audit Controls	(Standard.) Discusses what the organization should do to record and examine significant activity on its information systems that contain or use ePHI.
51	Integrity	(Standard.) Defines what the organization should do to appropriately protect the integrity of its ePHI.
52	Mechanism to Authenticate Electronic Protected Health Information	Discusses what the organization should do to implement appropriate electronic mechanisms to confirm that its ePHI has not been altered or destroyed in any unauthorized manner. (Addressable Implementation Specification for Integrity standard.)
53	Person or Entity Authentication	(Standard.) Defines what the organization should do to ensure that all persons or entities seeking access to its ePHI are appropriately authenticated before access is granted.
54	Transmission Security	(Standard.) Describes what the organization should do to appropriately protect the confidentiality, integrity, and availability of the ePHI it transmits over electronic communications networks.
55	Integrity Controls	Indicates what the organization should do to maintain appropriate integrity controls that protect the confidentiality, integrity, and availability of the ePHI it transmits over electronic communications networks. (Addressable Implementation Specification for Transmission Security standard.)
56	Encryption	Defines what the organization should do to appropriately use encryption to protect the confidentiality, integrity, and availability of ePHI it transmits over electronic communications networks. (Addressable Implementation Specification for Transmission Security standard.)
IV. ORGANIZATIONAL REQUIREMENTS		
57	Policies and Procedures	(Standard.) Defines what the requirements are relative to establishing organizational policies and procedures.
58	Documentation	(Standard.) Discusses what the organization should do to appropriately maintain, distribute, and review the security policies and procedures it implements to comply with the HIPAA Security Rule

59	Isolating Healthcare Clearinghouse Function	Purpose is to implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization (Required Implementation Specification for Information Access Management standard.)
60	Group Health Plan Requirements	(Standard.) The purpose is to ensure that reasonable and appropriate safeguards are maintained on electronic protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan.
V. SUPPLEMENTAL POLICIES FOR REQUIRED POLICIES		
61	Wireless Security Policy	The purpose is to implement security measures sufficient to reduce risks and vulnerabilities of the wireless infrastructure.
62	Email Security Policy	The purpose is to establish management direction, procedures, and requirements to ensure safe and successful delivery of e-mail.
63	Analog Line Policy	The purpose is to explains Company's analog and ISDN line acceptable use and approval policies and procedures.
64	Dial-in Access Policy	The purpose is to implement security measures sufficient to reduce risks and vulnerabilities of dial-in connections to the enterprise infrastructure
65	Automatically Forwarded Email Policy	The purpose is to prevent the unauthorized or inadvertent disclosure of sensitive company information.
66	Remote Access Policy	The purpose is to implement security measures sufficient to reduce risks and vulnerabilities of remote access connections to the enterprise infrastructure.
67	Ethics Policy	The purpose is to establish a culture of openness, trust and integrity in business practices.
68	VPN Security Policy	The purpose is to implement security measures sufficient to reduce the risks and vulnerabilities of the VPN infrastructure
69	Extranet Policy	The purpose is to describes the policy under which third party organizations connect to Company's networks for the purpose of transacting business related to Company
70	Internet DMZ Equipment Policy	The purpose is to define standards to be met by all equipment owned and/or operated by Company located outside Company's corporate Internet firewalls.
71	Network Security Policy	The purpose is to establish requirements for information processed by computer networks.

HIPAA Privacy Policies, Forms & Procedures

Total Cost: $300

Buy Now

Following are the 57 HIPAA Privacy forms, policies and procedures included in the HIPAA Privacy Policy & procedures template suite. These templates are updated for the HITECH act of 2009 and Omnibus rule of 2013. The policies can be used by any covered entity & business associate. All policies are available in MS Word format and can be easily customized as per your requirements. Each template is presented in a standard format reflecting critical organizational functions to consider in HIPAA remediation.

These HIPAA Privacy Policies cover areas like:

1) General policies regarding use and disclosure of PHI

2) Minimum necessary rule for use and disclosure of PHI

3) Patient rights regarding their own PHI

4) Uses and disclosures not requiring patient authorization

5) Special cases for restriction of uses and disclosures of PHI

6) Organizational issues and safeguards

The templates suite includes following HIPAA Privacy forms, policies and procedures.

- Accept Access Request
- Accounting for Disclosures
- Acknowledgement of Receipt
- Amendment to Record Form
- Authorization for Release of Protected Health Information
- Authorization To Use Disclose Protected Health Information
- Business Associate Agreement
- Business Associate Contracts and Other Arrangements

- Complaint Process
- Data Use Agreement Template
- De-identified Information and Limited Data Sets
- Denial Access Request
- Denial Request to Amend Form
- Disclosure Accounting Log for Medical Information
- Disclosure of PHI with and without authorization Template
- Disclosures Record Form
- Document Retention Requirements
- EHR accounting of disclosures
- Employee Confidentiality Agreement
- Execution of Business Associate Agreements with Contracts
- Health Plan Notice of Privacy Practices
- HIPAA Accept Amend Request Form
- Identifying PHI and Designated Record Sets
- Minimum Necessary
- Multi-Organization Arrangements
- Notice of Privacy Practices
- Patient Right to Access PHI
- PHI Release by Whistleblowers
- Privacy Officer
- Receipt of Payment when Disclosing PHI
- Release for Abuse Neglect or Domestic Violence
- Release for Confidential Communications
- Release for Fundraising Purposes
- Release for Health Oversight
- Release for Judicial or Administrative Proceedings
- Release for Law Enforcement
- Release for Marketing Purposes
- Release for Public Health
- Release for Research Purposes
- Release for Specific Government Functions
- Release for Workers Compensation
- Release of Information for Deceased Patients or Plan Members
- Release of Information for Legal Representatives
- Release of Information to a Minor
- Release of Information to a Minor's Parents
- Release of Information to Friends and Family Members
- Release of Psychotherapy Notes
- Release to Avert Serious Threat to Safety

- Request Confidential Communications Template
- Request Restriction
- Request to Amend Patient or Plan Member Record
- Requests for Restriction policy
- Required PHI Disclosures
- Right to Object to Release for Certain Purposes
- Safeguarding PHI
- Training Requirements
- Workforce Sanctions