



## HIPAA Security Policies & Procedures (HITECH updated)

---

### Why Create HIPAA Security Policies and Procedures?

The final HIPAA Security rule published on February 20, 2003 requires that healthcare organizations create HIPAA Security policies and procedures to apply the security requirements of the law — and then train their employees on the use of these policies and procedures in their day-to-day jobs. American Recovery and Reinvestment Act of 2009 (ARRA)'s HITECH act requires business associates to comply with security rule.

HIPAA rule has very specific requirements with regard to creating, implementing, or changing Policies and Procedures.

“Standard: Policies and Procedures -- A covered entity must implement policies and procedures with respect to protected health information that are designed to comply with the standards, implementation specifications, or other requirements of this subpart. The policies and procedures must be reasonably designed, taking into account the size of and the type of activities that relate to protected health information undertaken by the covered entity, to ensure such compliance. This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirement of this subpart.”

Likewise, any changes to your Policies and Procedures must be made in accordance with HIPAA regulations, and must reflect future changes in HIPAA (and other applicable) law: “Standard: Changes to Policies or Procedures -- A covered entity must change its policies and procedures as necessary and appropriate to comply with changes in the law, including the standards, requirements, and implementation specifications of this subpart.”

Developing or revising your organization’s security policies and procedures is a major task that takes time and attention to detail. Each policy must specifically reflect the Security regulations’ complex requirements, yet be worded simply enough to be understood and applied across the entire organization. Each security policy must set the foundation for the individual departmental procedures needed to support and implement the policy.

### Our HIPAA Security Policies and Procedures Templates/forms

We have developed 68 security policies which include 57 security policies & procedures required by HIPAA Security regulation and additional 11 policies, checklist and forms as supplemental documents to the required policies. These policies meet the challenges of creating enterprise-wide security policies. The suite addresses all major components of the HIPAA Security Rule and each policy can be adopted or customized based on your organization’s needs.

Category of HIPAA Policies & Procedures	Total HIPAA Policies and Procedures
Administrative Safeguards	29
Physical Safeguards	12
Technical Safeguards	12
Organizational Requirements	04
Supplemental Polices to required policy	11

Developed by certified security specialists with healthcare experience, the policies are mapped to HIPAA requirements,



## **HIPAA Security Policies & Procedures (HITECH updated)**

---

HITECH act new requirements (2009), based on security industry best practices and standards, and fine-tuned to the healthcare environments. The templates are intended to serve as the cornerstone of your security program.

The policies support the Security Rule's provisions for "scalability," meaning that they can be adjusted to the size and scope of the covered entity. Our HIPAA Security policies and procedures templates will save you at least 400 work hours and are everything you need for rapid development and implementation of policies. Our templates are created based on HIPAA requirements, NIST standards, ISO 17799 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.

### **Who should use our HIPAA Security Policy Template Suite?**

Our HIPAA policies and procedures templates are ideally suited for following categories of organizations: Hospital, Long Term Care organizations, Health Plans, Insurance Companies, Third Party Administrators, Clearing Houses, Physicians, County Government and State Agencies.

We would encourage Business Associates to also use our HIPAA Security Policy and templates as a better business practice. Using these policies helps in showing client your commitment of exceeding the HIPAA requirements and gaining the confidence of client and their business. With the HITECH act, Business Associates are now required to be HIPAA compliant by Feb 2010.

Purchasing the templates for these policies can save your organization thousands of dollars by avoiding customized development fees plus you gain the assurance that the policies were developed by the recognized leader in HIPAA compliance.

### **Easy to Customize Templates**

Our templates fully meet the requirements of the HIPAA Security Rules and guidelines. However, they are only a starting point for creating finished HIPAA Policies and Procedures specific to your organization. As with any "model" documents or forms, you will need to open each document and customize it to meet your unique needs. The Supremus Group cannot and does not assume any legal liability for the final Policies and Procedures you create from the model documents.

All the templates are available in MS Word document. You can modify the template as needed for your organization, including placing the name of your organization in the template and modifying it in any way that you feel is required to customize it for your situation. These templates will be sent by e-mail to you in zip file.

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

Our HIPAA Security policy and procedures template suite have 68 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, NIST standards, ISO 17799 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.



## HIPAA Security Policies & Procedures (HITECH updated)

Our HIPAA Security policy and procedures templates are ideally suited for following categories of organizations: Hospital, Long Term Care organizations, Health Plans, Insurance Companies, Third Party Administrators, Clearing Houses, Physicians, County Government, State Agencies, Business associates and other payor & providers.

The 68 HIPAA Security policy in the template suite (updated in July 2011 for HITECH act) are organized into following five major categories:

Category of Policies & Procedures	Total Policies and Procedures
Administrative Safeguards	29
Physical Safeguards	12
Technical Safeguards	12
Organizational Requirements	04
Supplemental Polices to required policy	11

I. HIPAA SECURITY POLICIES ON THE STANDARDS FOR ADMINISTRATIVE SAFEGUARDS		
S.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.



## HIPAA Security Policies & Procedures (HITECH updated)

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.)



## HIPAA Security Policies & Procedures (HITECH updated)

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.
<b>II. HIPAA SECURITY POLICIES ON THE STANDARDS FOR PHYSICAL SAFEGUARDS</b>		
30	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.



## HIPAA Security Policies & Procedures (HITECH updated)

31	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.)
32	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.)
33	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.)
34	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.)
35	Workstation Use	(Standard.) Indicates what the organization should do to appropriately protect its workstations.
36	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.
37	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.
38	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.)
39	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.)
40	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.)
41	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.)



## HIPAA Security Policies & Procedures (HITECH updated)

III. HIPAA SECURITY POLICIES ON THE STANDARDS FOR TECHNICAL SAFEGUARDS		
42	Access Control	(Standard.) Indicates what the organization should do to purchase and implement information systems that comply with its information access management policies.
43	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.)
44	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.)
45	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.)
46	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.)
47	Audit Controls	(Standard.) Discusses what the organization should do to record and examine significant activity on its information systems that contain or use ePHI.
48	Integrity	(Standard.) Defines what the organization should do to appropriately protect the integrity of its ePHI.
49	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.)
50	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.
51	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.
52	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.)



## HIPAA Security Policies & Procedures (HITECH updated)

53	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.)
<b>IV. ORGANIZATIONAL REQUIREMENTS</b>		
54	Policies and Procedures	(Standard.) Defines what the requirements are relative to establishing organizational policies and procedures.
55	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
56	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.)
57	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.
<b>V. SUPPLEMENTAL POLICIES FOR REQUIRED POLICIES</b>		
58	Wireless Security Policy	The purpose is to implement security measures sufficient to reduce risks and vulnerabilities of the wireless infrastructure.
59	Email Security Policy	The purpose is to establish management direction, procedures, and requirements to ensure safe and successful delivery of e-mail.
60	Analog Line Policy	The purpose is to explain Company's analog and ISDN line acceptable use and approval policies and procedures.
61	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
62	Automatically Forwarded Email Policy	The purpose is to prevent the unauthorized or inadvertent disclosure of sensitive company information.
63	Remote Access Policy	The purpose is to implement security measures sufficient to reduce risks and vulnerabilities of remote access connections to the enterprise infrastructure.
64	Ethics Policy	The purpose is to establish a culture of openness, trust and integrity in business practices.



## HIPAA Security Policies & Procedures (HITECH updated)

---

65	VPN Security Policy	The purpose is to implement security measures sufficient to reduce the risks and vulnerabilities of the VPN infrastructure
66	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
67	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.
68	Network Security Policy	The purpose is to establish requirements for information processed by computer networks.

**View Sample HIPAA Security Policy**

**Effective Date of This Revision:**      October 11, 2011



## HIPAA Security Policies & Procedures (HITECH updated)

---

<b>Contact:</b>	HIPAA Chief Security Officer	Responsible Department:
	"Insert Addressee Here"	
	"Insert Street Address Here"	
	"Insert Phone Number Here"	

### HIPAA REGULATORY INFORMATION: Workforce Security Standard

<b>Category:</b>	<input checked="" type="checkbox"/> Administrative Safeguard	<b>Type:</b>	<input type="checkbox"/> Standard
	<input type="checkbox"/> Physical Safeguard		<input checked="" type="checkbox"/> Implementation Specification
	<input type="checkbox"/> Technical Safeguard		<input type="checkbox"/> Required <input checked="" type="checkbox"/> Addressable

<b>Applies to:</b>	<input checked="" type="checkbox"/> Officers	<input checked="" type="checkbox"/> Staff/ Faculty	<input checked="" type="checkbox"/> Student clinicians	<input checked="" type="checkbox"/> Volunteers
	<input checked="" type="checkbox"/> Other agents	<input type="checkbox"/> Visitors	<input checked="" type="checkbox"/> Contractors	

### BACKGROUND:

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that access to Protected Health Information (PHI) will be managed to guard the integrity, confidentiality, and availability of electronic PHI (ePHI) data. According to the law, all "Covered Entity's Name" officers, employees and agents of units within a "Covered / Hybrid" Entity must preserve the integrity and the confidentiality of individually identifiable health information (IIHI) pertaining to each patient or client.

### SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:

*"Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) [Workforce Clearance Procedure] of this section."*

### PURPOSE:

Each Unit of "Covered Entity's Name" 's health care component (HCC), which handles ePHI, will have a documented process for terminating access to ePHI when the employment of workforce members ends or access is no longer appropriate as set forth in "Covered Entity's Name" 's Workforce Clearance Procedure implemented specification ("Policy Number" ), Information Access Management standard ("Policy Number" ) and Access Establishment and



## HIPAA Security Policies & Procedures (HITECH updated)

---

Modification implementation specification ("Policy Number" ), for example due to a change in position such that the workforce member no longer requires access to ePHI.

This policy provides guidance for "Covered Entity's Name" 's Security Office in adopting the addressable Termination Procedure Implementation Specification under the Workforce Security Standard [C.F.R. 164.308(a)(3)(i)].

### POLICY:

When a "Covered Entity's Name" 's workforce member will be ending their relationship with the covered entity, the affected Human Resources department and the workforce member's supervisor will give reasonable notice to the "Covered Entity's Name" HIPAA Security Compliance Officer, who will then plan the termination of access to the ePHI for the departing workforce member once s/he leaves in accordance with "Covered Entity's Name" 's Access Establishment and Modification policy ("Policy Number" ) and document all modifications in the Access Authorization Sheet

Each Unit of "Covered Entity's Name" 's (HCC) will log, track, and securely maintain receipts and responses to such termination of access notices, including the following information:

- Date and time of notice of *workforce member* departure received
- Date of planned *workforce member* departure
- Description of access to be terminated
- Date, time, and description of actions taken

When workforce members end their relationship with "Covered Entity's Name" , all privileges to access ePHI Systems, including both internal and remote information system privileges, will be disabled or removed by the time of departure, or if not feasible, as soon thereafter as possible.

When "Covered Entity's Name" workforce members need to be terminated immediately, "Covered Entity's Name" and/or "Covered Entity's Name" 's HCC will remove or disable their information system privileges before they are notified of the termination, when feasible. Information system privileges include workstations and server access, data access, network access, email accounts, and inclusion on group email lists.

Physical access to areas where ePHI is located will be terminated as appropriate in accordance with "Covered Entity's Name" 's Access Establishment and Modification policy ("Policy Number" )"Covered Entity's Name" 's HCC will be alert to situations where workforce members are terminated and may pose risks to the security of ePHI following the Facility Security Plan ("Policy Number" ).

"Covered Entity's Name" 's workforce members will have their ePHI information system privileges disabled after their access methods or user IDs have been inactive for "Number of Days" . "Covered Entity's Name" HIPAA Security Compliance Office will review privileges that are disabled due to inactivity and take the necessary steps to determine the cause of the inactivity. If inactivity is due to termination of employment, "Covered Entity's Name" will promptly terminate all information system privileges and notify appropriate "Covered Entity's Name" personnel to terminate physical access to areas where ePHI is located. If inactivity is due to other causes, "Covered Entity's Name" will complete a review and take



## HIPAA Security Policies & Procedures (HITECH updated)

---

measures to terminate, limit, suspend, or maintain the workforce member's access, as appropriately documented in "Covered Entity's Name" 's Access Establishment and Modification policy ("Policy Number" )

Each Unit of "Covered Entity's Name" 's HCC will ensure that cryptographic keys are recovered and made available to the appropriate managers or administrators if departing workforce members have used cryptography on ePHI.

A workforce member who ends employment with "Covered Entity's Name" will not retain, give away, or remove from "Covered Entity's Name" 's premises any ePHI. At the time of his or her departure, a workforce member will provide ePHI in his or her possession to his or her supervisor. "Covered Entity's Name" reserves the right to pursue any and all remedies against workforce members who violate this provision. Departing workforce members' supervisors will determine the appropriate handling of any ePHI that departing workforce members possess, in accordance with "Covered Entity's Name" 's Device and Media Controls policy ("Policy Number" ).

"Covered Entity's Name" will deactivate or change physical security access codes used to protect ePHI Systems of departing workforce members, when known.

Each Unit of "Covered Entity's Name" 's HCC will implement a documented procedure for return of supplied equipment and property that contains or allows access to ePHI, and will disable and remove access to ePHI Systems held by the workforce member, by the time of, or if not feasible, immediately after, the workforce member's departure.

Each Unit of "Covered Entity's Name" 's HCC will track and log the return of equipment and property containing or having the ability to access ePHI with the workforce member's name, date and time equipment and property was returned, and identification of returned items, and will securely maintain the tracking and logging information on the Inventory tracking sheet. The equipment and property that may contain, or allow or enable the workforce member to access ePHI may include, but is not limited to:

- Portable computers
- Personal Digital Assistants (PDAs)
- Name tags or name identification badges
- Security tokens
- Access Cards
- Building, desk, or office keys
- DVD, CD-Rom, Flash Drives etc.

### **ACTION:**

#### *Voluntary Termination (Resignation)*

Voluntary termination comes as a result of a workforce member resigning from his/her position. Notice of resignation may be verbal or in writing (preferred).



## HIPAA Security Policies & Procedures (HITECH updated)

---

Steps are as follows:

1. Workforce member notifies "Covered Entity's Name" or supervisor of resignation.
2. "Covered Entity's Name" or supervisor notifies Human Resources within 24 Hours of receipt of resignation. If the workforce member's work location is at a remote location, the notice of resignation will be faxed to Human Resources.
3. "Covered Entity's Name" or supervisor will provide Human Resources with the workforce member's last hours of work to be paid (if a paid position).
4. Human Resources will notify Payroll of termination; pull workforce member's personnel record (if appropriate); and schedule an exit interview with the workforce member (if appropriate).
5. Payroll will produce workforce member's final paycheck within appropriate timeframe and forward to Human Resources for distribution (if a paid position). Payroll will ensure the workforce member receives all pay legally required (e.g. wages, vacation payoff, etc.; if paid position).
6. Human Resources will secure the final paycheck. For workforce members working remotely, Human Resources will forward final pay to workforce member's supervisor or mail directly to the workforce member's home if the workforce member requests.
7. "Covered Entity's Name" or supervisor will notify the security officer or designee and request termination of all access to "Covered Entity's Name" systems and facilities no later than the date of termination, especially remote access to "Covered Entity's Name" network and systems
8. Human Resources will review the workforce member's separation file for completeness and forwards remaining legal notices to workforce member as applicable (e.g., COBRA, 401K, etc.).

### Involuntary Termination (Discharge Or Lay-Off):

Involuntary termination/separation may occur under two (2) circumstances: Discharge or Lay-Off. All involuntary terminations are to be reviewed by "Covered Entity's Name", designee or the Human Resources Department prior to taking any action.

**Discharge** – Discharge normally occurs due to misconduct (breach of company policy or procedure) or substandard work performance. Workforce members terminated for misconduct may not be eligible for rehire. Workforce members terminated for sub-standard work performance may be considered eligible for rehire if the performance-related problem occurs through no direct fault of the workforce member and they have demonstrated a willingness to reapply for another position within the company for which they may be better qualified. In all cases, the decision to rehire a former discharged workforce member remains at the sole discretion of "Covered Entity's Name".

Steps are as follows:



## HIPAA Security Policies & Procedures (HITECH updated)

---

1. Supervisor compiles all documentation to support termination and forwards the documentation to “Covered Entity’s Name” or designee prior to taking any action.
2. “Covered Entity’s Name” or designee will review the documentation submitted and consults with Human Resources regarding appropriateness and fairness of separation. “Covered Entity’s Name” will notify the supervisor of the action to be taken.
3. If discharge is approved, the supervisor will notify Human Resources the workforce member’s last working day and total hours worked that pay period (if in a paid position).
4. Human Resources will notify Payroll of termination, pull the workforce member’s personnel record (if applicable) and assist the supervisor prepare for involuntary termination.
5. Payroll will produce workforce member’s final paycheck within appropriate timeframe and forward to Human Resources for distribution (if a paid position). Payroll will ensure the workforce member receives all pay legally required (e.g. wages, vacation payoff, etc.; if paid position).
6. Human Resources will secure the final paycheck (if a paid position). For workforce members working remotely, Human Resources will forward final pay to the workforce member’s supervisor who may be required to travel to workforce member’s work location to complete involuntary termination.
7. “Covered Entity’s Name” or supervisor will notify the security officer or designee to terminate all access to “Covered Entity’s Name” network, systems and facilities no later than the date and prior to the time of the termination, especially remote access to “Covered Entity’s Name” computing systems
8. “Covered Entity’s Name” or supervisor will meet with the workforce member in private and inform the workforce member the reason for termination. If the workforce member works at a remote location, “Covered Entity’s Name” or supervisor will deliver the final paycheck at time of discharge (if a paid position).
9. If the workforce member works at “Covered Entity’s Name”’s facility, the supervisor will deliver the final paycheck at time of discharge (if a paid position)
10. Human Resources will reviews the workforce member’s separation file for completeness and forwards remaining legal notices to employee (e.g., COBRA, 401k, etc.).
11. If the reason for involuntary discharge is criminal in nature, “Covered Entity’s Name” or designee will confer with legal counsel and notify law enforcement and regulatory governmental agencies if appropriate.

**Workforce Reduction (lay off):** “Covered Entity’s Name” attempts to provide a work environment of growth and job security for its workforce members. However, due to economic or other issues, it may be necessary to reduce the size of the workforce. It is “Covered Entity’s Name”’s policy to affect the required workforce reduction in a fair and just manner.

1. Preliminary Measures
  - a. Affected workforce members will be encouraged to apply for transfer to other open positions if available.
  - b. Paid workforce members may be asked to reduce their scheduled work hours or use accrued paid time off.
2. Permanent Reduction in Force
  - a. The identification of affected workforce member(s) will be made by the “Covered Entity’s Name”, designee and, if applicable, reviewed by Human Resources.



## HIPAA Security Policies & Procedures (HITECH updated)

---

- b. The decision regarding which workforce members are affected shall be based on a combination of factors, including but not limited to:
  - i. Requirements of “Covered Entity’s Name” operations
  - ii. Documented qualifications to perform the work required
  - iii. Documented performance levels
  - iv. Documented counseling
  - v. Seniority in “Covered Entity’s Name” organization, based on actual hire date.
- c. Workforce members affected will be terminated from the active payroll and have no recall rights [*“Covered Entity’s Name” needs to take into account union or other contracts that may impact the “no recall rights” clause*]. However, they may apply for any open position for which they are qualified, and may be considered for re-employment as any other applicant. “Covered Entity’s Name” or “Covered Entity’s Name” management retains the right to offer any available job to the candidate who is best qualified based on skills, experience and education.
- d. Affected workforce members will receive all benefits as upon any termination, such as payout of all accrued paid time off and COBRA continuation of benefits (if a paid position).
- e. Severance Pay may be available to the affected workforce members. Severance Pay is designed to assist affected workforce members in their transition, according to the following guidelines:
  - i. Eligibility for Severance Pay is limited to regularly scheduled full-time and part-time employees. Temporary or volunteer staff are not eligible for Severance Pay. Contracted staff are governed by their specific contract.
  - ii. The amount of Severance Pay is based on [*“Covered Entity’s Name” severance pay basis, if any*].
  - iii. Severance Pay will be paid in one lump sum with all deductions, on the last day of employment, along with accrued paid time off, if any.
  - iv. If the affected employee refuses an offer of another position within the “Covered Entity’s Name” organization which is paid within 10% of his/her current base rate, and is located within a reasonable distance from the current job, Severance Pay will be denied.
  - v. If the affected employee returns to regular employment within one month of the original reduction in workforce, he/she may retain all prior seniority and benefits only if all Severance pay is returned at the time of rehire.
  - vi. Employees may voluntarily elect to be eliminated from the workforce to save another co-worker’s job, and will receive Severance Pay if otherwise eligible. However, “Covered Entity’s Name” reserves the right to refuse such offers based on “Covered Entity’s Name”’s needs.
  - vii. As with all policies, “Covered Entity’s Name” may modify, change, or eliminate this policy at any time, with or without notice.

Steps are as follows:

1. “Covered Entity’s Name” or supervisor will consult with appropriate senior management and Human Resources immediately when a workforce reduction is anticipated.
2. “Covered Entity’s Name” or supervisor will identify affected workforce members and validate with Human Resources to ensure compliance with the Workforce Reduction Policy.
3. Human Resources will determine whether notice or Severance Pay is appropriate.
4. “Covered Entity’s Name” or supervisor will meet with affected workforce member and provide them written notice of intent to lay-off and will provide as much notice as possible to all affected workforce members.
5. “Covered Entity’s Name” or supervisor will meets with remaining workforce members if appropriate and explains lay-off procedure and future effect.



## **HIPAA Security Policies & Procedures (HITECH updated)**

---

6. On the day before the effective date of the lay-off, "Covered Entity's Name" or supervisor will forward to Human Resources the workforce member's last working day and total hours worked that pay period (if in a paid position).
7. Payroll will produce workforce member's final paycheck within appropriate timeframe and forward to Human Resources for distribution (if a paid position). Payroll will ensure the workforce member receives all pay legally required (e.g. wages, vacation payoff, etc.; if paid position).
8. Human Resources will secure the final paycheck (if a paid position). For workforce members working remotely, Human Resources will forward final pay to the workforce member's supervisor or to the workforce member's home, if requested by the workforce member.
9. "Covered Entity's Name" or supervisor will meet with workforce member(s) on the workforce member's last day and individually communicate with all impacted workforce members and distribute final paychecks (if a paid position).
10. "Covered Entity's Name" or supervisor will notify the security officer or designee to terminate all access to "Covered Entity's Name" network, systems and facilities no later than the date of termination, especially remote access to "Covered Entity's Name" computing systems.
11. Human Resources will distribute final paychecks and conducts exit Interviews, if appropriate.

### Involuntary or Voluntary Termination of Relationship with Third Party Affiliates:

Relationship termination of a relationship with a third party affiliate may occur because of contract or affiliation termination/non-renewal, joint agreement to terminate affiliation or because of misconduct on the part of the third party affiliate. Under all circumstances, termination to "Covered Entity's Name" network, systems and facilities is required upon termination of the relationship.

Steps are as follows:

1. "Covered Entity's Name" will discuss with legal counsel any involuntary termination of affiliation with a third party to determine what steps are necessary such as notice in advance, contract termination, etc.
2. Following consultation with legal counsel, "Covered Entity's Name" will notify affiliated third party of the termination of the relationship and the reason for termination.
3. The affiliated third party may also sever the relationship with "Covered Entity's Name" with notice to "Covered Entity's Name", taking account of legal requirements related to any contractually agreements that may have been entered into between "Covered Entity's Name" and affiliated third party.
4. "Covered Entity's Name" or supervisor will notify the security officer or designee to terminate all access to "Covered Entity's Name" network, systems and facilities no later than the date of relationship termination, especially remote access to "Covered Entity's Name" computing systems.
5. "Covered Entity's Name" will require the return of any portable devices, media or other hardware or software that is the property of the "Covered Entity's Name" from the affiliated third party and take necessary legal steps if affiliated third party refuses to return "Covered Entity's Name" assets/ property.
6. If termination of the relationship is involuntary due to misconduct/violation of "Covered Entity's Name"'s privacy and security standards, the security officer or designee will terminate access on the date of termination but prior to the time of termination, especially to remote systems.
7. If the reason for involuntary relationship termination is criminal in nature, "Covered Entity's Name" or designee will confer with legal counsel and notify law enforcement and regulatory governmental agencies if appropriate.



## HIPAA Security Policies & Procedures (HITECH updated)

---

### DEFINITIONS:

HIPAA: Health Insurance Portability and Accountability Act of 1996

Electronic Protected Health Information (ePHI): Electronic health information or health care payment information, including demographic information collected from an individual, which identifies the individual or can be used to identify the individual. ePHI does not include students records held by educational institutions or employment records held by employers.

Individually Identifiable Health Information (IIHI): Information that is a subset of health information, including demographic information collected from an individual, and:

- Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
- Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
- That identifies the individual; or
- With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

"Covered Entity's Name" Health Care Component (HCC): Those units of "Covered Entity's Name" that have been designated by the "Covered Entity's Name" as part of its health care component under HIPAA.

"Covered Entity's Name" Security Officer: the individual appointed by "Covered Entity's Name" to be the HIPAA Security Officer under s. 164.306(2) of the HIPAA Security Rule.

Addressable: When a standard adopted under 45 CFR Part 164.312 includes addressable implementation specifications, a unit within the "Covered Entity's Name" HCC must (i) assess whether each implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting the unit's electronic ePHI and (ii) as applicable to the unit: (A) implement the implementation specification if reasonable and appropriate; or (B) if implementing the implementation specification is not reasonable and appropriate: (1) document why it would not be reasonable and appropriate to implement the implementation specification; and (2) implement an equivalent alternative measure if reasonable and appropriate.



## **HIPAA Security Policies & Procedures (HITECH updated)**

---

### **Related Policies:**

Access Establishment and Modification ("Policy Number" )  
"Covered Entity's Name" Confidentiality Agreement  
Information Access Management Standard ("Policy Number" )

### **Reference:**

Access to Electronic Health Information Flow Sheet  
Access Authorization ("Policy Number" )  
"Covered Entity's Name" Confidentiality Agreement  
HIPAA Final Security Rule, 45 CFR Parts 160, 162, and 164, Department of Health and Human Services, <http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/default.asp>, February 20, 2003.  
CMS, "CMS Information Systems Security Policy, Standards and Guidelines Handbook", CMS, February 2002.  
International Standards Organization (ISO/IEC 17799:2000(E))

### **View HIPAA Security Policy Template's License**

[http://www.training-hipaa.net/template\\_suite/SP\\_policy\\_agreement.htm](http://www.training-hipaa.net/template_suite/SP_policy_agreement.htm)

### **Buy Now \$495**

<http://www.supremusstore.com/SearchResults.asp?Cat=5>