

# Security Policies - Table of Contents

## Table of Contents (Policies & Procedures)

| <u>Description</u> | <u>Policy Number</u> |
|--------------------|----------------------|
|--------------------|----------------------|

### POLICIES

#### **ADMINISTRATIVE SAFEGUARDS**

|   |      |
|---|------|
| General Guidelines to Safeguard Protected Health Information  | 2025 |
| Risk Analysis and Ongoing Risk Management   | 2030 |
| Sanctions for Violating Privacy and Security Policies and Procedures  | 2035 |
| Activity Review of Information System Security  | 2040 |
| Assignment of Security Responsibility   | 2045 |
| Assignment and Management of Information Access Privileges  | 2050 |
| Termination or Modification of Access to Protected Health Information: Facility Controls and Electronic Systems | 2055 |
| Training Program: Security Awareness and Training to Safeguard Electronic Protected Health Information          | 2060 |
| Security Incident Procedures: Response and Reporting  | 2065 |
| Contingency Planning: Response to Unexpected Negative Events  | 2070 |
| Evaluation of the Security of Protected Health Information  | 2075 |
| Business Associates Contracts and Other Arrangements  | 2080 |
| Maintenance of Privacy and Security Policies and Procedures   | 2085 |

#### **PHYSICAL SAFEGUARDS**

|   |      |
|---|------|
| Assignment of Facility Access Controls or Privileges    | 2125 |
| Polices and Guidelines on Work Station Use and Security | 2130 |
| Device and Media Controls                               | 2135 |

#### **TECHNICAL SAFEGUARDS**

|   |      |
|---|------|
| Access Control                                      | 2225 |
| Audit Controls                                      | 2230 |
| Integrity   | 2235 |
| Authentication of Person or Entity                  | 2240 |
| Electronic Transmission Security of PHI             | 2245 |
| E-Mail and Protected Health Information             | 2250 |
| Facsimile Machines and Protected Health Information | 2255 |

# Security Policies - Table of Contents

## HIPAA Security P&P Checklist

|   | Have it already? | Customize Template | Refine with Team | Final Draft | Training Complete |
|---|------------------|--------------------|------------------|-------------|-------------------|
| <b>Administrative Safeguards</b>  |                  |                    |                  |             |                   |
| General Guidelines to Safeguard Protected Health Information  |                  |                    |                  |             |                   |
| Risk Analysis and Ongoing Risk Management   |                  |                    |                  |             |                   |
| Sanctions for Violating Privacy and Security Policies and Procedures  |                  |                    |                  |             |                   |
| Activity Review of Information System Security  |                  |                    |                  |             |                   |
| Assignment of Security Responsibility   |                  |                    |                  |             |                   |
| Assignment and Management of Information Access Privileges  |                  |                    |                  |             |                   |
| Termination or Modification of Access to Protected Health Information: Facility Controls and Electronic Systems |                  |                    |                  |             |                   |
| Training Program: Security Awareness and Training to Safeguard Electronic Protected Health Information          |                  |                    |                  |             |                   |
| Security Incident Procedures: Response and Reporting  |                  |                    |                  |             |                   |
| Contingency Planning: Response to Unexpected Negative Events  |                  |                    |                  |             |                   |
| Evaluation of the Security of Protected Health Information  |                  |                    |                  |             |                   |
| Business Associates Contracts and Other Arrangements  |                  |                    |                  |             |                   |
| Maintenance of Privacy and Security Policies and Procedures   |                  |                    |                  |             |                   |
| <b>Physical Safeguards</b>  |                  |                    |                  |             |                   |
| Assignment of Facility Access Controls or Privileges  |                  |                    |                  |             |                   |
| Policies and Guidelines on Work Station Use and Security  |                  |                    |                  |             |                   |
| Device and Media Controls   |                  |                    |                  |             |                   |
| <b>Technical Safeguards</b>   |                  |                    |                  |             |                   |
| Access Control  |                  |                    |                  |             |                   |
| Audit Controls  |                  |                    |                  |             |                   |
| Integrity   |                  |                    |                  |             |                   |
| Authentication of Person or Entity  |                  |                    |                  |             |                   |
| Electronic Transmission Security of PHI   |                  |                    |                  |             |                   |
| E-Mail and Protected Health Information   |                  |                    |                  |             |                   |
| Facsimile Machines and Protected Health Information   |                  |                    |                  |             |                   |

## EXAMPLE - POLICY & PROCEDURE

|   |   |
|---|---|
| <b>Practice:</b> Organization Name                | <b>Effective Date:</b> April 14, 2005                 |
| <b>Title:</b> General Guidelines To Safeguard PHI | <b>Date Revised:</b> April 14, 2005                   |
| <b>Policy Number:</b> 2025                        | <b>Reference:</b> 45 CFR § 164.308(a)(1)(ii)(A) & (B) |

### TITLE: GENERAL GUIDELINES TO SAFEGUARD PHI

**RESPONSIBILITY:** Security Official, Privacy Official, and all members of the *workforce*

### **BACKGROUND:**

The following guidelines are in accordance with the final Security Rule and consistent with the HIPAA privacy requirement to safeguard protected health information (PHI). See 45 CFR § 164.530(c). These are simple procedures that can be implemented at the start of the HIPAA compliance process. Use of these guidelines will improve the security of *protected health information*, and will also increase workforce awareness of the importance of keeping protected health information private.

For the most part, there are no specific requirements in HIPAA regulations to do the things listed in these guidelines. Rather, HIPAA leaves it to each *covered entity* to identify and implement practical steps such as these to achieve the general limitations on the use and disclosure of protected health information (PHI) that permeate the regulations. Modify these guidelines, as necessary, to fit the needs of your organization.

### **POLICY:**

[ENTITY] will use reasonable administrative, physical, and technical safeguards to protect the privacy of protected health information and limit incidental uses or disclosures of protected health information. An incidental *use* or *disclosure* is a secondary use or disclosure that cannot reasonably be prevented, is limited in nature, and that occurs as a by-product of an otherwise permitted use or disclosure. For example: a conversation that is overheard despite attempts by the speakers to avoid being heard.

All members of the [ENTITY] workforce will follow these guidelines in handling protected health information (PHI) in order to protect the privacy of protected health information and limit incidental uses and disclosures.

### **GUIDELINES TO SAFEGUARD PROTECTED HEALTH INFORMATION**

#### 1. Bulletin boards:

- a. Bulletin boards may not contain any documents with PHI of members, unless the member has authorized the display in accordance with the AUTHORIZATION TO USE OR DISCLOSE PROTECTED HEALTH INFORMATION. - This includes:
- b. Baby pictures (even without a name or other identifying information)
- c. Cards and notes of appreciation

## EXAMPLE - POLICY & PROCEDURE

|   |   |
|---|---|
| <b>Practice:</b> Organization Name                | <b>Effective Date:</b> April 14, 2005                 |
| <b>Title:</b> General Guidelines To Safeguard PHI | <b>Date Revised:</b> April 14, 2005                   |
| <b>Policy Number:</b> 2025                        | <b>Reference:</b> 45 CFR § 164.308(a)(1)(ii)(A) & (B) |

### 2. Cleaning personnel:

- a. Cleaning personnel do not need PHI to accomplish their work. Whenever reasonably possible, PHI will be placed in locked containers, cabinets, or rooms before cleaning personnel enter an area.
- b. When it is not reasonably possible to lock up PHI, it must be removed from sight before cleaning personnel enter an area, and an [ENTITY] supervisor must be present.

### 3. Computer Screens:

- a. Computer screens at each workstation must be positioned so that only authorized users at that workstation can read the display. When screens cannot be relocated, filters, hoods, or other devices may be employed.
- b. Computer displays will be configured to go blank, or to display a screen saver when left unattended for more than a brief period of time. The Privacy and Security Officials will determine the period of time. Wherever practicable, reverting from the screen saver to the display of data will require a password.
- c. Computer screens left unattended for longer periods of time will log off the user. The Security and Privacy Officials will determine the period of time.

### 4. Conversations:

- a. Conversations concerning members' claims or other PHI must be conducted in a way that reduces the likelihood of being overheard by others.
- b. Wherever reasonably possible, noise inhibitors may be used to reduce the opportunity for conversations to be overheard.

### 5. Copying claims and other PHI

- a. When PHI is copied, only the information that is necessary to accomplish the purpose for which the copy is being made, may be copied. This may require that part of a page be masked.

### 6. Desks and countertops

- a. Claims and other medical record documents that contain PHI must be placed face down on counters, desks, and other public places where third parties can see them.
- b. Wherever it is reasonably possible to do so, claims and other documents containing PHI will not be left on desks and countertops after business hours or for extended periods of time unsupervised. Supervisors will take reasonable steps to provide all work areas where PHI is used in paper form with lockable storage bins, lockable desk drawers, or other means to secure PHI during periods when the area is left unattended.