

Insert Your  
Logo  
Here

Insert Your Organization Name  
Here

Subject: HIPAA Security Policies & Procedures

Policy # ??-?

Title: Workstation Use

Page 1 of 6

---

Effective Date of This Revision: March 17, 2006

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

**HIPAA REGULATORY INFORMATION: Workstation Use Standard**

<b>Category:</b>	<input type="checkbox"/> Administrative Safeguard	<b>Type:</b>	<input checked="" type="checkbox"/> Standard
	<input checked="" type="checkbox"/> Physical Safeguard		<input type="checkbox"/> Implementation Specification
	<input type="checkbox"/> Technical Safeguard		<input type="checkbox"/> Required <input 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 checked="" 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) shall be managed to guard the integrity, confidentiality, and availability of electronic PHI (*ePHI*) data. According to the law, all "Cover 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:**

*"The Workstation Use Standard of the rule requires formal, documented policies and procedures that address how a covered entity addresses the safeguarding of EPHI in workstation use, and availability in an operational and development/test environment."*

---

HIPAA Requirement Facility Access Control Standard  
HIPAA Reference: 45 CFR 164.306 (2) (iii)  
Reviewed by: "Insert Text Here"  
Approved by: "Insert Text Here"  
Effective Date: "Insert Date Here"  
Supersedes Policy: "Insert Policy Number Here"

Copyright 2006 [www.training-hipaa.net](http://www.training-hipaa.net)  
Limited rights granted to licensee for internal use only.  
All other rights reserved.

## PURPOSE:

Workstation Use Rule requires "Cover Entity's Name" to implement workstation use policies and procedures that specify that address the functions performed at each workstation, the manner in which those functions are performed, and the physical attributes around each workstation that accesses EPHI. The general policies will be communicated with all employees, including expectations of workforce members with regard to their workstation and area.

- The proper functions to be performed
- The manner in which those functions are to be performed

## ACTION:

These policies are link to or reference the Workstation Use Standard policy:

Each Unit of "Cover Entity's Name" health care component (HCC), which handles ePHI, shall have policies and procedures in place to ensure the physical and logical security aspects of workstations or class of workstations that may access electronic protected health information (EPHI) as defined in "Cover Entity's Name" 's Workstation Security Standard ("Policy Number" ), such as hard drives, CD-Rom, Flash drives and Network partition access, i.e. Storage Area Networks.

Each Unit of "Cover Entity's Name" health care component (HCC), which handles ePHI, shall have facility security policies and procedures in place, to ensure availability, confidentiality, and integrity of ePHI; while limiting the minimum necessary privileges for a person or software application to perform their duties as defined in the [Covered Entity's Name]'s Facility Security Standard ("Policy Number" ).

Each Unit of "Cover Entity's Name" health care component (HCC), which handles ePHI, will need to consider what constitutes an appropriate solution for workstation security based on its Risk Analysis policy ("Policy Number" ) and Risk Management ("Policy Number" ) results.

Additionally the following steps will be implemented to conform to the standard:

- Identify Workstation Types and Functions or Uses – Document the different classifications and categories workstations are employed by workforce and non-workforce members
  - (1) Inventory workstations and devices.
  - (2) Develop policies and procedures for each type of workstation and workstation device, identifying and accommodating their unique issues (refer to the workstation definition)

- (3) Classify workstations based on the capabilities, connections, and allowable activities for each workstation used.
- Identify Expected Performance of Each Type of Workstation – Workforce members should be trained on workstation use and security policies and procedures. In addition, they should be taught Entities may require workforce members to sign acknowledgments, indicating they understand what is expected of them in terms of security.
  - Analyze the Risk Associated with classification and function of workstation – Determine which classification and function holds the greatest threat to security.
    - (1) Each Unit of "Cover Entity's Name" health care component (HCC) will strive to place workstations accessing ePHI in physically secure locations that minimize the risk of physical access by unauthorized persons.
    - (2) Ensure that any risks associated with a workstation's surroundings are known and analyzed for possible negative impacts.
  - Develop policies and procedures that will prevent or preclude unauthorized access of unattended workstations, limit the ability of unauthorized persons to view sensitive information, and erase sensitive information as needed.
  - Each Unit of "Cover Entity's Name" health care component (HCC) will take reasonable and appropriate steps to prevent unauthorized persons from viewing ePHI on workstations.
  - Each Unit of "Cover Entity's Name" health care component (HCC) will take reasonable and appropriate steps to require workforce members to protect the physical and logical security of portable and fixed workstations that store ePHI
  - Each Unit of "Cover Entity's Name" health care component (HCC) will require workforce members to attend training covering how to protect and how to maintain the security of their workstation and the workstations of others and what the acceptable uses of portable and fixed workstations that store ePHI are in accordance with "Cover Entity's Name" 's Security Awareness & Training policy ("Policy Number" )
  - Each Unit of "Cover Entity's Name" health care component (HCC) will require workforce members using remote access to IIHI do so via a remote terminal connection, in conjunction with a VPN tunnel and IPSEC encryption link to "Cover Entity's Name" local network. See "Cover Entity's Name" 's Encryption ("Policy Number" ) and VPN ("Policy Number" )policies
-

---

## 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.

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

"Cover Entity's Name" Security Compliance Officer: the individual appointed by "Cover 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 "Cover 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.

Insert Your  
Logo  
Here

**Insert Your Organization Name  
Here**

**Subject: HIPAA Security Policies & Procedures**

**Policy # ??-?**

**Title: Workstation Use**

**Page 5 of 6**

---

Any other device has been defined as:

- Both unintelligent and intelligent computer terminals
- Personal digital assistants (PDAs)
- Other types of wireless devices
- Operator's consoles associated with mini-, mid-range, or mainframe computers
- Diagnostic equipment that may contain and/or provide access to EPHI

---

HIPAA Requirement    Facility Access Control Standard  
HIPAA Reference:    45 CFR 164.306 (2) (iii)  
Reviewed by:        "Insert Text Here"  
Approved by:        "Insert Text Here"  
Effective Date       "Insert Date Here"  
Supersedes Policy:   "Insert Policy Number Here"

Copyright 2006 [www.training-hipaa.net](http://www.training-hipaa.net)  
Limited rights granted to licensee for internal use only.  
All other rights reserved.

Insert Your  
Logo  
Here

Insert Your Organization Name  
Here

Subject: HIPAA Security Policies & Procedures

Policy # ??-?

Title: Workstation Use

Page 6 of 6

---

### Related Policies:

Access Authorization ("Policy Number" )  
[Covered Entity's Name] Confidentiality Agreement  
Information Access Management Standard ("Policy Number" )  
Access Control and Validation Risk Analysis ("Policy Number" )  
Facility Security Plan ("Policy Number" )  
Facility Access Control ("Policy Number" )

### Reference:

Access to Electronic Health Information Flow Sheet  
Access Authorization ("Policy Number" )  
Risk Analysis ("Policy Number" )  
Risk Management ("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))

---

HIPAA Requirement	Facility Access Control Standard
HIPAA Reference:	45 CFR 164.306 (2) (iii)
Reviewed by:	"Insert Text Here"
Approved by:	"Insert Text Here"
Effective Date	"Insert Date Here"
Supersedes Policy:	"Insert Policy Number Here"

Copyright 2006 [www.training-hipaa.net](http://www.training-hipaa.net)  
Limited rights granted to licensee for internal use only.  
All other rights reserved.