

Insert Your  
Logo  
Here

Insert Your Organization Name  
Here

Subject: HIPAA Security Policies & Procedures

Policy # ??-?

Title: Workstation Use

Page 1 of 5

---

Effective Date of This Revision: April 5, 2014

<b>Contact:</b>	HIPAA Chief Security 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 "Business Associate's Name" officers, employees and agents of units within a "Business Associate's Name" Entity must preserve the integrity and the confidentiality of individually identifiable health information (*IIHI*) pertaining to each patient or client.

**SECURITY REGULATION STANDARD LANGUAGE:**

*"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 electronic protected health information."*

---

HIPAA Requirement: Facility Access Control Standard  
HIPAA Reference: 45 CFR 164.310 (b)  
Reviewed by: "Insert Text Here"  
Approved by: "Insert Text Here"  
Effective Date: "Insert Date Here"  
Supersedes Policy: "Insert Policy Number Here"

Copyright 2014 [www.training-hipaa.net](http://www.training-hipaa.net)  
Limited rights granted to licensee for internal use only.  
One company license only. All other rights reserved.

## PURPOSE:

Workstation Use Rule requires "Business Associate's Name" to implement workstation use policies and procedures that specify 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.

## ACTION:

1. Workstation assignment requires "Business Associate's Name" or management level approval and shall be assigned to workforce members and affiliated third parties on an as needed basis.
2. Workstations will be set up and maintained by IT support staff.
3. Standard configuration for different classes of workstations (e.g., laptops, workstations not connected to the Internet, workstations used to access patient information, etc.) shall be managed by IT support staff.
4. The hard drive of a workstation will not be used to store confidential data including but not limited to electronic protected health information (ePHI). All ePHI will be stored on "Business Associate's Name" network server.
5. Workstations are for the use of workforce members and affiliated third parties assigned a workstation and are not for unauthorized use.
6. Workforce members and affiliated third parties are not to install unapproved software on "Business Associate's Name" workstations. This includes personal software, non-approved business or medical software. Workforce members and affiliated third parties are not allowed to download software from the Internet and install the software on the workstation.
7. Software installation must be approved by a supervisor and installed by IT support staff.
8. Software installed on workstations must be fully licensed with licenses tracked by IT support staff.
9. If the workstation is a laptop, hard drive encryption software will be installed on the laptop by IT support staff.
10. If the assigned workstation will be used at a remote location, workforce members and affiliated third parties are prohibited from modifying the workstation configuration following assignment.

## 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.

"Business Associate'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.

"Business Associate's Name" Security Compliance Officer: the individual appointed by "Business Associate'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 "Business Associate'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 4 of 5**

---

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 164.310 (b)  
Reviewed by:        "Insert Text Here"  
Approved by:        "Insert Text Here"  
Effective Date        "Insert Date Here"  
Supersedes Policy:   "Insert Policy Number Here"

Copyright 2014 [www.training-hipaa.net](http://www.training-hipaa.net)  
Limited rights granted to licensee for internal use only.  
One company license only. All other rights reserved.

Insert Your  
Logo  
Here

Insert Your Organization Name  
Here

Subject: HIPAA Security Policies & Procedures

Policy # ??-?

Title: Workstation Use

Page 5 of 5

---

### Related Policies:

Access Authorization ("Policy Number" )  
[Business Associate'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" )  
[Business Associate'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 164.310 (b)
Reviewed by:	"Insert Text Here"
Approved by:	"Insert Text Here"
Effective Date	"Insert Date Here"
Supersedes Policy:	"Insert Policy Number Here"

Copyright 2014 [www.training-hipaa.net](http://www.training-hipaa.net)  
Limited rights granted to licensee for internal use only.  
One company license only. All other rights reserved.