virtualmedicalstaff

# TELEMEDICINE

## HIPAA/HITECH
## Privacy & Security

virtualmedicalstaff

## 1 Access Control – Role Based Access

### Criteria Description

The organization shall provide secure rolebased account management. Privileges granted utilizing the principle of least privilege.

*describe how user roles are defined and administered.*

- HIPAA 164.312(a)(2)(i) Unique User Identification
- HIPAA 164.308(a)(3)(ii)(B) Appropriate Access
- NIST special publication 800-53 recommended security controls AC-2

### How Each Criteria is Addressed

Roles based access is used to ensure the physician has the most restrictive amount of functionality necessary to perform his or her role. Observation rooms where patients are seen are given a low privileged account role that cannot be used to escalate their privileges or enable unauthorized features.

A host role is provisioned and access to the host accounts is restricted to only authorized Virtual Medical Staff support personnel.

Another mechanism in place is the ability to maintain further privacy by allowing the physician to lock the room. No parties will be able to gain access to the room once the lock is enabled. Only the physician and host can unlock the room.

## 2 Access Control – Local Authentication

### Criteria Description

When providing a local user access to ePHI or PII data, the organization shall employ authentication for system access that is NIST Special Publication 800-63 compliant in accordance with the organizational selection of level 2 or higher*.

*note password complexity, expiration, history requirements in response.*

- HIPAA 164.312(d) Authentication
- HIPAA 164.308(a)(5) Password Management
- NIST Special publication 800-63 Electronic Authentication Guideline

### How Each Criteria is Addressed

Provide password requirement for both application users and system administrators.

Example: Users of the website have a minimum password length of 6 characters. The web server administrators have a minimum password length of 14 characters.

Passwords for both the physician's computer and portal access use the following minimum requirements:

- Minimum Password Length: 6 characters
- Password contain uppercase and lowercase alpha characters

System administrators have separate accounts. Policies restrict support personnel from accessing the portal while a patient is in the observation room.

virtualmedicalstaff

## 3 Access Control – Remote Authentication

### Criteria Description

When providing a remote user access to ePHI or PII data, the organization shall employ multifactor authentication for system access that is NIST Special Publication 800-63 compliant in accordance with the organizational selection of level 3 or level 4. (e.g. Two Factor Authentication)

- HIPAA 164.312(d) Authentication
- NIST Special publication 800-63 Electronic Authentication Guideline

### How Each Criteria is Addressed

Provide password requirement for both application users and system administrators.

Example: Users of the website are restricted to accessing the site. The web server administrators utilize One-Time-Password Tokens when remotely managing the web server.

## 4 Access Control – Session Termination

### Criteria Description

The information system automatically terminates or locks a remote session after the organization-defined time period of inactivity requiring user re-authentication.

- HIPAA 164.312(a)(2)(iii) Automatic Inactivity Logoff

### How Each Criteria is Addressed

Sessions are terminated 15 minutes after the last attendee leaves the room or immediately if the Host of the room selects “End Conference option.”

## 5 Audit & Accountability – Auditable Events

### Criteria Description

The information system produces audit records that contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events (e.g., user authentication, access to data, modification of data).

- HIPAA 164.308(a)(5) Log-in Monitoring
- HIPAA 164.312(b) Audit Controls
- NIST special publication 800-53 recommended security controls AU-3

### How Each Criteria is Addressed

Our system audits usage. We capture the observation room ID, facility name, health group name, date and time started, duration, and number of attendees.

Additionally, we also capture both parties system usernames, date and time started, date and time ended, duration, and public IP.

virtualmedicalstaff

## 6 Audit & Accountability – Analysis & Reporting

### Criteria Description

The organization regularly* reviews/ analyzes audit records for indications of inappropriate or unusual activity. The organization investigates suspicious activity or suspected violations. (e.g., logs are reviewed daily, suspect activity is immediately investigated).

** note frequency in response*

- HIPAA 164.308(a)(1)(ii)(D) Activity Review
- HIPAA 164.308(a)(6) Security Incident Procedures

### How Each Criteria is Addressed

Currently there is no automation; reports are generated manually.

## 7 Media Protection – Media Storage

### Criteria Description

The organization protects portable information system media* containing sensitive information with an appropriate cryptographic mechanism.

*laptops, backup tapes, USB thumb drives, CD/DVD, etc.*

- HIPAA 164.312(a)(2)(iii) Automatic Inactivity Logoff

### How Each Criteria is Addressed

No ePHI/PHI passes through our system. Access to any EMR/EHR and/or other HIS systems is controlled by the client.

- HIPAA 164.312(a)(1) Access Control
- HIPAA 164.312(a)(2)(iv) Encryption

## 8 Audit & Accountability – Auditable Events

### Criteria Description

The information system produces audit records that contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events (e.g., user authentication, access to data, modification of data).

- HIPAA 164.308(a)(5) Log-in Monitoring
- HIPAA 164.312(b) Audit Controls
- NIST special publication 800-53 recommended security controls AU-3

### How Each Criteria is Addressed

Our system audits usage. We capture the observation room ID, facility name, health group name, date and time started, duration, and number of attendees.

Additionally, we also capture both parties system usernames, date and time started, date and time ended, duration, and public IP.

## 9 Physical Protection – Visitor Control

### Criteria Description

The organization controls physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides.

- HIPAA 164.310(a)(2)(iii) Access to Facilities

### How Each Criteria is Addressed

Virtual Medical Staff servers are located in secure facilities with restricted physical access.

## 10 Media Protection – Media Storage

### Criteria Description

The organization screens individuals requiring access to sensitive information and information systems prior to authorizing access.

- HIPAA 164.308(a)(3)(ii)(B) Workforce Screening

### How Each Criteria is Addressed

All physicians participate in a credentialing screening process. Screening process is either conducted by Virtual Medical Staff or the client before the physician begins providing services.

## 11 Personnel Security – Termination

### Criteria Description

The organization terminates information system access upon termination of individual employment.

- HIPAA 164.308(a)(3)(ii)(C) Workforce Termination

### How Each Criteria is Addressed

Access to the Virtual Medical Staff service is revoked at the earliest prior to termination notification or immediately proceeding termination notification.

## 12 Risk Management – Vulnerability Assessment

### Criteria Description

The organization scans for vulnerabilities in the information system at least annually.

- HIPAA 164.308(a)(1)(ii)(A) Risk Analysis

### How Each Criteria is Addressed

Currently deploy IPS services, net flow monitoring, and SNMP.

virtualmedicalstaff

## 13 Physical Protection – Visitor Control

### Criteria Description

The information system physically or logically separates user interface services (e.g., public web pages) from information storage and management services (e.g., database management).

- NIST special publication 800-53 recommended security controls SC-2

### How Each Criteria is Addressed

External web portals/parts are separated from the systems used to provide the Telemedicine services.

## 14 System & Communication Protection – Boundary Protection

### Criteria Description

The information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system (e.g., firewall between internet facing servers and the internal network).

- HIPAA 164.308(a)(1)(ii)(B) Risk Management
- NIST special publication 800-41 Guidelines on firewalls and firewall policy

### How Each Criteria is Addressed

Firewalls are in place and only allow the minimal set of protocols necessary to provide service availability.

## 15 System & Communication Protection – Transmission Confidentia

### Criteria Description

The information system employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measure.

- HIPAA 164.312(e)(1) Transmission Security
- HIPAA 164.312(a)(2)(iv) Encryption

### How Each Criteria is Addressed

Our solution uses 128-AES encryption between endpoints. 256-AES encryption is used internally.

virtualmedicalstaff

## 16 Physical Protection – Visitor Control

### Criteria Description

The organization installs newly released security patches, service packs, and hot fixes on the information system in a reasonable time frame* (e.g., deployment complete within 30 days from security patch release). The organization installs newly released security patches, service packs, and hot fixes on the information system in a reasonable time frame* (e.g., deployment complete within 30 days from security patch release).

** note time frame in response*

- HIPAA 164.308(a)(1)(ii)(B) Risk Management

### How Each Criteria is Addressed

Systems issued to physicians are provisioned to automatically install critical and security updates.

## 17 Media Protection – Sanitization & Disposal

### Criteria Description

The organization employs malicious code protection mechanisms at critical information system entry and exit points, and at workstations, servers, or mobile computing devices to detect and eradicate malicious code (e.g., antivirus on mail gateways).

- HIPAA 164.308(a)(5)(ii)(B)
  - Malicious Software

### How Each Criteria is Addressed

Systems issued to physicians are provisioned with a multi threat antivirus package. Definition updates are scheduled every two hours and weekly scans are scheduled. Password protection is enable and must be used to cancel a scan, change parameters, or disable protection.

virtualmedicalstaff

# 18 Physical Protection – Visitor Control

## Criteria Description

The organization employs tools and techniques to monitor events on the information system to detect attacks*, and provide identification of unauthorized use of the system (e.g., intrusion detection systems, intrusion prevention systems, audit record monitoring software, network monitoring software).

** if solution is a manual process please note frequency of review in response*

- HIPAA 164.308(a)(1)(ii)(D) Activity Review

## How Each Criteria is Addressed

Currently deploy IPS services, net flow monitoring, and SNMP.

2655 Northwinds Parkway
Alpharetta, GA 30009

877.732.7089

virtualmedstaff.com