NCSA HIPAA Facility Security Procedures

Document Name: NCSA HIPAA Facility Security Procedures
Version: 1.0a
Accountable: Adam Slagell
Authors: Adam Slagell
Approved: June 29, 2016

Purpose

This document specifies the procedures for bringing people and equipment in and out of a secured facility for processing or storing ePHI (electronic Personal Health Information) covered by HIPAA.

Scope

This applies to facilities operated by the NCSA Health Care Component, such as, the Advanced Computational Health Enclave.

Procedures

NCSA will track approvals and changes made to the applicable environment, keeping records for 6 years or from the inception of the program. Each step of the following workflows is approved by a member of the NCSA Health Care Component while logged in with their personal credentials, and each approval sends emails to the approver and other relevant parties.

Adding/Removing Personnel with Physical Access

The building manager has the only physical key and can use it to allow access for emergency personnel or if the electronic access control mechanism is broken. In these cases, they log access afterwards with a ticket assigned to the HIPAA Liaison subject "Emergency Access for HIPAA Enclave". This tells **who** was let in, **when**, and **why**. No one is left unescorted if they are not part of the covered entity.

All other access is made with an electronic control that identifies each person individually. People given electronic access must be a part of the covered entity. The workflow for granting access is as follows.

1. Request is submitted by the building manager to the HIPAA Liaison on behalf of a staff member with the reason for the request.
2. The HIPAA Liaison checks that they are in the covered entity and approves or rejects the request.
3. If approved, the building manager adds the person to the access control list.
4. The workflow is closed by the building manager. This sends an email to the building manager, HIPAA Liaison, the new staff member with access, and their manager.

The process for removing access can be triggered either via a role change from staff to non-staff (e.g., during the employee exit process), or at the request of the HIPAA Liaison.

1. Request is submitted and goes to the HIPAA Liaison for approval.
2. Building manager receives approved request and removes access.
3. Building manager closes the ticket. (If not closed within 24 hours or creation, Security Office is alerted). An email is sent to the person who lost access, their manager, the building manager, and the HIPAA Liaison.

Providing Access for non-Emergency Maintenance

Maintenance requests start with the building manager who works with Facilities & Services. The process for non-emergency maintenance is as follows.

1. The building manager submits a request with a description of the maintenance request.
2. The HIPAA Liaison approves or rejects the request.
3. If approved, the building manager submits a work order to F&S.
4. The building manager provides an escort(s) who is a part of the covered entity and who stays with the maintenance person while in the secured area.
5. After the work is completed, the building manager records when it was completed and by whom along with the identity of the escort.
6. The workflow is closed by the building manager. An email is sent to the HIPAA Liaison and building manager.

Physical Security in a Disaster

If there is a disaster that causes the access control mechanisms to fail open, University staff may or may not be allowed near the facility for some time. When they are allowed back, the building manager is responsible for providing physical security to any remaining systems until controls are restored. This may mean that a person within the covered entity is physically watching the area or that equipment is moved to secure, offline storage.

The response must be documented and given to the HIPAA Liaison. This documentation must include:

- Any potential exposure period during which staff were not allowed near the enclave
- Any missing equipment or equipment that has been clearly tampered with
- Who was responsible for watching the equipment and during what time periods
- How, who and when systems were moved to a secure, offline storage facility
- Who has access to the offline storage facility

Modifying Physical Security Controls

A request to modify physical security controls can start with the building manager, Security Office or HIPAA Liaison. The workflow is as follows.

1. The building manager makes sure the request has sufficient detail and forwards it to the Security Office for approval.
2. The Security Office reviews the changes and evaluates the impact of the change. The request is then rejected or approved and forwards approved requests to the HIPAA Liaison for approval.
3. The HIPAA Liaison approves or rejects the request.
4. If approved, the building manager submits a work order to F&S.
5. The building manager provides an escort(s) who is a part of the covered entity and who stays with the maintenance person or vendor while in the secured area doing the work.
6. After the work is completed, the building manager records when it was completed and by whom along with the identity of the escort.
7. The workflow is closed by the building manager. An email is sent to the HIPAA Liaison, Security Office and building manager.

Moving Equipment with ePHI

If equipment with ePHI is moved, it must stay within the secured facility or be moved to another secured facility. The following process is followed.

1. A request to move equipment with dates and customer impacts is submitted to the HIPAA Liaison.
2. The HIPAA Liaison works with the appropriate offices to ensure the schedule works for the customers impacted.
3. If applicable, data is backed up using a unique encryption key known to the person making the backup and the HIPAA Liaison.
4. If leaving the secured facility, ePHI will be securely wiped and verified by the Security Office.
5. The system will be powered-off and moved.
6. The system will be restored and verified by system administrators.
7. The ticket is closed by system administrators and an email is sent to the building manager, HIPAA Liaison, and others involved in the ticket or workflow.

Sanitizing Media for Removal

Media must be sanitized before disposal outside of the secure facility. This includes returning disks to vendors or repurposing equipment.

Wiping is done on a dedicated workstation by a method approved by the Security Office.

Anyone in the covered entity may initiate the process to remove media from the facility, but it follows the following process.

1. A request with the reason for removal is sent to the HIPAA Liaison who approves or rejects.
2. The requestor will place the media in the provided secure container.
3. Container shall be locked with a key kept in the secure area.
4. Security team will transport secure container for wiping / destruction.
5. The security team will unlock with second key kept at wiping / destruction station.
6. Each device will be wiped or destroyed per Security Office policy
7. The person wiping the media will electronically record the details of the wiped media and when it was sanitized. Then they will return the secure container to the secure area area.
8. The media is given to the building manager who closes the workflow and sends the drive on. If necessary, they have the original requestor fill out the RMA paperwork.