ACHE Access Control Policy and Procedures

Document Name: NCSA HIPAA Access Control Policy and Procedures
Version: 1.1
Accountable: James Eyrich
Authors: Adam Slagell

Reviewed: August 22, 2023
Approved: August 24, 2023 by IIB

Purpose

This document specifies the procedures for granting, revoking and auditing access control to systems processing or storing ePHI (electronic Personal Health Information) covered by HIPAA.

Scope

These processes apply only to staff in the NCSA Health Care Component. NCSA customers and other Business Associates (BAs) are responsible for authorization decisions of their own staff and can manage their access control groups directly. Users of the system from other parts of the University must be part of the University covered entity, and a Principal Investigator (PI) is responsible for authorization decisions for their project teams and can modify group credentials directly. Regardless of the approval process, NCSA will record the access changes made by Business Associates to ACHE resources through its authorization framework.

Policy

All requests to add or revoke access to the ACHE must be approved by the HIPAA liaison. The HIPAA liaison maintains a list of staff who have elevated privileges with the ability to make changes to the ACHE. The HIPAA liaison grants access in accordance with minimum necessary standard per the HIPAA Privacy Rule.

Procedures

NCSA will track approvals and changes made to access groups, 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.

Alerts are sent to the Security Office and HIPAA liaison anytime there are direct modifications to the group management system that were not triggered by the approval workflow engine. Such legitimate changes are checked for by automated systems at least daily.

Authorization

NCSA staff must be within the NCSA Health Care Component to make a valid request to be added to a system access group for system processing or storing ePHI. Being in the NCSA Health Care Component itself does NOT grant any access, which must instead be requested by the staff member via the following process.

1. Staff member submits request for access with the stated reason for the request. This request contains the requested access group name.
2. Staff member's manager approves or rejects the request.
3. Approved request proceeds to the HIPAA liaison who considers the staff member's role and reason for the request. They also verify that the person has taken approved HIPAA training.
4. If approved and they are in the NCSA Health Care Component group, they are added to the requested group(s).
5. Emails are sent to the staff member, their manager and the HIPAA liaison.

Deauthorization

Deauthorization can happen automatically or by request. For example, being removed from the staff group upon leaving the NCSA will automatically remove one from the NCSA Health Care Component and by consequence from any access group for systems with ePHI. Therefore, even if a person leaves NCSA and has another legitimate reason for access in another unit, they will have to be reapproved by a PI in that unit to be added to the necessary group(s) for their project. The security office can also disable credentials and remove anyone from any group at anytime, though an alert will be sent to them and the HIPAA liaison.

Employees, their managers, and the HIPAA liaison can request de-authorization as well via the following workflow.

1. Employee requests removal with justification and the access control groups they need to be removed from. (Optional: Can start with their manager)
2. Request is received by (or starts with) the employee's manager who approves the request or fills in the same details if they start the request. (Optional: Can start with the HIPAA Liaison).
3. The HIPAA Liaison either receives the request or starts a new one specifying the person and which groups they are to be removed from.
4. If approved, the person is removed from the access control groups.
5. Emails are sent to the staff member, their manager and the HIPAA liaison.

Audits

All NCSA group owners are required to review group membership annually and approve or modify it. This includes customers who are BAs and their point of contact and PIs at the University. Access control groups that provide access to systems with ePHI are owned by the HIPAA liaison who must do the same, or the group is suspended automatically.