

**Procedure 1601 PR.03**

**Access Control for Protect Health Information (PHI)**

Revision Date: 04/20/05

1 – Overview.....1  
 Access Control of Systems, Applications and Data .....1  
 Access to functions .....1  
 Eligibility for Access .....2  
 Access must reflect current status at the University .....2  
 2 – Determine what access is required .....2  
 Identify applications, functions and data needed .....2  
 3 – Training and access .....3  
 University HIPAA security training .....3  
 Guidelines for Approvers .....3  
 4 – Monitor Employee Access and Request Modification When Appropriate.....3  
 Review User Access Profiles .....3  
 Monitor Employee Status and Duties .....3  
 5 – Log-in Alerts for ePHI Information Systems .....3

**1 – Overview**

**Access Control of Systems, Applications and Data**

This procedure applies to Above-Threshold ePHI systems that are part of covered components at the University (including School of Medicine, the School of Nursing, Yale University Health Services, Department of Psychology clinics, and Group Health Plan). Access Control is required in order comply with federal HIPAA regulations and to safeguard the confidentiality, integrity and availability of sensitive and confidential information.

**Access to functions**

To the extent technologically feasible Users shall be granted access only to the protected health information required to perform their functions at the University. This document describes general procedures for requesting, modifying and deleting user access to systems, applications and data covered by HIPAA security regulations.

Units of the Covered Components (e.g. Yale University Health Services) may establish practices and procedures that apply specifically to that unit provided that the practice or procedure is consistent with University policy and requires equal or greater security for ePHI. Please contact your local IT support organization to determine if your unit may require more specific procedures.

Access can be restricted to specific functions within some applications. Whenever the software allows, access should be as granular as feasible. Individuals should only have read or write access to the specific ePHI data required for performing their appropriate function. In most cases access will fall into one of the following categories:

- **update (read/write)** access: the ability to enter and update data and submit transactions
- or
- **lookup (read-only)** access: the ability only to view information without being able to enter or change data.

In some cases appropriate access may consist of read/write access to one portion of a database, read-only access to other portions and, potentially, no access to yet other portions.

The minimum access control requirement is a username and [strong password](#). *Role-based* access may also be employed where it improves granularity of access. Role-based access allows end-users access to information and resources based on their role within the organization. Role - based access can be applied to groups of people or individuals.

Procedures for obtaining necessary ePHI during an emergency: systems with *primary source ePHI for treatment* are required to have a 'break-glass' procedure that allows for a person who does not have access privileges to certain information to gain access in an emergency. Knowledge of the break-glass procedure allows this individual extraordinary access.

- The reason for initiating break-glass access and a detailed audit trail must be documented whenever this procedure is invoked
- Break-glass procedures must be secured and available in hard copy for emergency use

---

### **Eligibility for Access**

Individuals may obtain access to PHI if appropriate approvals are obtained from the System Owner and documented. Considerations for granting access are described below in Sections 2 and 3. In order to obtain access, the individual must have an active record in the Yale University Human Resources database.

For individuals not affiliated with the University, refer to Procedure [3501 PR.22](#) 'Non-Employees: Directory Listing and Access Privileges'.

---

### **Access must reflect current status at the University**

Access to restricted applications, functions, and/or data sets should always be limited to those that are required for the performance of an individual's current duties.

- Whenever the individual's duties at the University change, the individual's access should also be changed to reflect this.
- If the individual no longer needs any access (for instance, upon termination of employment), all access should be terminated.

See 4 – Monitor status and request modification when appropriate

---

## **2 – Determine what access is required**

### **Identify applications, functions and data needed**

In configuring access, follow the concept of 'least privilege'. Every program and every user of the system should operate using the least set of privileges necessary to complete their job. This principle limits the damage that can result from an accident or error. It also reduces the number of potential interactions among privileged programs to the minimum for correct operation, so that unintentional, unwanted, or improper uses of privilege are less likely to occur. If a question arises related to misuse of a privilege, the number of programs that must be audited is minimized. Always run applications with just enough privilege to complete the task. You do not need to be an administrator to read email, nor do you require your account to be anything more than a user when writing documents. There are tasks that require greater capabilities, such as system configuration and administering user accounts, but few tasks require full privileges, and most users do not require administrative rights.

A procedure that can assist in implementing least privilege is to have the owner of the data or processes classify resources in categories that are communicated to the system administrator.

The System Owner of the PHI data or process should identify those individuals whose tasks require access to applications or data, and determine the specific applications or data sets the individual will need to use.

For each application, determine the specific functions and responsibilities for which the individual needs access. Bear in mind the sensitive nature of many restricted functions, and their potential for abuse and error, when making this determination.

#### **Examples:**

- User A needs to be able to access all lab results from a clinical trial study, but does not need to access personal contact information, so access to that information should be restricted if the application software allows that functionality.

- Employee B may need to view clinical trial data including contact information, but should not be able to enter or modify data.
- A user may need access to perform data entry functions. Approval and authorization functions, on the other hand, should be more narrowly distributed, to ensure effective control and oversight.

---

## 3 – Training and access

### University HIPAA security training

Individuals must complete specific HIPAA security training courses in order to receive access to any system with PHI. See <http://hipaa.yale.edu/training/>

---

### Guidelines for Approvers

Before approving a request for access, approvers should evaluate the impact of the requested access.

Use the following guidelines to determine if the request should be approved:

1. The individual has a current functional need for access to the data or application(s)
2. The requested access is at an appropriate level for the user's job and position.
3. The request will give the user access to a range of data that is necessary and appropriate for his/her duties.

---

## 4 – Monitor Employee Access and Request Modification When Appropriate

### Review User Access Profiles

Data owners and system administrators must periodically review user access to ensure that each person's access privileges are appropriate.

---

### Monitor Employee Status and Duties

A system activity review shall be conducted by the System Owners, Systems Administrators or their designees to evaluate who has access and whether access is still required and appropriate. Monitor the following types of events within the organizations to determine if individual user access needs to be modified or deleted:

- termination of employment or student status
  - change in status at the University
- [University HR Oracle reports](#) for monitoring security and access:
- Reports are available in the [START](#) application
  - Anyone with *START access for others* can run them. Departmental *Training & Access Coordinator* (see [list of departmental TACs](#)) can grant *START access for others* to a system administrator.

Adjust access privileges expeditiously.

---

## 5 – Log-in Alerts for ePHI Information Systems

Log-in alerts must be implemented by System Administrators. Banners are required to display warning text to potential users of a system that provides access to ePHI.

- Log-in alert text *must contain*:
  - “This system is to be used only for [Name of Provider] business purposes by authorized persons.”
  - “System activities are monitored for administrative and security purposes.”
  - “Anyone using this system consents to such monitoring and accepts responsibility to preserve the confidentiality, integrity, and availability of information accessed.”

- Log-in alert text *must not contain* the words, “welcome,” or “greetings” or other language that invites unauthorized parties to use the system.
- Log-in alert text *may contain* web links, phone numbers, and mailing addresses whereby additional information can be obtained.

The full contents of log-in alerts must be displayed before or immediately after user credentials are supplied to a system.

Log-in alerts must be displayed to each user that authenticates to a system.

Whenever possible, user interaction will be required to progress beyond the warning banner.

If no log-in alert can be integrated into the process of authenticating to a system, the alert must be displayed, in clear view, on the access device itself, or in immediate proximity of the device.

---

The official version of this information will only be maintained in an on-line web format. Any and all printed copies of this material are dated as of the print date. Please make certain to review the material on-line prior to placing reliance on a dated printed version.

---