

## ***Policy: Access to Clinical Information Systems***

### ***Objective***

This policy is designed and instituted to enable [facility name] to control access to its information and information systems by enacting procedures governing who can use specific information systems and when and how they can use them. This policy and procedure document outlines the requirements for granting and terminating access to [facility name]'s information systems and system resources and for determining the appropriate level of access for employees, volunteers, and business associates (i.e., employees, contractors, or representatives of entities doing business with [facility name]).

### ***Policy Statement***

Access to [facility name]'s information system is restricted to its own employees and in some cases to users who are volunteers of [facility name], and of those business associates who have executed a Chain of Trust Agreements with [facility name].

Only the [facility name]'s Privacy Officer or his/her authorized representative can grant access to the organization's information systems and then only after the employee or volunteer has attended the appropriate HIPAA Privacy and Security training or after the business associates has provided documentation of HIPAA training within their organization.

The Privacy Officer can revoke authorization to access the facility's information systems at any time if s/he suspects or detects that the individual is misusing information or information resources. Authorized users are granted access to use [facility name's] information resources only during scheduled work times.

## ***Specific Policies on Assigning, Modifying, and Terminating Access***

### ***Granting Access***

Users' level of access to information systems is defined by their job descriptions and their need to access particular types of information in order to carry out the responsibilities of their positions.

Users must meet these criteria before they are authorized access to information system resources:

- The user has completed orientation and has been assigned specific job responsibilities that require access to certain of the {facility name}'s information systems;
- or,
- The user is an employee of a business associate who has a completed Chain of Trust Agreement on file with the Privacy Officer;
- The employee has completed the HIPAA Privacy and Security training class;
- and
- The Privacy Officer has on file a copy of the *Policy on Security Code Use* signed by the employee or business associate.

Authorized users must sign the [facility name]'s policy statements covering the use of the facility's information resources.

### ***Granting Access in an Emergency***

The Privacy Officer has the authority to grant emergency access to users who have not completed HIPAA security awareness training if:

- the facility declares an emergency or is responding to a natural disaster that makes the management of patient information security secondary to immediate patient care activities.
- the Privacy Officer determines that granting immediate access is in the best interest of patient care.

If the Privacy Officer grants emergency access, s/he will review the impact of the emergency access within 24 hours of it being granted and report any potential violations of patient security to the CEO, CIO and Legal Counsel.

### ***Granting Emergency Access to an Existing User Access Code***

In some circumstances it may be necessary for the Privacy Officer to grant emergency access to a user's account without the user's knowledge or permission. The Privacy Officer may grant this emergency access in these situations:

- the user terminates or resigns without providing the password;
- the user is seriously ill, unable to communicate, or cannot be reached for a prolonged period;
- the user has not been in attendance and therefore is assumed to have resigned.

### ***Terminating or Modifying Access Rights***

The Privacy Officer or his/her designated representative is responsible for terminating a user's access to {facility's name}'s system in these circumstances:

1. If the Privacy Officer has evidence or reason to believe that the individual is using [facility's name]'s information systems or resources in a manner inconsistent with the *Policy for Workstation Use*.
2. If the user or Privacy Officer has evidence or reason to believe that the user's password as been compromised.
3. If the employee resigns or is terminated.
4. If the employee's job description changes and system access is no longer justified by the new job description.

Any user whose access to the system has been terminated must reapply for system access.

The Privacy Officer or his/her designated representative is responsible for modifying a user's level of access to {facility's name}'s system in these circumstances:

1. If the employee's job description changes and a different level of system access is justified by the new job description.
2. If the employee is suspected of accessing information outside of [facility name's] Policy for Information Systems Use.
3. If the employee is on an approved leave of absence and the user's system access will not be required for more than 3 weeks the Privacy Officer or his/her representative will suspend the user's account until the employee returns from their leave of absence.

## ***Procedures: System Access***

### ***Assigning Access***

1. The department head or business associate completes and submits to the Privacy Officer a written *Request for Information System Access* form (see attached) asking that a User Name and Password be created on specified systems so the individual can access those systems.
2. The user is granted access rights to information system resources based on the user's job description (see table).
3. The Privacy Officer's office creates a unique User Name and Password for the individual, who then obtains it from the Privacy Officer.
4. The user reads and signs a copy of the *Employee Policy on Security Code and System Access*, which the Privacy Officer keeps on file in the Privacy Office.
5. When users log onto the system for the first time, the system automatically prompts them to change the assigned password to one known only to themselves.
6. Passwords must be between 6 and 14 characters long and must include numbers and letters.

### ***Granting Emergency Access***

1. The CEO, CIO, Medical Director, or department head may make requests for emergency access, either verbally or in writing.
2. The Privacy Officer records information about emergency users and the emergency access rights assigned to them.
3. At the conclusion of the event that precipitated the granting of emergency access, the Privacy Officer ensures that each user's emergency access rights either are terminated or converted (using the standard access assignment procedure).

### ***Granting Emergency Access to an Existing User Access Code***

1. The CEO, Medical Director or Department Head must make written requests for emergency access to an existing user account. The request should contain this information:
  - the reason(s) why the specified individual needs emergency access to an existing user account;
  - the name of the new user who should be granted access to the existing user account.
2. The Privacy Officer grants access to the user's account without eliminating the existing user account information.

### ***Terminating or Modifying Access Rights***

1. The Privacy Officer, department head, or business associate completes a *Termination or Modification of Access Rights* form (see attached) to modify or end a user's access to a system or systems.
2. The Privacy Officer or his designated representative inactivates the user on the relevant systems without destroying information that may be linked to the user account;
3. In the event a user's need for system access changes, the Privacy Officer or his designated representative modifies the user's level of access to fit the new job description and as appropriate may deactivate the user on the relevant system(s) without destroying information that may be linked to the user account.
4. In the event a user is granted an extended leave of absence greater than 3 weeks department head or business associate will be responsible for notifying the Privacy Officer or his/her representative and requesting that the user's account be suspended.
5. The completed *Termination or Modification of Access Rights* form is filed in the Privacy Officer's office.

### ***Associated Policies and Procedures***

These documents contain material relevant to the policies and procedures covering System Access:

1. *Chain of Trust Agreement*
2. *Employee Policy on Security Code Use and System Access*
3. *Request for Information System Access*
4. *Termination Policy*
5. *Policy for Information System Use*

## **Request for Information System Access Form**

**Instructions:** Complete this form for each employee who requires access to [facility's name]'s information systems after the employee has attended HIPAA training on Privacy and Security of patient information. Return the form to the Privacy Officer at least one working day before the employee or business associate needs access to the designated system(s).

Employee Name: \_\_\_\_\_

Department: \_\_\_\_\_ Employee Number: \_\_\_\_\_

Job Description: \_\_\_\_\_

Requested Access Date: \_\_\_\_\_

Date(s) of HIPAA Training: \_\_\_\_\_

Type of User:

- |  |   |
|--|---|
| <input type="checkbox"/> System Manager                | <input type="checkbox"/> Cytologist     |
| <input type="checkbox"/> Vendor Support Representative | <input type="checkbox"/> Histologist    |
| <input type="checkbox"/> Hardware Maintenance          | <input type="checkbox"/> Billing Office |
| <input type="checkbox"/> Super User                    | <input type="checkbox"/> Clerical       |
| <input type="checkbox"/> Pathologist                   | Other (specify):                        |

Requesting Access to Systems (specify names of systems):

Requesting Suspense of User's Access (specify length of suspension):

Special Access Requests:

*Signature of Department Manager* \_\_\_\_\_

Access Granted By \_\_\_\_\_

Date:

|                               | Add new user | Modify user access | Delete user profile | Modify system configuration files | Modify system master files | Update system software | Review patient information | Add new patient information | Delete patient information | Modify patient information | Print patient reports | Create system reports | Release patient reports | Create addendums | Create Amendments | Review Audit Trail |
|-------------------------------|--------------|--------------------|---------------------|-----------------------------------|----------------------------|------------------------|----------------------------|-----------------------------|----------------------------|----------------------------|-----------------------|-----------------------|-------------------------|------------------|-------------------|--------------------|
| Privacy Officer               | Y            | Y                  | Y                   | N                                 | N                          | N                      | N                          | N                           | N                          | N                          | N                     | N                     | N                       | N                | N                 | Y                  |
| System Manager                | N            | N                  | N                   | Y                                 | Y                          | Y                      | N                          | N                           | N                          | N                          | N                     | N                     | N                       | N                | N                 | N                  |
| Vendor Support Representative | N            | N                  | N                   | Y                                 | N                          | Y                      | Y                          | N                           | N                          | N                          | N                     | Y                     | N                       | N                | N                 | N                  |
| Hardware Maintenance          | N            | N                  | N                   | Y                                 | N                          | N                      | N                          | N                           | N                          | N                          | N                     | N                     | N                       | N                | N                 | N                  |
| Super User                    | N            | N                  | N                   | N                                 | Y                          | N                      | Y                          | Y                           | Y                          | Y                          | Y                     | Y                     | N                       | N                | N                 | N                  |
| Pathologist                   | N            | N                  | N                   | N                                 | N                          | N                      | Y                          | Y                           | Y                          | Y                          | Y                     | N                     | Y                       | Y                | Y                 | N                  |
| Cytologist                    | N            | N                  | N                   | N                                 | N                          | N                      | Y                          | Y                           | Y                          | Y                          | Y                     | N                     | Y                       | Y                | Y                 | N                  |
| Histologist                   | N            | N                  | N                   | N                                 | N                          | N                      | Y                          | Y                           | N                          | N                          | Y                     | N                     | N                       | N                | N                 | N                  |
| Billing Office                | N            | N                  | N                   | N                                 | N                          | N                      | Y                          | N                           | N                          | N                          | N                     | N                     | N                       | N                | N                 | N                  |
| Clerical                      | N            | N                  | N                   | N                                 | N                          | N                      | Y                          | Y                           | N                          | Y                          | Y                     | N                     | N                       | N                | N                 | N                  |