<<organization>>

Access Control Policy

Effective Date:

Purpose

The purpose of this policy is to set a standard and require procedures for managing, reviewing and validating user access to information systems. Without proper access administration, undesired or unauthorized access could occur resulting in breach of PHI data, financial loss, loss of customers or business partner confidence, reputation damage or failure to meet HIPAA requirements. The intent of this policy is to provide a baseline standard for management of all access to [ORGANIZATION] systems.

Policy Statement

It is the policy of [ORGANIZATION] that access to PHI will be allowed only for persons who meet the conditions identified and documented in the HIPAA security and privacy rules. Any person who does not meet one of these conditions shall be prohibited from access. Each user shall be granted access using a unique ID or account. Sharing of accounts without explicit permission of the [ROLE] is a security violation. User rights are to be granted using the principle of least privilege and need to know.

To allow for the efficiency of clinical and other operations, roles may be combined and access rights shall be granted on the basis of potential need to know. Where the business requirements of [ORGANIZATION] require broader access to PHI other controls will be implemented to protect PHI from unapproved access. These controls include training, regular log inspection, separation of duties and sanctions.

To ensure consistent compliance with the HIPAA privacy and security rules, access rights to PHI and other sensitive data will be based on the functional roles of staff, contractors, visitors and other users of the [ORGANIZATION] IT infrastructure, applications and data. We will determine an appropriate set of functional roles that adequately define what users require access to which. At a minimum the functional roles must accommodate the following use types:

- Non-privileged employee/doctor user accounts
- Privileged administrator accounts
- Temporary, contractor and external user accounts

These access permissions based on clinical, business and other workflow requirements will be mapped to the authorization roles used to assign access rights to specific data.

Access will be granted by the [ROLE] based on:

- Least Privilege: Users will only be granted access to PHI for the purpose of executing their responsibilities and duties. Right to access PHI shall not be granted unless there is a legitimate business or medical need.
- Segregation of Duties: Users should not be able to grant themselves rights. Administrative accounts shall be monitored. To the maximum extent logs shall be maintained.
- Role Based Access: Users will be assigned access rights to PHI based on functional roles they assume in the course of doing the [ORGANIZATION] business.

Any changes to access privileges and roles must be actively managed and documented. Deactivation or termination of an account must immediately remove all access to PHI. Emergency access to PHI and other data shall be established where needed to facilitate emergency mode operation. Emergency access shall only be used during emergencies and in testing of emergency operations. Emergency access will be removed as soon as no longer needed.

Policy Owner

Security Compliance Officer

Standards

1.0 Account Types

Provisioning of accounts and their privileges across [ORGANIZATION] systems and applications must conform to the following requirements.

- Default Accounts (Accounts available out-of-the box; e.g. Administrator and Guest)
  - Default accounts shall be disabled removed or renamed for all devices. Passwords for all renamed default accounts must be changed before activation.
- Service or Process Accounts:
  - Service or Process account settings are defined in the System Configuration Policy and associated procedures.
- Generic Accounts:
  - Disabled generic accounts may be used as templates to create new accounts of various types as long as names and default passwords are changed in conformance with the Password Policy.
- Privileged Accounts:
  - Administrator and other privileged accounts shall be created only where needed to manage the system. Procedures must be implemented to ensure separation of administrative duties and oversight.
- Individual User Accounts
  - Each user account will be assigned one or more roles based on the user's access requirements. Procedures that define the roles and maintain a record of access rights granted to each user will be maintained along with the start date, end date and supervisor/administrator approving the role.
- Temporary Accounts:
  - From time to time temporary accounts will need to be created to allow work by short term contractors, guests or auditors. These shall be explicitly created using the role based access control method used for all individuals. Each account must have an expiration date on which access will be revoked. Temporary users must meet workforce requirements for temporary workers as described in the Workforce Policy.
- External and Contractor Accounts
  - External users and contractors must meet the same standards as Temporary account holders. Where such users are permanently assigned to the organization, the user must meet all of the requirements for staff called for in the Workforce Security Policy.

2.0 Access Log Inspection

- Use of accounts shall be monitored as specified in the Information System Monitoring Policy.
- Users shall be notified when their accounts are created or access rights are changed and notification will include the current Acceptable Use Policy.

3.0 De-Provisioning

- User Accounts:
  - User account access will be revoked within 24 hours of a user's departure. The account may be suspended or deleted as necessary. Notice to the account administrator must be initiated as part of the termination process.
- Temporary Accounts
  - Temporary Accounts will be deactivated upon the expiration date or the date of departure of the guest, contractor or visitor, whichever occurs first. If no automatic expiration is configured, a POC must be designated to ensure that access to facilities and data are revoked as required.
- Account audit:
  - Each [YEAR/QUARTER/MONTH] an audit of all accounts will be conducted to ensure that all active accounts are provisioned only to individuals authorized as above and all accounts that should be deactivated or suspended are not active. The result of this audit shall be reported to the security compliance repository.

References

Internal

1. Workforce Security Policy
2. Information System Monitoring Policy

External

1. 45 C.F.R. § 164.308 (a)(3)(i): Standard: Workforce security. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.

2. 45 C.F.R. § 164.308 (a)(3)(ii)(A): Authorization and/or supervision (Addressable). Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.

3. 45 C.F.R. § 164.308 (a)(3)(ii)(C): Termination procedures (Addressable). Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.

4. 45 C.F.R. § 164.308 (a)(4)(i): Standard: Information access management. Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.

5. 45 C.F.R. § 164.308 (a)(4)(ii)(B): Access authorization (Addressable). Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.

6. 45 C.F.R. § 164.308 (a)(4)(ii)(C): Access establishment and modification (Addressable). Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

7. 45 C.F.R. § 164.312 (a)(1): Standard: Access control. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).

8. 45 C.F.R. § 164.312 (a)(2)(i): Unique user identification (Required). Assign a unique name and/or number for identifying and tracking user identity.