IDAHO STATE UNIVERSITY
POLICIES AND PROCEDURES (ISUPP)
HIPAA Security - Technical Access Control
10390

POLICY INFORMATION

Major Functional Area (MFA): MFA X **-** Office of General Counsel & Compliance

Policy Title: Technical Access Control

Responsible Executive (RE): General Counsel

Sponsoring Organization (SO): Office of General Counsel

Dates: Effective Date: 4-20-12

Revised:

Annual Review: 4-20-13

I. INTRODUCTION:

It is the objective of ISU to implement and maintain appropriate technical access control capabilities to support the Information Access Management process. These technical controls include policies, procedures and technical system implementations for controlling access to electronic confidential or sensitive information including electronic protected health information (ePHI). This policy is intended to ensure user accountability, confidentiality of information and minimize the risk of unauthorized user accounts on information systems being authorized, established and/or modified.

II. POLICY STATEMENT:

It is the policy of ISU to establish and maintain technical access controls to support the Information Access Management process. These controls are to be in place as a security standard regarding all systems containing confidential or sensitive information, including ePHI. This can be accomplished through the implementation of policies, procedures and technical controls for access to confidential or sensitive information, including ePHI.

III. AUTHORITY AND RESPONSIBILITIES

ISU is a hybrid entity in accordance with ISU's HIPAA Privacy Policy 10010. Only the health care component (i.e., covered functions) of ISU must comply with this policy. All references in this policy to "ISU" shall be construed to refer only to the health care component of ISU.

IV. PROCEDURES TO IMPLEMENT:

To achieve the objectives of this policy, the following implementation specifications are **<u>required</u>:**

A. <u>Unique User Identification</u>:

1. A user ID is a unique identifier that allows a workforce member to access the organization's information systems. Each user ID is for use by a single authorized individual only (each a User). A person's unique user ID provides access to all systems for which he or she has approved access from the Security Official or his/her authorized representative within the Information Systems Department (IS). Each user is to be uniquely identified and authenticated (e.g., no generic User lDs) when accessing confidential or sensitive information, including ePHI. All exceptions must have documented approval from the Security Official. Users are to maintain the confidentiality of access methods and security safeguards.

2. Most operating systems and security software have User IDs predefined by the software developer, thus allow the respective users to perform wide-ranging functions, including installing, changing, and deleting software functions, as well as granting other users access to information and system functions. All software or system-supplied accounts (such as a guest account) should be removed. If these accounts cannot be removed then minimize security exposure by renaming the account, changing the password, or deactivating the account. If someone must know the password, Information Technology Services must be contacted to establish the appropriate access to systems.

3. Unique IDs must be combined with at least one other form of authentication when accessing confidential or sensitive information, including ePHI. Such authentication must include a password, PIN, token, biometrics, or other appropriate form of authentication.

B. Emergency Access Procedure:

For all systems that contain confidential or sensitive information, including ePHI, an emergency access procedure must be in place. The procedure must define who has access to the system and ensure the following:

1. At least two individuals possess the highest access level with sufficient rights to add, remove, modify, backup and restore the data contained in the system.
2. At least two individuals possess the highest access clearance for physical access to the console that manages the information.
3. The conditions under which this emergency access procedure is to be implemented.

In addition, the following implementation specifications are **addressable:**

C. Automatic Logoff

Each system must be evaluated and a determination made as to whether an automatic logoff of a workstation would be appropriate. The following procedures should be implemented during the evaluation process:

1. If the workstation is located within a non-clinical setting where the physical placement of the workstation is secured within a separate room and away from view by those not authorized to access confidential or sensitive information, including ePHI, an automatic logoff is not necessarily required but is preferred.

2. If a workstation is located in an area where individuals who are not authorized to access confidential or sensitive information, including ePHI, may view the contents of the screen: if feasible, an automatic logoff at the application level should be in place for all applications that access such information. The timeout for such automatic logoff should be sufficient to protect the confidentiality of the information. When automatic logoff is not available other options should be considered such as password protected screensavers and third party software.

D. Encryption and Decryption

Encryption and decryption of data is an access control mechanism designed to protect the confidentiality of the information encrypted. All external communications of ePHI should be encrypted whenever practicable. If encryption is utilized, the following components must be implemented:

1. Keys that are used to encrypt ePHI must be protected with the same care as the information itself.
2. Any encryption application used must comply with current industry standards and/or NIST encryption standards, whichever standard is higher.
3. Data encryption must take place before confidential or sensitive information, including ePHI, is placed on a public or wireless network for transmission.

V. ATTACHMENTS

N/A

VI. REFERENCES

45 C.F.R. § 164.312

PRESIDENTIAL CERTIFICATION

_______________________________________ Date:____________________

Approved by Arthur C. Vailas
President, Idaho State University

OGC use only:
Received by OGC on _________________ by _________ (initial).

Published to ISUPP on ___________________ by _________ (initial).