UNIVERSITY OF OKLAHOMA
Information Technology
Security Standard

Subject: Access to Sensitive Data Standard

Standard number: Information Security S-
Regulation: HIPAA, FERPA, GLB, PCI DSS, State of Okla. ISPPG
Effective: 03/29/2007

Coverage: OU Health Science Center and Health Care Components
Version: 1.2

Reviewed: 02/18/2013

Purpose:

The purpose of this *Access to Sensitive Data Standard* is to provide a framework for developing processes and procedures for the protection of *sensitive* University data.

Standard:

Workforce Security

Access levels to *sensitive* data must be formally defined and documented. Access level definitions must be periodically reviewed and revised.

Definition of which roles have a legitimate need for access and which levels of access to specific information in order to accomplish job responsibilities must be defined and documented.

Identification and definition of permitted access methods to sensitive data must be documented.

Procedure for granting or changing an access method (e.g. password or token) for both distributed and non-distributed networked and non networked environments must be established and documented.

Identification and definition of how long access will be granted to user must be documented.

Process/Procedure to train workforce members regarding access and handling of sensitive data must be established and documented.

Authorization and/or Supervision

Procedure for granting different levels of access to sensitive data must be established and documented.

Procedure for tracking and logging authorization of access to sensitive data must be established and documented.

Procedure for regularly reviewing and revising, as necessary, the authorization of access to sensitive data must be established and documented.

Procedures must ensure access to information systems containing sensitive data is prevented until properly authorized.

Appropriate stewards/owners and delegates must be designated and authorize all access to sensitive data. The stewards/owners and delegates must be formally documented.

Workforce Clearance

Procedures must be in place to ensure the backgrounds of individuals accessing sensitive data have been adequately reviewed during the hiring process. This includes candidates provided via third party or agency.

Procedures must be in place for a confidentiality agreement in which the workforce

member agrees not to provide sensitive data or to discuss confidential information to which they have access to unauthorized persons. Confidentiality agreements must be reviewed and signed by workforce members who access sensitive data.

Procedures must be in place to affirm the responsibility for the protection of the confidentiality, integrity, or availability of sensitive data and related processes. This must be documented, signed and must include the sanctions or reference to the sanctions which may be applied if employees do not meet their responsibilities.

Termination/Resignation

A formal, documented process for terminating access to sensitive data when the employment of a workforce member ends must be established and documented.

As part of this process their information systems resource privileges, both internal and remote, must be disabled or removed by the time of departure and consideration should be given to physical access to areas where sensitive data is located.

This must include a documented notification process which must be tracked and logged for the notification to account managers including the receipt and response to such notices. At a minimum, such tracking and logging must provide the following information and must be securely maintained:

- Date and time notice of employee departure received
- Date of planned employee departure
- Brief description of access to be terminated
- Date, time, and description of actions taken

Procedures must be in place to ensure all supplied equipment has been returned by the time of departure and has been tracked and logged. Such equipment includes, but is not limited to:

- Portable computing Devices (PCD's)
- Name tags or name identification badges
- Building, desk or office keys
- Access cards
- Security tokens, encryption keys, or PIN's

Procedures must be in place to ensure all physical security access codes/methods used to protect sensitive data/resources that are known by a departing workforce member must be deactivated or changed.

Procedure must be in place to ensure resident files are reviewed to determine the appropriate transfer or disposal of any confidential information.

Access Management and Authorization

Owners/stewards or their chosen delegates must define, authorize and document all access to sensitive data.

Procedures for granting different levels of access to sensitive data must be established, documented and implemented.

Procedures for tracking and logging the authorization of access to sensitive data must be established, documented and implemented.

Procedures for regularly reviewing and revising, as necessary, the authorization of access to sensitive data must be implemented.

Access Establishment/Modification

	Procedures for modifying access privileges to sensitive data must be established, documented and implemented. Procedures for both granting a workforce member an access method (e.g. password or token) and changing an existing access method must be established, documented and implemented. This includes procedures for managing access rights in a distributed and networked environment. Unique user identifiers (user IDs) that enable individual users to be uniquely identified must be used. User IDs must not give any indication of the user's privilege level. Common or shared identifiers must not be used to gain access to sensitive data. When unique user identifiers are insufficient or inappropriate, shared identifiers may be used to gain access to information systems resources not directly containing sensitive data. Procedures for the prompt removal or disabling of access methods for persons and entities that no longer need access to sensitive data must be established, implemented and documented. Procedures to verify redundant user identifiers are not issued must be established, documented and implemented. All revisions to workforce member access rights must be tracked and logged. At a minimum, such tracking and logging must provide the following information and be securely maintained: • Date and time of revision • Identification of workforce member whose access is being revised • Brief description of revised access right(s) • Reason for revision • Who made the change • Who authorized the change
Related Documents:	Data Classification Policy, Data Disposal and Reuse Policy, Risk Assessment Policy, Risk Management Policy, PHI Server Consolidation Policy, Minimum Necessary Rule (OU HIPAA Privacy-21 (Uses & Disclosures))