
TITLE: **INFORMATION ACCESS MANAGEMENT AND CONTROL**

PURPOSE:

Actively manage and control access to electronic information based on their data classification.

APPLICABILITY:

Hospital staff, employees, affiliates, owners, custodians, and users of information systems

POLICY:

1. Access to information is provided in the following two ways:

   A. *Application user*: By providing authentication privilege to an individual to sign on to and use an information application; and
   B. *Data flow*: By providing a manual or automated method of transfer of information from one application to another application or entity.

   Application users access information through the user interface to accomplish their work related tasks.

   A. Only authorized users may access applications and data within the applications. Applications are accessed only from devices that meet the criteria set in the ***Device and Media policy*** (#I240).
   B. Application users may not collect information to create an application without appropriate authorization and the requisite risk analysis of applications specified in ***Information Security Management Process policy*** (#I210).
   C. Application users must complete the Hospital's HIPAA Privacy and Security training specified in ***General Information Security policy*** (#I220).

   Data flows are created for purposes of integrating information views, streamlining workflows, deriving analytics and reporting.

   A. Data flows are authorized by a Hospital Vice President.
   B. Data flows of PHI data within the Hospital require that the applications are authorized in the Hospital and have undergone information security risk

analysis as specified in the ***Information Security Management Process policy*** (#I210).

C. Data flows of PHI data between the Hospital and its affiliates require that the affiliate is a covered entity, and the affiliate's application is authorized by the Information Security Office of the affiliate institution and has undergone formal information security risk analysis.

D. Data flows between the Hospital and an external entity require that an appropriate legal contractual agreement is in place, and the data flow is authorized. A Business Associate Agreement is required for such data flows with Protected Health Information (PHI).

2. Reasonable steps are taken to implement appropriate technical safeguards to control and restrict access to information systems and to implement secure data flows.

3. Any information systems that do not comply with appropriate technical safeguards are identified and evaluated according to risk analysis methods in the ***Information Security Management Process policy*** (#I210).

PROCEDURE:

Access for Application users

1. Owners and custodians are responsible for establishing, describing, and documenting different levels of access through the user interface in *Access authorization grid/rules* and *Custodian and vendor (non-end-user) access* documents as required in the ***Information Security Management Process policy*** (#I210). For applications with PHI, owners and custodians determine user access using the ***Minimum Necessary policy*** (#L125) as a guide.

   Access authorization is specified in 2 ways:

   A. Role-based Access. Roles are defined based on user attributes such as titles, departments, credentialing information, and specific authorizations in the application are assigned to such roles. A user, by virtue of belonging to a role, is entitled to the authorized access into the application. Once a role is verified, such users may be provisioned to applications, manually or automatically, without any additional approvals. The process is documented in *Account Request Procedure.*

   B. Individual Access. When an individual requires a specific or additional authorization in an application for their work, a request is made by management of the individual for specific privileges to the Information

Technology (IT) department's Service Desk which coordinates with application custodians for approval and execution of the access. The request, approvals and request status though its complete lifecycle are documented and retained in IT Service Management system. The process is documented in *Account Request Procedure.*

2. Application users may not use an application that is not authorized for use at the Hospital. All authorized applications are listed in the application inventory maintained by IT (see *Asset Inventory Procedure*).

3. In a clinical emergency, a credentialed and privileged health care professional is permitted to look up PHI of a patient, including on behalf of another health care provider who is caring for the patient and is unable to retrieve the information himself/herself for a legitimate reason. The professional providing the clinical information as well as the professional requesting the information should inform their managers with details about the access as soon as it is feasible. The Information Security Office may also be notified depending upon the extent and nature of the access.

4. Remote access to Hospital information systems is restricted to essential use as determined by appropriate managerial approval. Only secure encrypted devices using approved, secure methods such as Virtual Private Network, Information Technology Access, etc. to access Hospital assets are permitted. The following rules define remote access:

   A. All physicians and other credentialed members are permitted to access information remotely.
   B. All managers and above are permitted to access information remotely.
   C. Managers may request remote access privileges for the employees managed by them when essential in performing official duties based on a business case justification through submission of a request to the IT Service Desk.
   D. Directors may request remote access privileges for the vendor and affiliate staff sponsored and managed by them when essential in performing official duties based on a business case justification through submission of a request to the IT Service Desk.

5. The access rights to information systems are periodically reviewed and revised as necessary to ensure that access is granted only to workforce members to accomplish legitimate business-related tasks (see *Access Certification Procedure*).

6. Authentication

   A. Information systems support appropriate types of authentication or access control technology with unique user identifiers and passwords to protect the confidentiality of information.

   B. A process to assign unique user identifier called Center-Wide Identifier (CWID) to each workforce member is defined in *Center-wide Identifier Creation Procedure*. CWIDs are used to establish user accounts unless system limitations do not permit use of CWID.

   C. User accounts are terminated based on the process defined in *Termination and Account Inactivation Procedure*.

   D. Central authentication services based on Microsoft Active Directory and Oracle Java Directory Service are made available to the applications for common sign on for users. These services also enable automated provisioning and de-provisioning of accounts.

   E. Generic User Ids, necessary for service (automation) accounts, are documented by the process in *Risk Analysis Procedure*.

Data flows

7. Owners and custodians are responsible for establishing, describing, and documenting PHI data flows from and to the application in *EPHI Data Flow* document as required in the *Risk Analysis Procedure*.

8. Managers report all PHI data flows to the IT Service Desk in order to document authorization for the flow and for the inventory and risk analysis purposes.

9. All PHI data flows are collected and documented in an inventory in the IT Service Management system as specified in the *Asset Inventory Procedure.*

RESPONSIBILITY:

Information Security Office

REFERENCES:

All information security policies
Account Request Procedure (IT-CS-002)
Asset Inventory Procedure (IT-CS-004)
Access Certification Procedure (IT-SEC-003)
Center-wide Identifier Creation Procedure (IT-SEC-006)
Termination and Account Inactivation Procedure (IT-SEC-007)
Risk Analysis Procedure
Health Insurance Portability and Accountability Act of 1996, 45 CFR
164.308(a)(4)(i), 164.308(a)(4)(ii)(B), 164.308(a)(4)(ii)(C),
164.312(a)(1), 164.312(a)(2)(i), 164.312(a)(2)(ii), 164.312(a)(2)(iv),
164.312(c)(1), 164.312(c)(2),
164.312(d),
164.312(e)(1), 164.312(e)(2)(i), 164.312(e)(2)(ii)

REVIEW/REVISION DATE:

March 2005
June 2009
June 2011
Reviewed: June 2013; **March 2015**