

**TITLE: EPHI2. INFORMATION ACCESS MANAGEMENT AND CONTROL**

**POLICY:**

1. CUMC implements a documented process for authorizing, establishing, documenting, reviewing and modifying appropriate access to its Electronic Protected Health Information (EPHI) systems. User access is determined and authorized by EPHI systems owners, custodians and representatives of end users using ***Minimum Necessary policy*** as the basis for the type and extent of authorized access.
2. CUMC limits access to EPHI systems to its workforce members needing specific information in order to complete legitimate work related tasks. Workforce members are granted access to EPHI systems only when properly authorized. Workforce members are prohibited from providing access to EPHI systems to unauthorized workforce members or other unauthorized persons.
3. CUMC takes reasonable steps to implement appropriate technical safeguards to control and restrict access to EPHI and to limit access to persons and software programs that are authorized to have such access. The access control technology chosen is implemented effectively. Any EPHI systems that do not comply with appropriate technical safeguards are identified and evaluated according to risk analysis methods in ***Information security management process policy*** (#EPHI1).

**PURPOSE:**

CUMC actively manages and controls access to EPHI.

**APPLICABILITY:**

CUMC faculty, staff, students, owners, custodians, and users of EPHI systems

**PROCEDURE:**

1. Owners and custodians are responsible for creating and maintaining the following required documentation for EPHI systems:
  - A. Procedure for establishing and describing different levels of access.
  - B. Procedure for authorization of access for a user.
  - C. Procedure for granting, revising, and terminating authorization of access.

Consult Information Security Office for *Application security document list: Access authorization grid/rules* and *Custodian and vendor (non-end-user) access*.

- 
2. The access rights to EPHI systems are periodically reviewed and revised as necessary in order to confirm that access is granted only to workforce members to accomplish legitimate business-related tasks.
  3. EPHI systems support appropriate types of authentication (access control) technology with unique user identifiers to protect the confidentiality, integrity and availability of EPHI, including one or more of the following: user-based, role-based, context-based. Generic (user-independent) identifiers, when necessary, are documented by owners and custodians describing their purpose and how they are managed. Consult Information Security Office for *Application security documents list: Generic userID management*.
  4. A process to assign unique user identifiers (Center-Wide Identifier – CWID or NetID) to workforce members is implemented, as well as a process to identify terminated workforce members. All EPHI systems owners are strongly urged to use CWID to establish and terminate user accounts. Alternately, owners may choose to use Universal Network Identifier (UNI) supported by CUIT at Columbia University. Consult Information Security Office for *Information security procedures list: Center-wide identifier creation procedure and Termination procedure*.
  5. The confidentiality of EPHI at rest and during transit is protected by encrypting information when it is determined to be necessary, reasonable and appropriate through the risk analysis process. Unless specifically excluded with documentation, all communication of EPHI over the Internet outside the networks controlled by CUMC and its affiliates should be encrypted.
  6. The integrity of EPHI at rest and during transit is protected by implementing integrity controls such as message hashing, encryption, and reliable transport protocols when it is determined to be necessary, reasonable and appropriate through risk analysis process.
  7. The following are considered to determine whether EPHI stored or maintained on information systems or transmitted over the network should be encrypted or should have additional integrity controls:
    - A. sensitivity of the information
    - B. risks to the information
    - C. expected impact to functionality and workflow if the information is encrypted or has additional integrity controls
    - D. alternate methods to protect the confidentiality, integrity and availability of the information
    - E. cost of the additional measures
  8. In a clinical emergency, which is reasonably determined, any health care professional is permitted to look up EPHI of a patient, including on behalf of

another health care provider who is unable to retrieve the information himself/herself for a legitimate reason, and is caring for the patient. 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. Information Security Officer may also be notified depending upon the extent and nature of the access.

9. An application may not be accessed through scripts, programs or other automated methods (screen-scraping, etc.) to collect or modify data stored in the application without permission from the application owner. Such methods are discouraged because they add security risks to the data and performance risks to the application.

**POLICY MAINTENANCE:**

Information Security Office

**REFERENCES:**

*All information security policies*

*CU Administrative policies in Computing & Technology*

Health Insurance Portability and Accounting 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)(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:**

November 2007