

TITLE: EPHI8. INFORMATION SECURITY: FACILITY ACCESS CONTROL AND SECURITY

POLICY:

CUMC protects all facilities in which Electronic Protected Health Information (EPHI) systems are located commensurate with identified threats and risks to the physical access to the systems.

PURPOSE:

CUMC requires physical protection of its assets that contain EPHI data and systems.

APPLICABILITY:

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

PROCEDURE:

1. **Facility Access Control.** Physical access to EPHI systems and the facilities in which they are located is restricted to workforce members who are properly authorized to have access.
 - A. The perimeter of facilities that house EPHI systems are made physically sound, the external walls are properly constructed and the external doors have appropriate protections against unauthorized access.
 - B. Doors and windows of all facilities are locked when unattended. External protections, such as window guards or bars are installed on all windows at ground level and any other windows as reasonably necessary to prevent unauthorized entry.
 - C. Delivery and loading areas have procedures to prevent delivery staff from unauthorized access to its facilities.
 - D. The level of protection provided for facilities in which EPHI systems are housed is commensurate with identified threats and risks to these areas. The following categories are assigned to the facilities:
 - a. *Highly-Sensitive* – Areas where highly sensitive information (including Electronic Protected Health Information (EPHI) is created, received, transmitted or maintained but only a small, select group of workforce need access to complete their job duties (e.g., data center, network closet, etc.).

- b. *Sensitive* – Areas where sensitive information is created, received, transmitted or maintained and a moderately sized group of workforce need access to complete their job duties (e.g., radiology reading room, medical records department, etc.).
 - c. *Monitoring-Required* – Areas where large amounts of information are created, received, transmitted or maintained and a large group of workforce need access to complete their job duties (e.g., inpatient unit, outpatient clinic, public areas such as waiting room, etc.)
- E. Owners determine which workforce members are granted physical access rights to *Highly-Sensitive* areas where information systems (servers, storage area networks, etc.) are maintained. Physical access rights are provided to workforce members having a need for access to such an area in order to complete job responsibilities, and are periodically reviewed and revised. Consult Information Security Office for appropriate documentation that should be filled in *Application security documents list: Physical security, media security, media disposal*. Columbia University Biomedical and Health Information Services (CUBHIS) Department manages “Data Centers” as physical locations that are *Highly-Sensitive*.
- F. Departments managing the physical space and institutional functions associated with *Sensitive* and *Monitoring-Required* areas determine which workforce members are granted physical access rights to the area.
- G. Workforce members are required to visibly wear identification badges. Workforce members are required to report unescorted strangers or anyone not wearing visible identification to the Public Safety Department.
- H. All visitors are required to show proper identification and to sign in prior to gaining physical access to areas where information systems are located.
- I. The Security department conducts a periodic review of physical access controls used at its facilities to protect information systems.
2. **Facility Security.** Facility Security is implemented by the Public Safety Department in order to protect physical assets in CUMC facilities from unauthorized access, tampering or theft.
3. **Maintenance Records.** For *Highly-Sensitive* areas, repairs and modifications made to the physical security components such as walls, doors, etc. are documented. The owner and custodian of the area are responsible for maintaining this documentation. The documentation may include:

- A. Date and time of repair or modification
 - B. Description of physical component prior to repair or modification
 - C. Reasons(s) for repair or modification, including any damage and any related security incident, if applicable
 - D. Person(s) performing repair or modification
 - E. Outcome of repair or modification
4. **Contingency Operation.** Based on institution's Disaster Recovery and Emergency Mode Operation plan in ***Information security: Disaster contingency and recovery plan policy*** (#EPHI9), in the event of a disaster or emergency, appropriately authorized workforce members can enter appropriate facilities to take the necessary actions as documented. Such members are authorized by the owners of the EPHI systems, and are permitted to administer or modify processes and controls that protect the security of information.

POLICY MAINTENANCE:

Directors of Public Safety, Information Security Office

REFERENCES:

All information security policies

CU Administrative policies in Computing & Technology

Health Insurance Portability and Accounting Act of 1996, 45 CFR

164.310(a)(1),

164.310(a)(2)(i), 164.310(a)(2)(ii),

164.310(a)(2)(iii), 164.310(a)(2)(iv)

REVIEW/REVISION DATE:

November 2007