

TITLE: EPHI6. WORKFORCE SECURITY CLEARANCE, TERMINATION AND AUTHORIZATION

POLICY:

CUMC workforce members with access to Electronic Protected Health Information (EPHI) systems receive appropriate clearance prior to access and are terminated from accessing EPHI systems when they are no longer part of the workforce.

PURPOSE:

CUMC implements appropriate access to information systems by authorized users.

APPLICABILITY:

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

PROCEDURE:

Workforce Clearance Procedures

1. The Human Resources Department will review prospective workforce members' backgrounds who will work with EPHI during the hiring process. This practice includes but is not limited to employment reference checks, verifying professional licensure, criminal background checks and HHS OIG database checks. Employment Services, in consultation with the department head determines the appropriateness of a credit check based on the duties and responsibilities of the position.
2. All employees receive privacy and confidentiality training at the time of employment.
3. When non-CUMC employees are hired or engaged in a Department, and are given access to EPHI systems, the Department Chair or a staff at Director level (or higher) is responsible for assuring compliance with this policy.
 - A. When temporary agency staff is assigned to CUMC, it is the agency's responsibility for assuring background checks are completed as outlined in the contract.
 - B. When a volunteer, vendor, consultant or any other non-employee is provided with access to EPHI systems it is the responsibility of the sponsoring Department Chair or a staff at Director level (or higher) to assure that appropriate language covering the background checks, privacy and confidentiality training and confidentiality agreement information is included in the contract.

Termination Procedure

5. CUMC has established the following procedure to terminate access of a workforce member to EPHI systems when the member's employment at the CUMC ends or access is no longer appropriate. (Also see **Information access management and control policy**.) It is the responsibility of the Department Chair (or a designee) or a manager at Director level (or above) to notify the Owner (or Custodian) of applications the user had access to when a workforce member terminates employment. For all applications for which the Columbia University Biomedical and Health Information Services (CUBHIS) Department handles the account creation process, the CUBHIS service desk should be informed. Additionally, NewYork-Presbyterian Hospital Information Services service desk may also be informed. This will make sure that all privileges to access EPHI systems, including both internal and remote, are disabled or removed by the time of the departure, or if not feasible, immediately after. Information system privileges include workstations, server, data application and network access.
6. The Department Chair (or a designee) or a manager at Director level (or above) is responsible for retaining the individual's CUMC identification badge, access cards, keys for department, office, and desk, institution-owned portable computers (laptops), Personal Digital Assistants (PDA's), cell phones and security tokens and any other items owned by CUMC and are relevant for access to EPHI assets. Prior to or at the time of departure, a workforce member must turn over all incidental data and all removable memory sticks, USB ports, CD-ROMs (or destroy all PHI) including EPHI records in his/her possession to his/her manager.
7. The Department Chair (or a designee) or a manager at Director level (or above) is responsible for assuring that a terminated workforce member does not retain, give away, remove or destroy any EPHI from CUMC premises.

Authorization

8. A workforce member is authorized to access EPHI based on access authorization rules established for relevant EPHI assets as required in **Information access management and control policy** (#EPHI2).

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)(3)(i),

164.308(a)(3)(ii)(A), 164.308(a)(3)(ii)(B), 164.308(a)(3)(ii)(C)

REVIEW/REVISION DATE:

November 2007