

**TITLE:        EPHI4. INFORMATION SECURITY: AUDIT AND EVALUATION**

**POLICY:**

CUMC implements mechanisms to record activity on its Electronic Protected Health Information (EPHI) systems, and conducts periodic evaluation of its security safeguards, including policies, controls and processes.

**PURPOSE:**

CUMC uses audit methods to evaluate its security controls and processes with information systems in order to provide and maintain security.

**APPLICABILITY:**

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

**PROCEDURE:**

**Audit Mechanisms**

1. Custodians and owners of EPHI systems document and implement the audit mechanisms, frequency of log review, and log retention period determined as a result of the risk analysis. To the extent the procedures in this policy are not followed, custodians must document reasons for non-compliance. Consult Information Security Office for *Application security documents list: Audit Mechanisms and Login Process*.
2. The audit mechanisms implemented in EPHI systems provide the following information for each auditable event:
  - A. Date and time of activity
  - B. Description of attempted or completed activity
  - C. Identification of user performing activity
  - D. Origin of activity (for example, IP address, workstation identifier)
3. The audit mechanisms generate reports of auditable events, such as:
  - A. Failed authentication attempts
  - B. Use of audit software programs or utilities (for example, system logs)
  - C. Access to EPHI systems
  - D. EPHI system start up or shutdown
  - E. Use of privileged accounts (for example, system admin account)
  - F. Security incidents
  - G. Changes to user's security information (for example, user privileges)
  - H. Vendor and temporary account activities

- 
4. Custodians perform self-audits and report metrics (consult Information Security Office for *Application security documents list: Security metrics*), and initiate investigations and appropriate corrective actions.
  5. Custodians review the audit mechanisms annually. The risk analysis considers the following factors with respect to the frequency of reviews of audit mechanisms:
    - A. The merit or sensitivity of the information system.
    - B. The degree to which the information systems are connected to other information systems and the degree to which that connection poses a risk to the system.

### **Evaluation of Security Safeguards**

6. Departments and workforce members are included in the evaluation as appropriate, possibly including:
  - A. EPHI system owners and custodians
  - B. Executive Management
  - C. General Counsel Department
  - D. Internal Audit Department
7. The evaluation may be conducted or certified by a third party if the Information Security Office deems it necessary and appropriate.
8. Each evaluation includes:
  - A. A review of security policies and procedures to evaluate their appropriateness and effectiveness at protecting against any reasonably anticipated threats or hazards to the confidentiality, integrity and availability of EPHI systems.
  - B. An assessment and evaluation of security controls and processes as reasonable and appropriate protections against the risks identified for EPHI systems.
9. The evaluation process and results are documented by the responsible workforce member(s) in a report that is provided to the Information Security Officer. Consult Information Security Office for *Application security documents list: Information security analysis questionnaire* and *Security metrics*.
10. After an initial evaluation is completed to determine the extent of compliance with the institutional security standards, subsequent periodic reevaluations are conducted in response to environmental or operational changes occurring since the last evaluation that might impact the confidentiality, integrity or availability of information systems. Changes that may trigger a reevaluation of security safeguards include:
  - A. Known security incidents
  - B. New threats or risks to security of information systems
  - C. Changes to organizational or technical infrastructure

---

D. New security technologies that are available and new security recommendations

11. Following each evaluation, security policies, procedures, controls and processes are updated if the results of the evaluation show that such updates are required in order to protect against any reasonably anticipated threats or hazards.

### **Log-in Monitoring Process**

12. The log-in process has the following attributes:

- A. Notification displays upon log-in stating that the EPHI system must only be accessed by an authorized workforce member. Consult Information Security Office for *Notification display and confidentiality agreement standard*
- B. After maximum six (6) unsuccessful attempts to enter a password, the involved UserID must be either suspended until reset by a system administrator/ helpdesk personnel, or temporarily disabled for no less than three (3) minutes.
- C. Prior to successfully completing the log-in process, information system or application identifying information is minimized.
- D. The log-in process on information systems, has the ability to:
  - i. Record failed log-in attempts.
  - ii. Upon completion of a successful log-in, the date and time of the previous successful log-in are recorded.

13. If the above procedure cannot be followed, custodians must document reasons for non-compliance of the log-in process.

### **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)(1)(ii)(D),

164.308(a)(5)(ii)(C),

164.308(a)(8),

164.312(b)

### **REVIEW/REVISION DATE:**

November 2007

