

TITLE: EPHI1. INFORMATION SECURITY MANAGEMENT PROCESS

POLICY:

1. CUMC takes reasonable steps to implement information security (confidentiality, integrity and availability) of Electronic Protected Health Information (EPHI) by implementing appropriate and reasonable policies, procedures and controls to prevent, detect and correct security violations. The management process includes:
 - A. Security controls, policies and procedures that appropriately and reasonably prevent, detect, contain and correct identified risks to the confidentiality, integrity and availability of EPHI.
 - B. Periodic reviews and revisions of security controls, policies and procedures.
 - C. Ongoing training and awareness for workforce members on these security controls, policies and procedures.
2. CUMC information security policies and procedures, and controls take into consideration:
 - A. Size, complexity and capabilities of the organization
 - B. Technical infrastructure, hardware and software capabilities
 - C. Cost of implementing security controls
 - D. Probability and criticality of risks to EPHI

PURPOSE:

CUMC uses a risk-based approach to protect EPHI critical to institution's mission of health care, research and education.

APPLICABILITY:

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

PROCEDURE:

Responsibility

1. **Responsibility of Owners and Custodians.** A workforce member at a title of Director (or above) or a Faculty member or a CUMC-affiliated Physician who has the final responsibility for proper operation of an information system application is designated as the **Owner**. Workforce members who operationally manage the application, systems and sub-systems deployed to store and process information

are referred to as **Custodians**. Owners and Custodians have the following security management responsibilities:

- A. Protecting the confidentiality, integrity and availability of information for which they are responsible by managing security controls associated with the respective application or system.
 - B. Identifying and approving the use of security procedures and controls for which they are responsible.
 - C. Appropriately authorizing access to the information for which they are responsible to workforce members.
 - D. Immediately reporting risks, security incidents and violations of policies, procedures and controls relating to the information for which they are responsible to appropriate authority.
 - E. Supporting investigations of security violations with respect to the information for which they are responsible.
 - F. Endorsing and enabling information security training and awareness for workforce members.
2. **Responsibility of Users.** Workforce members who use information using an application or system over institutional networks and computers are referred to as **Users**. The security management responsibilities of Users include:
- A. Using information and computing resources that contain information only for appropriate purposes and consistent with their approved level of access and authorization.
 - B. Being aware of and using approved security controls.
 - C. Complying with appropriate information security policies, procedures and standards.
 - D. Immediately reporting any information security violation to the management and/or the Information Security Officer.
 - E. Attending appropriate information security training.
3. **Responsibility of Information Security Officer.** The Information Security Officer is responsible for information security management. These responsibilities include:
- A. Confirm that systems do not compromise the confidentiality, integrity or availability of information including EPHI.
 - B. Develop, document and disseminate appropriate information security policies, procedures and standards for the users, custodians and owners of information systems.
 - C. Confirm that a periodic risk analysis of information systems is completed on an ongoing basis, and oversee an effective risk management program.

- D. Approve and oversee the administration, implementation and selection of security controls for information systems.
 - E. Confirm that workforce members receive security training on an ongoing basis.
 - F. Consult the Privacy Officer to confirm that security policies, procedures and controls support compliance with the HIPAA Privacy Regulations.
 - G. Confirm the threats and risks to the confidentiality, integrity and availability of information are monitored and evaluated.
 - H. Confirm compliance and continuously evaluate information received from security incident reporting.
4. A documented risk analysis process is used as the basis for the identification, definition and prioritization of risks. The risk analysis process includes the following (Consult Information Security Office for the *Information security risks standard* document) :
- A. Identification and prioritization of the threats to information assets.
 - B. Identification and prioritization of the vulnerabilities of information systems.
 - C. Identification that a threat may exploit a vulnerability.
 - D. Qualitative identification of the impact to the confidentiality, integrity and availability of information if a threat exploits a specific vulnerability.
 - E. Identification and definition of measures used to protect the confidentiality, integrity and availability.
5. The risk analysis process is updated when environmental, operational, or technical changes arise that impact the confidentiality, integrity or availability. Such changes include:
- A. New threats or risks towards information assets.
 - B. An information security incident.
 - C. Changes to information security requirements or responsibilities that impact information. (e.g., new state or federal regulation, new role defined in the institution, new or modified security controls implemented).
 - D. Change to organizational or technical infrastructure that impacts information. (e.g., addition of a new network, new hardware/software standard implemented, new method of creating, receiving, maintaining, or transmitting information).
6. **Risk Analysis.** The risk analysis is based on the following steps:
- A. Inventory – Owners of an information system are responsible for maintaining an ongoing inventory of critical information systems and the security

measures implemented to protect those systems is conducted. Information assets are classified as follows:

Tier A assets are defined as an information system or data collection (database, files, etc.) with

1. More than 20 users with or without EPHI; or
2. More than 10 devices with EPHI (servers and workstations that store EPHI data including medical devices but not workstations used only to access EPHI using an application).

Tier B assets are defined as an information system or data collection (database, files, etc.) with:

1. 20 users or less; and
2. 10 devices with EPHI or less (servers and workstations that store EPHI data including medical devices but not workstations used only to access EPHI using an application).

Owner of a Tier A asset must complete *Information Security Risk Analysis Questionnaire* and create the documents in *Application security documents list* describing security processes for the asset. Owner of a Tier B asset must complete *Information Security Risk Questionnaire and Documentation (Limited Access)* for the asset. Consult Information Security Office for the templates for the documents.

All Tier A and Tier B assets and associated documents must be registered with the Department Head and the Information Security Office.

- B. Information Security measures analysis - The security measures that have been implemented to protect the information are analyzed to ascertain if they meet the information security policies, procedures and standards.

For Tier A assets, analysis is done by the Information Security Office based upon *Information Security Risk Analysis Questionnaire* response, and the contents of other documents in *Application security documents list* describing security processes for the asset.

For Tier B assets, the *Information Security Risk Questionnaire and Documentation (Limited Access)* in its entirety represents risk analysis, determination, and acceptance (if so indicated) for the corresponding asset.

- C. Risk determination - When security measures for an asset does not meet a security standard, risks are identified and expressed. Three factors are considered when determining the risk and its likelihood: 1) type of possible threat and its applicability, 2) the extent of effectiveness of current security

controls, and 3) likely level of impact. Risks are qualitatively expressed as high, low, and minimal.

D. The results of the risk analysis are documented and reviewed by the management, and maintained as asset documentation.

7. **Risk Management.** The strategies for risk management are proportionate with the risks to the information. The selected and implemented information security measures reasonably protect the confidentiality, integrity and availability and the risk is managed on a continuous basis. The following methods are used to manage risk:

- i. Risk elimination, mitigation, or limitation
- ii. Risk avoidance
- iii. Risk acceptance
- iv. Risk transference

The risk management process is based on the following:

- A. Risk prioritization - Risks are prioritized from high to minimal based on the potential impact to operations of the institution. Resources to address the risks, as available, are allocated according to the identified risks.
- B. Method identification - The appropriate security methods to mitigate identified risks to information are identified. Information security methods are identified based on the nature, feasibility and effectiveness of the specific method.
- C. Cost-benefit analysis - The institution considers the costs and benefits of implementing or not implementing identified security methods, as well as takes into account information plans in the future to assess the feasibility and utility of a method.
- D. Security method selection - Based on the cost-benefit analysis, the most appropriate, reasonable and cost-effective security methods for reducing identified risks is selected. The Owners and Custodians are responsible for consulting with the Information Security Office, and then creating and completing a plan of implementation.

Alternately, the risk may be accepted by senior management (Vice President (or above), or the Chair of a Department) with appropriate documentation, and a periodic review. If a previously accepted risk is realized in a real incident, the risk analysis and management are repeated with new information, and re-addressed with greater sensitivity and urgency based on the nature and extent of the incident.

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)(i)

164.308(a)(1)(ii)(A)

164.308(a)(1)(ii)(B)

164.308(a)(2)

REVIEW/REVISION DATE:

November 2007