---

**TITLE:** **INFORMATION SECURITY MANAGEMENT PROCESS**

## POLICY:

1. Reasonable steps are taken to implement information security (confidentiality, integrity and availability) of electronically maintained information including Electronic Protected Health Information (EPHI) and Personally Identifiable Information (PII) by implementing appropriate and reasonable policies, procedures and controls to prevent, detect and correct security violations. The management process includes:

    A. Classification of information in a Data Classification scheme for appropriate security of information based on its value.
    B. Security controls, policies and procedures that appropriately and reasonably prevent, detect, contain and correct identified risks to the confidentiality, integrity and availability of electronic information.
    C. Periodic reviews and revisions of security controls, policies and procedures.
    D. Ongoing training and awareness for workforce members on these security controls, policies and procedures.

2. The 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 information

## PURPOSE:

Protect information critical to institution's mission of health care, research and education using a risk-based approach.

## APPLICABILITY:

Hospital staff, employees, affiliates, owners, custodians, and users of information systems

**PROCEDURE:**

1. **Data Classification scheme**
   Data owned, used, created or maintained is classified into one of the following three categories:
   - Public
   - Institutional
   - Sensitive

   A. Public Data
   Public Data is information that is open to the public, routinely disclosed and freely made available. It is used by persons or systems external to the Hospital such as patients. Public Data is information with no local, national, or international legal restriction to access or usage, and is approved for distribution to the public without restriction and without potential harm to the Hospital, affiliates, patients or employees.

   Public Data generally has a very low risk. However, it still warrants proper protection since data integrity and availability must be maintained.

   Examples of Public Data include:
   - Public websites such as www.nyp.org
   - Press releases
   - Annual report

   B. Institutional Data
   Institutional Data is information that is guarded due to legal, proprietary, ethical or confidentiality considerations and is protected from unauthorized access, modification, transmission, deletion, storage or other use. It is intended for internal Hospital business use only with access restricted to a specific workgroup, department or group of individuals or affiliates with a legitimate business purpose for accessing such data. Institutional data is generally not made available to parties outside of the Hospital workforce members. Unauthorized disclosure of this type of data could adversely impact the Hospital, affiliates, patients or employees.

   Institutional Data generally has a low to moderate risk level. It warrants reasonable authorization but strict integrity and availability.

   Examples of Institutional Data include:
   - Hospital Intranet (infonet)
   - Policies and procedures
   - Patient Safety Friday information
   - Operational dashboards

- Physician privileges

C. Sensitive Data

Sensitive Data is information protected by statutes, regulations, Hospital policy or contractual agreements. It is highly sensitive data intended for limited, specific use by a workgroup, department, or group of individuals on a legitimate need-to-know basis. Unauthorized disclosure of sensitive data will have a serious adverse impact on the Hospital or affiliates, privacy of patients and/or employees, or on compliance with federal or state laws and regulations. Sensitive Data requires special precautions to ensure the confidentiality, integrity and availability of the information in its access, modification, transmission, deletion, storage or other use. This information must be protected from unauthorized modification or retrieval.

Sensitive Data has the highest risk level.

Examples of Sensitive Data include:

- Protected Health Information (PHI) in electronic and paper forms
- Personally Identifiable Information (PII) which include:
  - Identification information of a person, and
  - Social Security Number, or Credit card information, or Driver's license information of the person
- Restricted Hospital financial information
- Quality and performance improvement indicators
- Incidents and sentinel events
- Restricted Hospital legal information
- Passwords and their hashes, other IT configuration files

Information security measures should reasonably protect the confidentiality, integrity and availability of the information based on their data classification. For example, sensitive data must be encrypted.

2. **Responsibility of Owners and Custodians**

A workforce member at a title of Director (or above) 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 contain, store, process, transmit or receive information are referred to as **Custodians**. **Owners** and **Custodians** have the following security management responsibilities:

A. Determining the appropriate content and corresponding data classification of information;

B. Following *System Acquisition Procedure* to evaluate a potentially new information system application;
C. Registering a new application according to *Asset Inventory Procedure*;
D. Initiating and completing a risk analysis for the application according to the *Risk Analysis Procedure on a periodic basis and before any substantive change, upgrade or expansion*;
E. Addressing identified vulnerabilities to the application system or subsystems according to the *Risk Analysis Procedure*.
F. Adhering to *Change Management Procedure* for all operational and environmental changes in the application systems and subsystems including code, configuration, operating system and hardware;
G. Protecting the confidentiality, integrity and availability of information for which they are responsible by managing security controls associated with the respective application or system;
H. Implementing ***Information Access Management And Control policy* (I215)** for managing information access authorization and data flow;
I. Identifying and implementing security procedures and controls for the assets for which they are responsible based on the information security policies and procedures;
J. Immediately reporting risks, new vulnerabilities and violations of policies, procedures and controls relating to the information for which they are responsible to management and Information Security Office;
K. Immediately reporting any information security incident to management and/or the Information Security Office according to ***Information Security Incident Procedure* policy (I255)** and supporting investigations of security incidents;
L. Preparing a backup and disaster recovery plan according to ***Information Security: Disaster Contingency and Recovery Plan policy* (I250)**;
M. Enabling and completing information security training for custodians.

3. **Responsibility of Users**
Workforce members who access information using an application or system 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 in general with all information security policies and procedures, and specifically ***General Information Security policy* (I220), *Workstation Use and Security policy* (I230)**, ***Device and Media***

***Controls policy* (I240)** and ***Acceptable Use of Electronic Devices and Information policy* (HR-107)**;

D. Immediately reporting any information security incident to management and/or the Information Security Office according to ***Information Security Incident Procedure policy* (I255)**;
E. Completing information security training.

4. **Responsibility of Privileged Users**
Workforce members with empowered accounts (system administrator, applications administrator, database administrator, super-user) are referred to as **Privileged Users,** and have additional responsibilities:
   A. User accounts that have system-level privileges granted through group memberships or programs such as Microsoft Windows "User Account Control" or Unix "root accounts" have a unique account and complex password different from all other accounts held by that user. Less powerful individual user accounts are used for performing non-administrative tasks;
   B. Activities performed as administrator or super-user and use of sensitive utilities are logged and monitored where it is feasible to do so. Procedures for reviewing logs are documented in *Audit Log Processing Procedure* and *Platform Audit Log Processing Procedure*.

5. **Responsibility of Managers**
**Managers** of users have additional information security responsibilities as they determine how information is handled and used in a functional area or by a group of users under their management. In addition to the responsibilities of a User, responsibilities of **Managers** include:

   A. Consulting and complying with *System Acquisition Procedure* and ***Information Access Management and Control policy* (I215)** prior to acquiring or using a new information system or implementing a data flow within Hospital, affiliates, or with external agencies and registries;
   B. Properly authorizing a user for information access to Sensitive data as required, and specifically on personal devices and remote access as specified in ***Information Security: Device and Media Controls policy* (I240)**;
   C. Knowing the applications that are used by users for their work activities and checking that these applications are authorized applications (a list maintained by Information Technology department), and reporting them if they are not;
   D. Following ***Workforce Security Clearance, Termination and Authorization policy* (I235)** for personnel changes;
   E. Performing access certification reviews for all staff, affiliates and sponsored accounts (viz. for vendors and consultants) on a periodic basis and upon transfer to a new role or department;
   F. Implementing ***Information Security: Facility Access Control and Security policy* (I245)** for protection of physical areas under their control;

G. Preparing a business continuity plan according to ***Information Security: Disaster Contingency and Recovery Plan policy*** **(I250).**

6. **Responsibility of Information Security Office**

The Information Security Office is responsible for information security management. These responsibilities include:

A. Confirming that systems do not compromise the confidentiality, integrity or availability of electronic information;
B. Developing, documenting and disseminating appropriate information security policies and procedures or users, custodians and owners of information systems;
C. Confirming that a periodic risk analysis of information systems is completed, and overseeing an effective risk management program;
D. Approving and overseeing the administration, implementation and selection of security controls for information systems;
E. Preparing information security material for training, and confirming that workforce members receive security training on an ongoing basis;
F. Confirming that security policies, procedures and controls support compliance with applicable regulations;
G. Confirming the threats and risks to the confidentiality, integrity and availability of information are monitored, evaluated and addressed;
H. Confirming compliance and continuously evaluating information received from security incident reporting;
I. Staffing the Information Security Office with information security and risk management professionals.

7. **Risk Analysis**

A documented risk analysis process is the basis for the identification, definition and prioritization of risks. Risk analysis is done by the Information Security Office based upon *Risk Analysis Procedure*, and the contents of documents in *Application Security Documents List* describing security processes for the asset. The analysis assesses risk in the following areas:

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 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 of information.

The risk analysis process is updated when environmental, operational, or technical changes arise that impact the confidentiality, integrity or availability of information. Such changes may 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).

When security measures for an asset do not meet a security standard, risks are identified and documented. Three factors are considered when determining the risk and its likelihood:

a. Type of possible threat and its applicability,
b. The extent of effectiveness of current security controls, and
c. Likely level of impact.

Specific risks are qualitatively expressed as high, medium and low. Applications are risk rated as Critical, Elevated, Moderate and Reduced.

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

8. **Risk Management**

Strategies for risk management are proportional to the risks to the information. Risk management is an ongoing activity. The following methods are used to manage risk:

a. Risk elimination, mitigation, or limitation;
b. Risk avoidance;
c. Risk acceptance;
d. 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 severity of identified risks.

B. Method identification – 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 identified security methods, and takes into account strategic information system plans 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 are selected. The Owners and Custodians are responsible for consulting with the Information Security Office, and then creating and completing a plan of remediation implementation.

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

## RESPONSIBILITY:

Information Security Office

## REFERENCES:

*All information security policies*
Acceptable Use of Electronic Devices and Information policy (HR-107)
Asset Inventory Procedure (IT-CS-004)
Audit Log Processing Procedure (IT-SEC-004)
Change Management Procedure (IT-CS-003)
Platform Audit Log Processing Procedure (IT-SEC-005)
Risk Analysis Procedure (IT-SEC-001)
System Acquisition Procedure (IT-SEC-002)
Application Security Documents List (IT-SEC-001-F2)
Health Insurance Portability and Accountability 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:**

March 2005
June 2009
June 2011
June 2013
**Revised: March 2015**