



UNIVERSITY POLICY

SUBJECT: CORPORATE COMPLIANCE **TITLE:** PROTECTION OF SENSITIVE ELECTRONIC AND PRIVACY INFORMATION (SEI)

CODING: 00-01-15-50:00 **ADOPTED:** 02/16/05 **AMENDED:** 02/16/05

I. PURPOSE

To develop an overall policy to facilitate the University's compliance with the Health Insurance Portability and Accountability Act (HIPAA) Security Standards Final Rule CFR Part 164, the Family Educational Rights and Privacy (FERPA), the Gramm-Leach-Bliley (GLB) Safeguard Rules, and other applicable state and federal regulations which will:

- A. provide for the development and implementation of policies and procedures to prevent, detect, contain, and correct security violations;
- B. provide for the development and implementation of policies and procedures to ensure that all members of the University workforce have appropriate access to sensitive electronic information (SEI) and to prevent those workforce members who do not have access from obtaining access to SEI;
- C. provide for the development and implementation of policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed;
- D. provide for the development and implementation of policies and procedures for responding to an emergency or other occurrence that damages systems that contain SEI;
- E. provide for the development and implementation of policies and procedures that govern the receipt and removal of hardware and electronic media that contain SEI into and out of a facility, and the movement of these items within the facility;
- F. provide for the development and implementation of policies and procedures that address the final disposition of SEI, and/or the hardware or electronic media on which it is stored;
- G. provide for the development and implementation of policies and procedures that document repairs and modification to the physical components of University facilities which are related to security (for example, hardware, walls, doors, and locks);
- H. provide for the development and implementation of policies and procedures to protect SEI from improper alteration or destruction;
- I. provide for the development and implementation of procedures for removal of SEI from electronic media before the media are available for re-use; and
- J. provide for the development and implementation of electronic procedures that terminate an electronic session after a predetermined time of inactivity.

II. ACCOUNTABILITY

Under the direction of the President, the Senior Vice President for Administration and Finance, the Senior Vice President for Academic Affairs, Vice President for Legal Management, Vice President for Research, Vice President for Information Services and Technology, Vice President for Operations, and Presidents/CEOs of the Healthcare Units shall ensure compliance with this policy.

III. APPLICABILITY

This policy shall apply to any SEI that is generated during provision of education, research, or health care under the auspices of the University or by any of its agents. The responsibility for protecting University SEI applies to University workforce members and business associates working at University facilities and at any other locations where University SEI may reside.

IV. DEFINITIONS

- A. Data Steward - a person who creates, maintains, or stores a file which contains SEI and is responsible for that database.
- B. Hardware and Electronic Media - any device capable of creating, maintaining, storing, transmitting or receiving data.
- C. Workforce - the individuals who have authorized access to University SEI.
- D. SEI Officer - the individual with unit specific responsibility for publishing and disseminating policies, developing procedures, tracking SEI security training, and assisting with SEI security breaches. The SEI Officer could be either a HIPAA Officer, a GLB Officer, a FERPA Officer, or any other Officer designated to comply with the other applicable state and federal regulations, or a combination thereof.
- E. Technical Coordinator - the individual assigned to assist the SEI Officer with implementing their unit specific responsibilities.
- F. Sensitive Electronic Information (SEI) - includes electronic information that is protected by state or federal regulations. As such, it includes Protected Health Information (PHI) as defined under HIPAA regulations, as well as information governed by GLB and other applicable regulations.

V. REFERENCES

- A. Department of Health and Human Services, 45 CFR Parts 160, 162, and 164, Health Insurance Reform: Security Standards; Final Rule
- B. Federal Trade Commission 16 CFR Part 314, Standards for Safeguarding Customer Information (GLB Safeguards Rule)
- C. Information Management [00-01-10-30:00](#)
- D. Rights & Responsibilities for the Use of University-Accessed Electronic Information Systems [00-01-10-40:00](#)
- E. Records Management [00-01-10-50:00](#)
- E. Standards for Privacy of Individually Identifiable Health Information [00-01-15-05:00](#)
- F. Uses and Disclosures of Health Information With and Without an Authorization [00-01-15-15:00](#)

- G. Patient Confidentiality and Health Information [00-01-40-60:00](#)
- H. Renovation/Alteration/New Construction [00-01-70-45:00](#)
- I. Access to University Administered Systems [00-01-95-10:00](#)
- J. Protection and Authentication of Electronically Communicated Confidential or Sensitive Information [00-01-95-15:00](#)

VI. POLICY

A. Security Violations

1. Each University unit shall maintain in retrievable and usable form audit trails that log accesses to SEI. The logs should include information such as the date and time of access, the information or record accessed, the user ID under which access occurred, and if possible the reason for the access. Audit trail information shall be kept in a safe place to prevent erasure or modification. Procedures shall be established for regularly reviewing and analyzing audit logs or a random sample thereof to detect inappropriate accesses. Audit trails should be used together with system generated prompts or warning screens informing users of the sensitive content of SEI and reminding them about audit logs and sanctions for unauthorized access.
2. Security incidents such as security breaches, violations of policy, unauthorized access, audit trail data or other system warnings about unusual or inappropriate activity, and identified weaknesses in security measures shall promptly be reported by the Data Steward to the Compliance Hotline at 1-800-215-9664.
3. The SEI Officer for each University unit shall be responsible for developing the procedures specific to their unit.

B. Access to SEI

1. Access to institutional databases, servers and networks is a privilege granted by the University, to be used only for those purposes for which the access is authorized. The nature and extent of authorized access to institutional databases, servers and networks shall be determined by legitimate needs to fulfill job responsibilities.

Access to and use of these resources for purposes or activities which do not support the University's mission are subject to regulation and restriction to ensure that they do not interfere with legitimate work; any access to or use of these resources and services that interferes with the University's missions and goals is prohibited. The use and/or release of University data is further restricted under specific laws such as FERPA, GLB Safeguards Rule, and Health Information Portability and Accountability Act (HIPAA) and laws that govern intellectual property rights.

2. In general, only workforce members and business associates of the University shall have access to SEI. Under certain circumstances non-employees may be granted access under carefully monitored and restricted conditions. Such access is determined by the legitimate needs to fulfill job responsibilities. The access must be justified to have benefit to the operation of the institution. The University will require an executed confidentiality agreement before such access is granted.

3. Privileged access (often called root access) to operating system or database administration tools and interfaces for enterprise systems or systems housing confidential data or information will be at the discretion of the Vice President for IST.
4. Each individual who develops or is given access to institutional databases or networks shall read and understand this policy and all derivative policies.
5. Each individual with access to institutional databases or networks is responsible for all actions and transactions occurring during each exercise of his or her access privilege.
6. Each Data Steward shall have responsibility for:
 - a. approving authorized access to the databases/files that a person has created, maintained, or stored which contain SEI within the scope of one's job responsibilities.
 - b. ensuring prompt (within 24 hours of notification) termination or alteration of access for routine changes in an individual's status. Examples include termination of employment, graduation or withdrawal from the University, transfers to other UMDNJ departments, changes in role or responsibility, or when special vendor or courtesy accounts are no longer needed;
 - c. ensuring prompt (within 24 hours of notification) notification to IST via the Service Center of changes covered by 6b above.
 - d. ensuring security compliance;
 - e. periodically reviewing and modifying as necessary the users right of access (authorization).
7. The Vice President for IST shall be responsible for providing the University wide infrastructure with the proper level of security and authentication mechanisms by which access will be restricted to specific systems, applications and data for authorized users.
8. In order to establish individual accountability for actions on line and to implement access controls based on individual needs, every individual shall have a unique identifier or log on ID for use in logging into patient care information systems.
9. Users will be authorized to access and retrieve only that information for which they have a legitimate need to know.

C. Safeguarding Facilities and Workstations that House Electronic Information Systems from Unauthorized Physical Access While Allowing Properly Authorized Access

1. Physical access to the University data control centers shall be controlled by an appropriate authentication or access mechanism. This access system shall be monitored and maintained by Public Safety.
2. Each individual user at their workstation shall have their account authenticated through a unique logon name and password. If the user does not provide the appropriate account combination they will be denied access to the network and its resources.
3. Each individual user's logon name and password will physically allow them to only access those networks, servers, applications, programs, etc. for which they have been authorized.

4. Each workstation or group of workstations shall be housed in a secure room within the facility.
5. Each user shall be responsible for ensuring that all security devices responsible for the security of the room containing their workstation are functioning as designed, and any malfunctions shall be reported to Physical Plant for appropriate action in accordance with University policy Physical Plant Work Requests, 00-01-70-60:00.
6. All University workstations shall have screen savers that are triggered after the system has not been accessed for a defined period of time.

D. Disaster Recovery and Business Continuity Plan

1. The University's Disaster Recovery and Business Continuity Plan will include the following HIPAA Security mandated procedures.
 - a. Procedures to restore any loss of data;
 - b. Procedures to enable continuation of critical business processes for protection of the security of SEI while operating in the emergency mode;
 - c. Procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency;
 - d. Procedures for periodic testing and revision of contingency plans;
 - e. Procedures for obtaining necessary SEI during an emergency;
 - f. Procedures to create and maintain retrievable exact copies of SEI.
2. The Information Services and Technology Recovery Team will be responsible for coordination of the University's Disaster Recovery and Business Continuity Plan with the SEI Officers for each University unit.

E. The University believes that it is not feasible to maintain a record of the movements of hardware and electronic media throughout the University for the following reasons:

1. Due to the evolving technology throughout the University, there are numerous uncontrollable devices now meeting the definition of hardware and electronic media, i.e. memory sticks, PDAs, cell phones, etc.
2. Due to the size of the University, it is impractical to account for the movement of all hardware and electronic media.

As an alternative measure, the University will require that all SEI be stored, maintained, and transmitted on University supported systems in a secure environment. In addition, all units are required to utilize University approved naming conventions and to ensure that University tools for threat protection and remote diagnostics are properly installed on all eligible devices. As a final measure, when needed, the Data Steward will create and maintain retrievable exact copies of SEI that solely reside on a piece of equipment prior to this piece of equipment being moved.

F. Final Disposition of SEI and/or the Hardware or Electronic Media on Which it is Stored

1. SEI and/or the hardware or electronic media on which it is stored will not be disposed of until all New Jersey State record retention guidelines are met.

2. All SEI and/or the hardware or electronic media on which it is stored will be disposed of in a manner consistent with all HIPAA Privacy and Security Guidelines.

G. Protection of SEI from Improper Alteration or Destruction

1. Information Services and Technology (IST) shall ensure the installation of virus checking programs on all centrally supported servers University wide.
2. All University employees will be responsible for ensuring that their workstation (desktop/laptop) is running the current version of the IST defined standard threat protection software.
3. IST shall formally assess the security and vulnerabilities of the University's information systems on an ongoing basis, e.g. running "hacker scripts" and password "crackers" against the systems, and routinely using software protection tools such as virus detection software and software checksum protection.
4. Individuals may not run or install on any University computer system a program that may result in intentional damage to a file, or that may intentionally compromise the integrity of the University's systems or the integrity of other computing environments via the University's network (e.g., computer viruses, Trojan horses, worms or other rogue programs).
5. To protect against inadvertent damage, no data or program material may be transferred to non-removable storage (hard disk) of a computer or workstation without the expressed consent of the department or office responsible for the computer. Under no circumstances may program material (executable code) be transferred except from the original commercial distribution media. Exceptions may apply to software developed within the University after the program material is traced to its source.
6. Security incidents such as security breaches, violations of policy, unauthorized access, audit trail data or other system warnings about unusual or inappropriate activity, and identified weaknesses in security measures shall promptly be reported by the Data Steward to the Compliance Hotline.
7. Workforce members who spot security breaches or the potential for security breaches are responsible for reporting this information to either their supervisor or directly to IST. Workforce members always have the option of reporting such information to the Compliance Hotline.
8. Security related events on critical or sensitive systems will be logged and audit trails will be maintained subject to the capabilities of the particular system, and the ability to store detailed logs. IST will designate the individual(s) responsible to maintain a frequency and rotation of backups along with a retention schedule which complies with regulatory needs, and provides prudent recovery capability.
9. On a regular basis, audits will be performed on logged security related events on critical or sensitive systems by IST Security or their designee. Security related events include, but are not limited to:
 - a. Port-scan attacks;
 - b. Evidence of unauthorized access to privileged accounts;
 - c. Anomalous occurrence that are not related to specific applications on the host;and

- d. Continual, unsuccessful log in attempts.

H. Documentation of Repairs and Modifications to the Physical Components of UMDNJ Facilities Which are Related to Security

1. The Physical Plant Department shall be responsible for the maintenance of the following security related physical components of University facilities:
 - a. defective doors, hinges, and closers
 - b. broken window units and glass
 - c. damaged interior and exterior walls (except those special use areas that require specialized maintenance due to programmatic needs and/or non standard materials).
2. All maintenance repairs of the aforementioned Physical Plant security related components shall be documented by the requestor by completing a Physical Plant Work Request Form (hard copy or on-line on the Physical Plant website). These completed forms should be phoned, mailed, faxed, hand delivered, or submitted on-line to the requestor's Campus Physical Plant Work Control Center.
3. The procedures to implement the Physical Plant Departmental responsibilities shall be in accordance with University policy Physical Plant Work Requests, 00-01-70-60:00.
4. The University Locksmith Unit of the Public Safety Department shall be responsible for maintenance of the security related physical components of University facilities related to keys, locks, doorknobs, push bars, and latches.
5. All maintenance repairs or replacement of the aforementioned Locksmith security related components shall be documented by the requestor completing a Locksmith Work Request Form and submitting the form to the Locksmith Unit of the Public Safety Department.
6. The procedures to implement the Locksmith Unit of the Public Safety Department responsibilities shall be in accordance with University policy Issuance of Keys, 00-01-10-80:20.

I. Removal of SEI from Electronic Media Before the Media are Available for Re-use

1. The University will not re-use electronic media that contains SEI.
2. IST will develop procedures to ensure that all SEI has been removed from electronic media before the media are made available for re-use.

J. Termination of an Electronic Session After a Predetermined Time of Inactivity

1. Electronic sessions will be terminated if there is a period of inactivity to protect information systems that maintain SEI from unauthorized access.
2. IST shall be responsible for developing an appropriate time period of inactivity before the units' SEI systems terminate an electronic session.
3. IST will be responsible for developing procedures specific to each unit to ensure that all electronic sessions terminate when the predetermined time of inactivity is reached.

K. In coordination with a Technical Coordinator, a designated SEI Officer (i.e. HIPAA Officer, GLB Officer, FERPA Officer, etc) shall be responsible on a unit specific basis for:

1. publishing and disseminating the policies as set forth in this overall University policy
2. developing procedures to implement the policies as set forth in this overall University policy
3. assisting with the tracking SEI security training
4. assisting with the handling of SEI security breaches
5. overall responsibility for ensuring compliance with SEI policy.

VII. SANCTION

Any individual who violates this policy or is responsible for unauthorized breaches of SEI confidentiality shall be subject to discipline up to and including dismissal from the University as well as civil and criminal penalties. Sanctions shall be applied consistently to all violators regardless of job titles or level in the organization.

By Direction of the President:

Vice President for Legal Management

Vice President for Information Services and Technology