Protection of Sensitive Electronic Information

ROWAN UNIVERSITY POLICY

Title: Protection of Sensitive Electronic Information
Subject: Office of Compliance & Corporate Integrity (OCCI)
Policy No: OCCI:2013:P12
Applies: RowanSOM
Issuing Authority: President
Responsible Officer: Chief Audit, Compliance & Privacy Officer; Director of Information Security
Date Adopted: 07/01/2013
Last Revision: 03/30/2020
Last Reviewed: 03/30/2020

I. PURPOSE

To develop an overall policy to facilitate the Rowan University School of Osteopathic Medicine (RowanSOM) 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 provide for the development and implementation of policies and procedures:

1. to prevent, detect, contain, and correct security violations;
2. to ensure that all members of RowanSOM 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;
3. 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;
4. for responding to an emergency or other occurrence that damages systems that contain SEI;
5. 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;
6. that address the final disposition of SEI, and/or the hardware or electronic media on which it is stored;
7. to protect SEI from improper alteration or destruction;
8. that document repairs and modification to the physical components of RowanSOM facilities which are related to security (for example, hardware, walls, doors, and locks);
9. for removal of SEI from electronic media before the media are available for re-use; and
10. that terminate an electronic session after a predetermined time of inactivity.

II. ACCOUNTABILITY

Under the direction of the President, the Senior Vice President and CIO, the Dean, Director of Information Security and the Chief Audit, Compliance & Privacy Officer, shall ensure compliance with this policy. The Associate Dean for Clinical Affairs, the Clinical Chairs and the Executive Director shall implement the 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 RowanSOM or by any of its agents. The responsibility for protecting RowanSOM SEI applies to RowanSOM workforce members and business associates working at RowanSOM facilities and at any other locations where RowanSOM SEI may reside.

IV. DEFINITIONS

1. ***Data Steward*** - a person who creates, maintains, manages, controls or stores data or a file which contains SEI and is responsible for that data, file or database. Data Steward acts as the primary contact for issues related to the data for which the data steward is responsible.
2. ***Hardware and Electronic Media*** - any device capable of creating, maintaining, storing, transmitting or receiving data.
3. ***Workforce*** - Faculty, staff, students, volunteers, trainees, and other persons whose conduct, in the performance of work for RowanSOM and/or its units, is under the direct control of such entity(ies), whether or not they are paid by RowanSOM.
4. ***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; the Chief Audit,Compliance & Privacy 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.
5. ***Technical Coordinator*** - the individual assigned to assist the SEI Officer with implementing their unit specific responsibilities.
6. ***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

1. Department of Health and Human Services, 45 CFR Parts 160, 162, and 164, Health Insurance Reform: Security Standards; Final Rule
2. Federal Trade Commission 16 CFR Part 314, Standards for Safeguarding Customer Information (GLB Safeguards Rule)
3. Records Management
4. Standards for Privacy of Individually Identifiable Health Information
5. Uses and Disclosures of Health Information With and Without an Authorization
6. Patient Confidentiality and Health Information
7. Renovation/Alteration/New Construction
8. Physical Plant Work Requests
9. Access to University Administered Systems
10. Rights & Responsibilities for the Use of University-Accessed Electronic Information Systems
11. Protection and Authentication of Electronically Communicated Confidential or Sensitive Information
12. Information Classification
13. Information Security: Mobile Computing and Removable Media
14. Health Information Technology for Economic and Clinical Health Act (HITECH)
15. NIST SP 800-88 “Guidelines for Media Sanitization”

VII. POLICY

1. Security Violations
    a. Data Stewards shall define “security violation” with regard to the information they manage. A violation could include but is not limited to:
        i. Unauthorized access or modification to information,
        ii. Excessive unsuccessful attempts to access information,
        iii. Misuse (alteration or destruction) of information,
        iv. Excessive unsuccessful log on or break-in attempts.
    b. An audit trail shall be maintained where technically feasible containing sufficient information such that the violation and the user responsible may be identified. The audit trail shall contain information to identify the user ID under which the access or attempted access occurred, time and date of occurrence, the information accessed and the action in violation. The audit trail shall be kept safe to prevent modification or destruction.

c. 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 1-855-431-9967.
d. The SEI Officer for RowanSOM shall be responsible for developing the procedures specific to their unit including:
    i. Review of the audit trail,
    ii. Frequency of review,
    iii. Parties to be notified upon discovery of a violation.
e. Documentation showing evidence of the audit trail reviews, violations issued and corrective action taken shall be maintained in a secure manner.

2. Access to Sensitive Electronic Information
    a. Access to institutional databases, servers and networks is a privilege granted by RowanSOM, 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.
    b. Access to and use of these resources for purposes or activities which do not support RowanSOM' 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 RowanSOM's missions and goals is prohibited. The use and/or release of RowanSOM 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.
    c. In general, only workforce members and business associates of RowanSOM shall have access to SEI. Under certain circumstances non-employees may be granted access under carefully monitored and restricted conditions. The access must be justified to have benefit to the operation of the institution. RowanSOM will require an executed confidentiality agreement before such access is granted.
    d. Privileged 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 Senior Vice President and CIO.
    e. Each individual who develops or is given access to institutional databases or networks shall read and understand this policy and all derivative policies.
    f. Each user is responsible for all actions and transactions occurring under his/her userID while the ID is logged onto RowanSOM's network or systems.
    g. Each Data Steward shall have responsibility for:
        i. The classification of RowanSOM's information under their control as Confidential, Private, Internal or Public.
        ii. The maintenance of an inventory of all systems that create, process, collect, store or transmit their information identifying:
            1. organization name (as stated in their Business Impact Analysis (BIA))
            2. business unit name (as stated in their BIA)
            3. business function name (as stated in their BIA)
            4. business function narrative description (as stated in their BIA)
            5. name of the information system
            6. name of the data steward
            7. name of the business unit's compliance officer
            8. information system manager
            9. inherent risk of the information system (as calculated in the Information Security Risk Assessment;
        iii. Annually assess and update the Information and Risk Classification of their information, and report any changes to the Dean, the Director of Information Security and the information system manager.
        iv. Establish procedures to comply with the NIST Guidelines for Media Sanitization to securely wipe information classified as Confidential or Private stored on mobile computing devices or removable media.
        v. periodic reviewing and modifying as necessary; the users' right of access (authorization).

    h. The Senior Vice President and CIO shall be responsible for providing RowanSOM 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.
    i. 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.
    j. Users will be authorized to access and retrieve only that information for which they have a legitimate need to know.
3. Safeguarding Facilities and Workstations that House Electronic Information Systems from Unauthorized Physical Access While Allowing Properly Authorized Access
    a. Physical access to RowanSOM data control centers shall be controlled by an appropriate authentication or access mechanism. This access system shall be monitored and maintained by Public Safety.
    b. 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.
    c. Each individual user's logon name and password will allow them to only access those networks, servers, applications, programs, etc. for which they have been authorized.
    d. Each workstation or group of workstations shall be housed in a secure room within the facility.
    e. Anyone noting a malfunction in any security devices shall report the malfunction to his/her manager and to Physical Plant for appropriate action.
    f. All RowanSOM workstations shall have screen savers triggered after the system has been inactive for a defined period of time.
4. Disaster Recovery and Business Continuity Plan
    a. RowanSOM's Disaster Recovery and Business Continuity Plan will include the following HIPAA Security mandated procedures.
        i. Procedures to restore any loss of data;
        ii. Procedures to enable continuation of critical business processes for protection of the security of SEI while operating in the emergency mode;
        iii. 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;
        iv. Procedures for periodic testing and revision of contingency plans;
        v. Procedures for obtaining necessary SEI during an emergency;
        vi. Procedures to create and maintain retrievable exact copies of SEI.
    b. The Office of Information Services and Technology Recovery Team will be responsible for coordination of the University's Disaster Recovery, Business Impact Analysis and Business Continuity Plan with the SEI Officers for RowanSOM.
5. RowanSOM believes that it is not feasible to maintain a record of the movements of hardware and electronic media throughout RowanSOM for the following reasons
    a. Due to the evolving technology throughout RowanSOM, there are numerous uncontrollable devices now meeting the definition of hardware and electronic media, i.e. memory sticks, PDAs, cell phones, etc.
    b. Due to the size of RowanSOM, it is impractical to account for the movement of all hardware and electronic media.
    c. As an alternative measure, RowanSOM will require that all SEI be stored, maintained, and transmitted on RowanSOM supported systems in a secure environment. In addition, all units are required to utilize RowanSOM approved naming conventions and to ensure that RowanSOM 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.
6. Final Disposition of SEI and/or the Hardware or Electronic Media on Which it is Stored
    a. 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.
    b. 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.
7. Protection of SEI from Improper Alteration or Destruction

a. Information Services and Technology (IST) shall ensure the installation of virus checking programs on all centrally supported servers RowanSOM wide.
b. RowanSOM workforce must not disable or otherwise tamper with anti-virus or other security related software installed on RowanSOM owned equipment or cause such software to fail to function.
c. IST shall formally assess the security and vulnerabilities of the RowanSOM's information systems on an ongoing basis.
d. Individuals may not run or install on any RowanSOM computer system a program that may result in intentional damage to a file, or that may intentionally compromise the integrity of the RowanSOM's systems or the integrity of other computing environments via the RowanSOM' s network (e.g., computer viruses, Trojan horses, worms or other rogue programs).
e. 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 except for electronic information shared for the purpose of "treatment, payment or operations of health care business (TPO)." Under no circumstances may program material (executable code) be transferred except from the original commercial distribution media. Exceptions may apply to software developed within RowanSOM after the program material is traced to its source.
f. Security incidents (such as security breaches, violations of policy, or unauthorized access), 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 (855-431-9967).
g. Workforce members who identify 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.
h. 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, who upon authorized request from the Data Steward, will maintain a frequency and rotation of backups along with a retention schedule to ensure compliance with regulatory needs, and provides prudent recovery capability as required.
i. On a regular basis, audits will be performed on logged security related events on critical or sensitive systems by Data Stewards. Security related events include, but are not limited to:
    i. Evidence of unauthorized access to privileged accounts;
    ii. Continual, unsuccessful log in attempts.

8. Documentation of Repairs and Modifications to the Physical Components of Rowan SOM Facilities Which are Related to Security
    a. The Physical Plant Department shall be responsible for the maintenance of the following security related physical components of RowanSOM facilities:
        i. defective doors, hinges, and closers
        ii. broken window units and glass
        iii. damaged interior and exterior walls (except those special use areas that require specialized maintenance due to programmatic needs and/or non standard materials).
    b. 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.
    c. The procedures to implement the Physical Plant Departmental responsibilities shall be in accordance with University policy Physical Plant Work Requests.
    d. 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.
    e. 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.

    f. The procedures to implement the Locksmith Unit of the Public Safety Department responsibilities shall be in accordance with RowanSOM policy, Issuance of Keys.
9. Removal of SEI from Electronic Media Before the Media are Available for Re-use
    a. Business units shall develop procedures to ensure that all SEI has been removed from electronic media before the media are made available for re-use. Procedures shall be in compliance with NIST standards.
10. Termination of an Electronic Session After a Predetermined Time of Inactivity
    a. Electronic sessions will be terminated if there is a period of inactivity to protect information systems that maintain SEI from unauthorized access.
    b. IST shall be responsible for developing an appropriate time period of inactivity before the units' SEI systems terminate an electronic session.
    c. IST will be responsible for developing procedures specific to each unit to ensure that all electronic sessions terminate when the predetermined time of inactivity has reached.
    d. Any exceptions to the above policy will require a formal business waiver initiated by the business unit for the area represented and will require the approval of the Systems Director of Information Security and the Chief Audit, Compliance & Privacy Officer
    e. Screen savers are to be used on all Workstations unless exempted by specific Information Security waiver.
    f. Screen savers on Workstations will be configured to automatically enable after predetermined minutes of inactivity with the following controls:
        i. All Clinical workstations will be set to time out at a predetermined timeout period without requiring a password lock.
        ii. All Common workstations will be set to time out at a predetermined timeout period with a password lock.
        iii. Any exceptions to the above policy will require a formal business waiver initiated by the business unit for the area represented and will require the approval of the Systems Director of Information Security and the Chief Audit, Compliance & Privacy Officer.
11. 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:
    a. publishing and disseminating the policies as set forth in this overall University policy
    b. developing procedures to implement the policies as set forth in this overall University policy
    c. assisting with the tracking HIPAA Compliance training
    d. assisting with the handling of SEI security breaches
    e. all responsibility for ensuring compliance with SEI policy.
12. SANCTION
    a. 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 RowanSOM 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:

Signature on file

_____

Senior Vice President and CIO

Signature on file

Chief Audit, Compliance & Privacy Officer

Signature on file

Director of Information Security