

Standards for Privacy of Individually Identifiable Health Information

ROWAN UNIVERSITY POLICY

Title: Standards for Privacy of Individually Identifiable Health Information

Subject: Office of Compliance & Corporate Integrity (OCCI)

Policy No: OCCI:2013:P01

Applies: RowanSOM

Issuing Authority: President

Responsible Officer: Chief Audit, Compliance & Privacy Officer; Rowan Security Officer

Date Adopted: 07/01/2013

Last Revision: 04/01/2020

Last Reviewed: 04/01/2020

I. PURPOSE

To ensure Rowan University School of Osteopathic Medicine (RowanSOM) in compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 and the Omnibus Privacy Final Rule of 2013 to establish standards for Privacy of Individually Identifiable Health Information.

II. ACCOUNTABILITY

Under the direction of the President, the Senior Vice President for Academic Affairs, the Deans, Chief Audit, Compliance & Privacy Officer, Vice President for Administration, General Counsel, Vice President for Research, Vice President for Finance and Treasurer, Vice President for Human Resources and the Vice President, Supply Chain Management shall ensure compliance with this policy.

III. APPLICABILITY

This policy shall apply to health information that is generated during provisions of health care services to patients in any of RowanSOM's patient care units, patient care centers or faculty practices as well as Human Subjects research under the auspices of RowanSOM or by any of its agents in all RowanSOM, departments and RowanSOM owned or operated facilities.

IV. REFERENCES

1. 45 CFR, 160, Code of Federal Regulations, Title 45, Part 160, Subpart C, General Administrative Requirements, Compliance and Enforcement
2. 45 CFR, 164.514(e), Code of Federal Regulations, Title 45, Part 164, Subpart E, Security and Privacy, Privacy of Individually Identifiable Health Information
3. 45 CFR, 164.530, Code of Federal Regulation, Security and Privacy, Administrative Requirements
4. Accounting of Disclosures of Health Information
5. Disclosures of Personally Identifiable Health Information to Business Associates
6. Protected Health Information Breach Notification Policy
7. Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009
8. Omnibus Privacy Final Rule of 2013

V. POLICY

RowanSOM will implement and maintain a Privacy Program to assure compliance with state and federal laws and RowanSOM policies protecting the confidentiality of individually identifiable health information of its patients and/or Human Subjects. The Privacy Program will complement the Information Security policies of RowanSOM.

All RowanSOM employees, students, and individuals working on behalf of RowanSOM in any capacity (including Board members, medical staff, business associates, independent contractors, and volunteers) will conduct themselves and their activities in a manner so as to protect the confidentiality of patients' individually identifiable health information as required by state and federal laws and in conformance with RowanSOM policies.

A. Requirements:

1. RowanSOM's Privacy Program will consist of the following elements:

- a. University-wide and Unit Privacy Liaisons
 - i. The Chief Audit, Compliance & Privacy Officer will oversee the development, implementation and maintenance of RowanSOM's Privacy Program. The Privacy Program will complement the Information Security policies of RowanSOM.
 - ii. The Chief, Audit and Compliance Officer will also serve as RowanSOM Privacy Officer. The Privacy Officer will be implementing the Privacy Program and University-wide policies and procedures within the schools/units, and overseeing the development, implementation and maintenance of school/unit or departmental privacy policies and procedures as appropriate.
 - iii. RowanSOM's Institutional Review Boards (IRBs), will assure that informed consents include appropriate authorizations for disclosure or that authorization has been appropriately waived.
- b. School and Healthcare Unit Custodian of Medical Records
 - i. The President and the Dean maintaining Protected Health Information (PHI), will appoint a Custodian of Medical Records.
 - ii. It will be the responsibility of the Custodian of Medical Records to assure that processes are in place at their unit, and subordinate work units, to implement and monitor compliance with the elements detailed in Section V.A.1.c., below.
- c. The Chief Audit, Compliance & Privacy Officer with the assistance of appropriate Custodian of Medical Records, will direct that the following elements are developed, implemented and maintained in conformance with state and federal requirements, and are reflected in policies and procedures accordingly:
 - i. Providing notice to patients of RowanSOM's privacy practices for Protected Health Information (PHI);
 - ii. Protecting the confidentiality of uses and disclosures of PHI, including requiring appropriate authorizations, and/or an opportunity to agree or object when mandated by law for uses and disclosures of PHI;
 - iii. Implementing appropriate and reasonable administrative, technical, and physical safeguards to protect the privacy of PHI from unauthorized use or disclosure;
 - iv. Assuring that a written process is in place that allows individuals to restrict uses and disclosures of their health information. RowanSOM, however, is not required to agree to such requests.
 - v. Assuring that patients can receive communications of their health information by alternate means or alternate locations, if requested.
 - vi. Implementing a written process for maintaining and providing an accounting of RowanSOM's uses and disclosures of PHI to requesting individuals to whom the information pertains.
 - vii. Assuring that a written process is in place that allows individuals to, access, inspect and/or obtain a copy their health information;
 - viii. Assuring that a process is in place that allows individuals to request that a unit amend their health information. RowanSOM, however, may deny requests under specified circumstances;

- ix. The Chief Audit, Compliance & Privacy Officer will be the designated contact person for individuals seeking further information or clarification to the Unit's health information policies, and privacy and patient rights requirements covered under the notice. The Chief Audit, Compliance & Privacy Officer will be designated to receive complaints concerning RowanSOM and its compliance with health information privacy and patient rights requirements.
- d. All existing or new unit or departmental policies and procedures addressing any of the items in section V.A.1.c. above, or that concern the use or disclosure of PHI, and all consent/authorization forms for the disclosure of PHI, must be presented to the Chief Audit, Compliance & Privacy Officer for review to assure compliance with RowanSOM policies, as well as state and federal requirements.
- e. The Chief Compliance & Privacy Officer will communicate periodically, with the Rowan President or RowanSOM Dean on the status of all policies and procedures concerning PHI, the Privacy Program, including its implementation, training, any recommended changes or amendments. The Chief Audit, Compliance & Privacy Officer will handle any complaints or issues of non-compliance with RowanSOM or Corporate Compliance and Privacy policies.
- f. RowanSOM will promptly revise its policies and procedures related to the Privacy Program as discussed above as necessary and appropriate to comply with changes in the law. All policies and procedures will be reviewed periodically by the Chief Audit, Compliance & Privacy Officer to assure compliance with the laws, as well as for operational effectiveness. If the changes in the law also materially affect privacy practices stated in RowanSOM's notice to patients regarding privacy practices (NPP), the notice must also be changed in a timely manner.
- g. All notices to patients concerning RowanSOM privacy practices must state that RowanSOM reserves the right to make changes in its privacy practices at any time.

2. Education and Training

- a. The Chief Audit, Compliance & Privacy Officer will recommend training to refresh the RowanSOM workforce regarding the Privacy Program, policies and procedures and the regulatory requirements, as appropriate
- b. The Office of Compliance and Corporate Integrity will take necessary efforts to offer new members of the workforce privacy training within 60 days of hire.
- c. The Chief Audit, Compliance & Privacy Officer will coordinate additional training of the workforce whose functions are affected by a material change in the policies and procedures within a reasonable period of time after the change becomes effective.
- d. Training provided will be appropriately documented and the documentation will be maintained by the Chief Audit, Compliance & Privacy Officer for a minimum of six (6) years or as specified by the New Jersey State Retention Schedule.

3. Non-retaliation for exercise of Patient Rights

RowanSOM will maintain in the Code of Conduct and other applicable policies and procedures that state intimidating, threatening, coercing, discriminating or taking other retaliatory action against the following is prohibited as outlined in the Notice of RowanSOM Privacy Practices for Protected Health Information (NPP):

- a. Patients for exercising any right established by HIPAA privacy guidelines, 45 CFR 164, subpart E;
- b. Individuals and others for filing a complaint with the Secretary of Health and Human Services under 45 CFR 160, subpart C;
- c. Individuals and others for testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing under Part C of Title XI; or
- d. Individuals or others for opposing any act or practice made unlawful by 45 CFR 164, subpart E, provided the individual or person has a good faith belief that the practice opposed is unlawful, and the manner of the opposition is reasonable and does not involve a disclosure of PHI in violation of 45 CFR 164, subpart E.

B. Responsibilities:

- 1. The Chief Compliance & Privacy Officer shall be responsible for communicating and enforcing the above policy as it relates to all employees University-wide.
- 2. The President of RowanSOM and the Research Deans shall be responsible for communicating and enforcing the above policy as it relates to persons involved in patient and human subject contact.

3. The Vice President, Supply Chain Management or his or her designee shall be responsible for communicating and enforcing the above policy as it relates to vendors, independent contractors, business associates, etc.
4. RowanSOM and its units may not require individuals to waive their rights to file a complaint with the Secretary of Health and Human Services or any other right under CFR 164, subpart E, including 164.500 through 164.530, as a condition of the provision of treatment, payment, enrollment in a health plan or eligibility for benefits.
5. Monitoring and Evaluation
 - a. The RowanSOM Compliance Committee is the governing body for the evaluation and monitoring of the Privacy Program and will review compliance issues as appropriate.
 - b. The IRBs and Chief Audit, Compliance & Privacy Officer will monitor compliance with requirements for research related disclosures.
 - c. The Chief Audit, Compliance & Privacy Officer will periodically request external or internal audits to be conducted to ensure compliance with this policy.
 - d. The Chief, Audit, Compliance & Privacy Officer is responsible for investigating and reporting on allegations of non-compliance with RowanSOM privacy policies.
 - e. The Chief Audit, Compliance & Privacy Officer, under the direction of Rowan President, may be asked to conduct investigations of non-compliance with RowanSOM privacy policies.
6. Sanctions for Non-Compliance
 - a. RowanSOM will apply appropriate sanctions, against any member of the workforce who fails to comply with RowanSOM privacy policies and procedures.
 - b. The Dean, with the assistance of the Department of Human Resources, will enforce the sanctions appropriately and consistently.
 - c. RowanSOM will document all sanctions that are applied.
7. Documentation
Documentation evidencing implementation of the Privacy Program, including complaints, training, sanctions, auditing, etc., will be maintained for a minimum of six (6) years or the time period specified by the New Jersey State Retention Schedule, whichever is longer.

By Direction of the President:

Signature on File

Chief Audit, Compliance & Privacy Officer