Rowan University Policy

Title:	Breach Notification Policy
Subject:	Office of Compliance & Corporate Integrity
Policy No.:	OCCI:2013:P11
Applies:	Rowan University & Rowan-School of Osteopathic Medicine (RowanSOM)
Issuing Authority:	Rowan President & RowanSOM Dean
Responsible Authority:	Chief Compliance & Privacy Officer & Chief Information Security Officer
Adopted:	11/28/2011
Amended:	7/1/2013, 5/13/2015
Last Reviewed:	4/28/2015

I. PURPOSE

To facilitate compliance with the Health Information Technology for Economic and Clinical Health Act (HITECH) component of the American Recovery and Reinvestment Act of 2009 (ARRA) and Omnibus Privacy Final Rule 2013 breach notification of unsecured protected health information (PHI), Personal Identifiable Information (PII), Family Educational Rights and Privacy Act (FERPA), and other federal or state notification law requirements.

The Federal Trade Commission (FTC) has published breach notification rules for vendors of personal health records as required by ARRA/HITECH. The rule applies to breaches of security that are discovered on or after September 24, 2009.

II. ACCOUNTABILITY

Under the direction of the President and the Dean of RowanSOM, the Chief Compliance & Privacy Officer, General Counsel and Executive Management shall implement and ensure compliance with this policy.

III. APPLICABILITY

This policy shall apply to health information that is generated and maintained during the provision of healthcare to any RowanSOM patients and any Human Subject research under the auspices of RowanSOM or by any of its agents in all Rowan University Units, Departments and Rowan University owned or operated facilities or with any business associates of any of the above to include other Personal Identifiable Information (PII) and information applicable to FERPA.

IV. DEFINITIONS

A. **Access** - the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.

B. **Breach** - Breach of Section 13400 HITECH
(1)(A) Breach – (is the) unauthorized acquisition, access, use, or disclosure of' PHI which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.

(B) Exceptions – Breach does not include:
(i) any unintentional acquisition, access or use of PHI by an employee or individual acting under the authority of a CE or BA
(I) such acquisition was made under good faith and within the course and normal scope of employment or professional relationship…with CE or BA
(II) such information is not further acquired, accessed or used
(ii) any inadvertent disclosure for an individual who is otherwise authorized to access PHI at a facility operated by a CE or BA…
(iii) any such information received as a result of such disclosure is not further acquired, accessed, etc.
(iv) An EHR (electronic health record) created, gathered, managed, and consulted by authorized health care clinicians and staff.
(v) A PHR (personal health record) is managed, shared, and controlled by or primarily for the individual.

C. **Breach Notification**
The Organization defines Breach Notification as does ARRA / HITECH, See Section 13402. In a CE that accesses, maintains, retains, modifies, records, stores, destroys or otherwise holds, uses or discloses unsecured health information (as defined in subsection (h)(1)) shall, in case of Breach of such information that is discovered by the CE, notify each individual who unsecured PHI/PII or as related to FERPA has been or is reasonably believed by the CE or University to have been accessed, acquired or disclosed as the result of such Breach.

D. **Business Associate** - with respect to a covered entity, is a person who:

a) On behalf of such covered entity, but other than in the capacity of a member of the workforce of such covered entity or arrangement, performs, or assists in the performance of creating, receiving, maintains or transmits PHI on behalf of the covered entity, which:

i. includes claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and re-pricing;

ii. or Any other function or activity regulated by HIPAA; or

b) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in 45 CFR§ 164.501), management, administrative, accreditation, or financial services to or for RowanSOM or Rowan University and/or its units, or to or for an organized health care arrangement in which RowanSOM and/or its units participates, where the provision of the service involves the disclosure of individually identifiable health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.

E. **Covered Entity** - a health plan, health care clearinghouse, or a healthcare provider who transmits any health information in electronic form in connection with a transaction covered by HIPAA.

F. **Disclosure** - the release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information.

G. **Family Educational Rights and Privacy Act (FERPA)** - The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

H. **Harm Threshold Analysis**- the processes by which the Organization determines whether there exists any potential for financial, reputational or other harm to the patient/individual from what has been determined to be a Breach of unsecured PHI/PII or as related to FERPA.

I. **Individually Identifiable Health Information** -information that is a subset of health information, including demographic information collected from an individual, and is created or received by a health care provider, health plan, employer, or health care clearinghouse; and relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and identifies the individual; or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

J. **Law Enforcement Official** - any officer or employee of an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to investigate or conduct an official inquiry into a potential violation of law; or prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

K. **Organization** - for the purposes of this policy, the term "organization" shall mean the covered entity to which the policy and breach notification apply.

L. **Protected Health Information (PHI)** - individually identifiable health information:

• Except as provided in paragraph two (2) of this definition, that is: a) transmitted by electronic media; b) maintained in electronic media; or c) transmitted or maintained in any other form or medium.

• Protected health information excludes individually identifiable health information in: a) Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g; b) Records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and c) Employment records held by a covered entity in its role as employer.

M. **Unsecured Protected Health Information** –

• Protected health information (PHI) that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of technology or methodology specified by the Secretary of the Department of Health and Human Services (HHS) in the guidance issued under section 13402(h)(2) of Pub. L.111-5 on the HHS website. HHS has issued the following guidance to protect identifiable healthcare information.

http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/federalregisterbreachrfi.pdf

• Electronic PHI should be encrypted as specified in the HIPAA Security rule by the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without the use of a confidential process or key and such confidential process or key that might enable decryption has not been breached. To avoid a breach of the confidential process or key, these decryption tools should be stored on a device or at a location separate from the data they are used to encrypt or decrypt. The following encryption processes meet this standard.

• Valid encryption processes for data at rest (i.e. data that resides in databases, file systems and other structured storage systems) are consistent with National Institute of Standards and Technology NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices.

• Valid encryption processes for data in motion (i.e. data that is moving through a network, including wireless transmission) are those that comply, as appropriate, with NIST Special Publications 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; 800-77, Guide to IPsec VPNs; or 800-113,

Guide to SSL VPNs, and may include others which are Federal Information Processing Standards FIPS 140-2 validated.

• The media on which the PHI is stored or recorded should be destroyed in the following ways:

• Paper, film, or other hard copy media have been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed. Redaction is specifically excluded as a means of data destruction.

• Electronic media have been cleared, purged, or destroyed consistent with NIST Special Publications 800-88, Guidelines for Media Sanitization, such that the PHI cannot be retrieved.

N. **Workforce** - employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.

O. **Personal Information (PI)** - an individual's first name or first initial and last name linked with any one or more of the following data elements: 1) Social Security number; 2) driver's license number or State identification card number; or 3) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. Dissociated data that, if linked, would constitute personal information is personal information if the means to link the dissociated data were accessed in connection with access to the dissociated data.

P. **Personally Identifiable Information (PII)** - Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

Q. **Sensitive information** - Any information, the loss, misuse, or unauthorized access to or modification of which could adversely impact the interests of Rowan University in carrying out its programs or the privacy to which individuals are entitled. It includes the following:

Information that is exempt from disclosure under the New Jersey Open Public Records Act (OPRA) and the Federal Family Education Rights and Privacy Act (FERPA) such as trade secrets and commercial or financial information, information compiled for law enforcement purposes, personnel and medical files, and information contained in bank examination reports (see PL 2001, chapter 404 (c47:1A-1 – 1A-13) for further information); personal identifier such as; home address, home email address, name and DOB, unlisted phone numbers, home phone numbers, bank account numbers, social security numbers, nationality, private health information.

Information under the control of RowanSOM and Rowan University contained in a Privacy Act system of record that is retrieved using an individual's name or by any other criteria that identifies an individual (see FDIC Rules and Regulations, 12 C.F.R. Part 310, for further information).

PII about individuals maintained by RowanSOM and Rowan University that if released for unauthorized use may result in financial or personal damage to the individual to whom such information relates. Sensitive PII, a subset of PII, may be comprised of a single item of information (e.g., Social Security Number (SSN)) or a combination of two or more items (e.g., full name along with, financial, medical, criminal, or employment information). Sensitive PII presents the highest risk of being misused for identity theft or fraud, information about insurance assessments, resolution and receivership activities, as well as enforcement, legal, and contracting activities, as well as, information about insurance assessments, resolution and receivership activities, as well as enforcement, legal, and contracting activities.

R. **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 Gramm-Leach-Bliley Act (GLB) and other applicable regulations.

V. REFERENCES

A. 45 CFR 164.528, Title 45, Code of Federal Regulations, Part 164, Section 528, Security and Privacy, Accounting of Disclosures of Protected Health Information.

B. 45 CFR 164.512 (i), Title 45, Code of Federal Regulations, Part 164, Section 512, Security and Privacy, Uses and Disclosures for Which Consent, an Authorization or Opportunity to Agree or Object is not Required, Uses and Disclosures for Research Purposes

C. 45 CFR 164.514(e), Title 45, Code of Federal Regulations, Part 164, Section 514, Subpart E, Security and Privacy, Privacy of Individually Identifiable Health Information.

D. Section 13410(d) of the HITECH Act - Breach Notification Interim Final Regulation (74 FR 42740) - August 2009.

E. New Jersey Identity Theft Prevention Act - P.L. 1997, c.172 Chapter 226

F. FDIC Rules and Regulations, 12 C.F.R. Part 309

G. Privacy Act of 1974, 5 U.S.C. § 552a.

H. Open Public Records Act, P.L. 2001, c. 404

I. Identity Theft Red Flags Rule, 16 CFR 681.2

J. The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99)

K. US General Services Administration (GSA) Rules of Behavior for Handling Personally Identifiable Information (PII) {2180.1 CIO P}

The following policies provide additional and related information:

L. Access to University Records
M. Media Release: Academic, Clinical
N. Identity Theft Prevention Program

O. Standards for Privacy of Individually Identifiable Health Information
P. Access of Individuals to Protected Health Information
Q. Uses and Disclosures of Health Information With and Without an Authorization

R. Protection of Sensitive Electronic Information (SEI)
S. Reporting Compliance and Ethics Concerns
T. Information Technology Incident Management Policy and Standards
U. Omnibus Final Privacy Rule of 2013

VI. POLICY

It is the intent of RowanSOM and Rowan University to have in place a reasonable breach notification policy including procedures that address both the protection of certain information, including PHI,PI/PII or FERPA, as defined in Section IV and the prompt notification of those individuals actually or potentially affected by a breach of such information.

A suspected or confirmed breach of PHI,PI/PII or FERPA must be reported to the Office of Compliance and Corporate Integrity (OCCI) –Chief Compliance & Privacy Officer. The Chief Compliance & Privacy Officer will coordinate the investigation of the report with the affected Unit designee, and/or the Breach Incidence Response Team as necessary in determining if PHI/PII or FERPA sensitive information has been breached requiring a breach notification to the affected individual(s), and/or authorities in compliance with regulatory requirements.

In the event that a public notification of the breach may appear to be warranted, the President, Dean of RowanSOM, President & Executive Vice President for Academic and Clinical Affairs and General Counsel are to make the final determination of whether a public notification of the event is warranted.

With respect to violations of FERPA, the Office of Compliance & Corporate Integrity will log the information and notify the Rowan Office of General Counsel. Legal Counsel is responsible for directing the issue to conclusion.

Steps in Response to an Alleged Breach Investigation:

Alleged Breach of PHI:

1. Discovery of an Alleged Breach: A breach of PHI shall be treated as "discovered" as of the first day on which such breach is known to RowanSOM, or, by exercising reasonable diligence would have been known to RowanSOM (includes breaches by RowanSOM's business associates). RowanSOM shall be deemed to have knowledge of a breach if such breach is known or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent (business associate) of RowanSOM. Following the discovery of a potential breach, RowanSOM will begin an investigation which includes a risk assessment of harm. If the results of the risk assessment warrant the process will begin to notify each individual who's PHI has been, or is reasonably believed by RowanSOM to have been, accessed, acquired, used, or disclosed as a result of the breach. RowanSOM shall also begin the process of determining what external notifications are required or should be made (e.g., Secretary of Department of Health & Human Services (HHS), media outlets, law enforcement officials, etc.).

2. Breach Investigation: The Chief Compliance & Privacy Officer should manage the investigation unless otherwise directed by Rowan General Counsel and Senior Management. The management of the breach investigation will include the completion of a risk of harm assessment in coordination with others in RowanSOM as appropriate (e.g., administration, security incident response team, human resources, risk management, public relations, legal counsel, etc.) The Chief Compliance & Privacy Officer and Rowan General Counsel shall be the key facilitators for all breach notification processes to the appropriate entities (e.g., HHS, media, law enforcement officials, etc.). All documentation related to the breach investigation, including the risk of harm assessment, shall be retained by the OCCI for a minimum of six years.

3. Probability that the PHI has been compromised: For an acquisition, access, use or disclosure of PHI to constitute a breach, it must constitute a violation of the Privacy Rule. A use or disclosure of PHI that is incident to an otherwise permissible use or disclosure and occurs despite reasonable safeguards and proper minimum necessary procedures would not be a violation of the Privacy Rule and would not qualify as a potential breach. To determine if an impermissible use or disclosure of PHI constitutes a breach and requires further notification to individuals, media, or the HHS secretary under breach notification requirements, the investigator will need to perform a risk

assessment to determine if there is significant probability that PHI has been compromised as a result of the impermissible use or disclosure. RowanSOM shall document the probability of PHI has been compromised as part of the investigation, noting the outcome of the assessment process. RowanSOM has the burden of proof for demonstrating that all notifications were made as required or that the use or disclosure did not constitute a breach. Based on the outcome of the assessment, RowanSOM will determine the need to move forward with breach notification. The probability of PHI being compromised assessment and the supporting documentation shall be fact-specific and address:

I. The nature and extent of the PHI involved, which includes type of identifiers and the probability of re-identification;

II. The unauthorized person who used the PHI or to whom the PHI was disclosed to; and

III. Whether the PHI was acquired or just viewed and the extent to which the risk to the PHI has been mitigated

4. Timeliness of Notification: Upon determination that breach notification is required, the notice shall be made without unreasonable delay and in no case later than 60 calendar days after the discovery of the breach by RowanSOM or the business associate involved. It is the responsibility of RowanSOM to demonstrate that all notifications were made as required, including evidence demonstrating the necessity of delay

5. Delay of Notification Authorized for Law Enforcement Purposes: If a law enforcement official states to RowanSOM that a notification, notice, or posting would impede a criminal investigation or cause damage to national security, RowanSOM shall:

a). If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting of the time period specified by the official; or

b). If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described above is submitted during that time.

6. Content of the Notice: The notice shall be written in plain language and must contain the following information:

a. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.

b. A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, Social Security Number, date of birth, home address, account number, diagnosis, disability code or other types of information were involved).

c. Any steps the individual should take to protect themselves from potential harm resulting from the breach.

d. A brief description of what steps RowanSOM is performing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches.

e. Contact procedures for individuals to ask questions or learn additional information, which includes providing them a toll-free telephone number, an e-mail address, information on the RowanSOM Web site home page, or postal address.

7. Methods of Notification: The method of notification will depend on the individuals/entities to be notified. The investigator will utilize the following methods accordingly:

Notice to Individual(s): Notice shall be provided promptly and in the following form:

1. Written notification by first-class mail to the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification shall be provided in one or more mailings as information is available. If RowanSOM knows that the individual is deceased and has the address of the next of kin or personal representative of the individual, written notification by first-class mail to the next of kin or personal representative shall be carried out.

2. Substitute Notice: In the case where there is insufficient or out-of-date contact information (including a phone number, email address, etc.) that precludes direct written or electronic notification, a substitute form of notice reasonably calculated to reach the individual shall be provided. A substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative.

3. In a case in which there is insufficient or out-of-date contact information for fewer than 10 individuals, then the substitute notice may be provided by an alternative form of written notice, telephone, or other means.

4. In the case in which there is insufficient or out-of-date contact information for 10 or more individuals, then the substitute notice shall be in the form of either a conspicuous posting for a period of 90 days on the home page of RowanSOM's website, or a conspicuous notice in a major print or broadcast media in RowanSOM's geographic areas where the individuals affected by the breach likely reside. The notice shall include a toll-free number that remains active for at least 90 days where an individual can learn whether his or her PHI may be included in the breach.

Notice to Risk Management: Upon notice of a PHI breach incident, the Chief Compliance & Privacy Officer and Rowan General Counsel shall take the steps needed to protect RowanSOM's interest under any policies of insurance that may offer coverage.

Notice to Media: Notice shall be provided to prominent media outlets serving the state and regional area when the breach of unsecured PHI affects more than 500 patients. The Notice shall be provided in the form of a press release.

Notice to Secretary of HHS: Notice shall be provided to the Secretary of HHS as follows below. The Secretary shall make available to the public on the HHS Internet website a list identifying covered entities involved in all breaches in which the unsecured PHI of more than 500 patients is accessed, acquired, used, or disclosed.

a. For breaches involving 500 or more individuals, RowanSOM shall notify the Secretary of HHS as instructed at www.hhs.gov at the same time notice is made to the individuals.

b. For breaches involving less than 500 individuals, RowanSOM will maintain a log of the breaches and annually submit the log to the Secretary of HHS during the year involved (logged breaches occurring during the preceding calendar year to be submitted no later than 60 days after the end of the calendar year). Instructions for submitting the log are provided at www.hhs.gov.

Maintenance of Breach Information/Log: As described above and in addition to the reports created for each incident, RowanSOM shall maintain a process to record or log all breaches of unsecured PHI regardless of the number of patients affected. The following information should be collected/logged for each breach:

1. A description of what happened, including the date of the breach, the date of the discovery of the breach, and the number of patients affected, if known.

2. A description of the types of unsecured protected health information that were involved in the breach (such as full name, Social Security Number, date of birth, home address, account number, etc.).

3. A description of the action taken with regard to notification of patients regarding the breach.

4. Resolution steps taken to mitigate the breach and prevent future occurrences.

Business Associate Responsibilities: The business associate (BA) of RowanSOM that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information shall, without unreasonable delay and in no case later than 10 calendar days after discovery of a breach, notify RowanSOM of such breach using RowanSOM notification form. Such notice shall include the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the BA to have been, accessed, acquired, or disclosed during such breach. The BA shall provide RowanSOM with any other available information that RowanSOM is required to include in notification to the individual at the time of the notification or promptly thereafter as information becomes available. Upon notification by the BA of discovery of a breach, RowanSOM will be responsible for notifying affected individuals, unless otherwise agreed upon by the BA to notify the affected individuals (note: it is still the burden of the Covered Entity to document this notification).

Workforce Training: RowanSOM shall train all members of its workforce on the policies and procedures with respect to PHI as necessary and appropriate for the members to carry out their job responsibilities (refer to Policies; HIPAA Policies; Standards for Privacy of Individually Identifiable Health Information). Workforce members shall also be trained as to how to identify and report breaches within RowanSOM.

Alleged Breach of FERPA:

1. Contact the Office of Compliance & Corporate Integrity at 856-566-6136.
2. The Office of Compliance & Corporate Integrity will log the incident and direct the information to the Legal Department for continued investigation and follow-up.
3. **Maintenance of Breach Information/Log:** Rowan University shall maintain a process to record or log all breaches as related to FERPA regardless of the number of individuals affected. The following information should be collected/logged for each breach:
   a. A description of what happened, including the date of the breach, the date of the discovery of the breach, and the number of patients affected, if known.
   b. A description of the types of unsecured protected health information that were involved in the breach.
   c. A description of the action taken with regard to notification of affected individuals regarding the incident.
   d. Resolution steps taken to mitigate the breach and prevent future occurrences.

Alleged Breach of PII:

1. All incidents are required to be reported immediately to the IRT Support Desk utilizing one of the following methods to file an incident report:
   a. On the Internet, visit http://support.rowan.edu. Login with your Rowan network username and password. If you do not know your Rowan username or password go to http://www.rowan.edu/password to reset your password and/or retrieve your username
   b. Send an email message to support@rowan.edu
   c. By telephone, if on campus call Extension 4400. If off campus, dial 856-256-4400
2. All incidents will be logged and tracked
3. All incidents should be reported to the Office of Compliance & Corporate Integrity at 856-566-6136.

Sanctions for Non-Compliance:

a. Rowan University will apply appropriate sanctions against any member of the workforce who fails to comply with Rowan University privacy policies and procedures.

University Sanctions, Penalties, Fines and Discipline consist of but are not limited to:

Based on the severity of the incident and the level of severity (Low, Medium, High) the following will apply and be typical for each level:

Low – retraining and to be reviewed with the employee during annual appraisal. Also, any cost shall be borne by the Department. The Department Chair or VP will determine how these funds will be assigned.

Medium – retraining and to be reviewed with the employee during annual appraisal. Discipline will be considered up to and including dismissal from the University. Also, all costs will be borne by the Department. The Department Chair or VP will determine how these funds will be assigned.

High – retraining and to be reviewed with employee during annual appraisal. Discipline will be unpaid suspension for a minimum of three (3) days with a consideration of up to and including dismissal from the University. Civil and criminal penalties may apply. Also, all costs will be borne by the Department. The Department Chair or VP will determine how these funds will be assigned. The Deans of each College, Vice Presidents, and University President, with the assistance of the Department of Human Resources, will enforce the sanctions appropriately and consistently to all violators regardless of job titles or level within the University and in accordance with bargaining agreements for represented employees.

b. The President and Dean of RowanSOM, with the assistance of the Department of Human Resources, will enforce the sanctions appropriately and consistently.

c. Rowan University will document all sanctions that are applied.

Retaliation/Waiver: Rowan University may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise by the individual of any privacy right. Rowan University may not require individuals to waive their privacy rights as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

Sample Notification Letter to Secretary of Health & Human Services –
http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html.

Examples of Violations and Notification Recommendations:
http://www.hhs.gov/news/press/2013pres/08/20130814a.html
http://www.hhs.gov/news/press/2013pres/07/20130711b.html
http://www.hhs.gov/news/press/2013pres/01/20130102a.html

By Direction of the President:

Signature on File

Chief Compliance & Privacy Officer