

Regis University Student Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Policy

Introduction

Regis University, as an educational institution, is like all universities, subject to and governed by the Family Educational Rights and Privacy Act (FERPA), which protects the privacy of a student's education records (20 U.S.C § 1232g; 34CFR Part 99). However, in recent years, some areas of the University have begun to include non-students in their services – Regis Neighborhood Health, Counseling, and some research projects involving patient/participant specific demographics, requiring the University to address the laws and regulations that govern privacy and security of non-student records. These laws are the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. §§ 300gg. 1181 et seq. and 1320d et seq.; 45CFR Parts 144, 146, 160, 162 and 164), also known as HIPAA, and the related security rules in the HITECH Act of 2009 (42 U.S.C §§ 300jj et seq. and §§ 17901 et seq.)

While the HIPAA Privacy and Security Laws apply mostly to “covered entities” such as hospitals, clinics, and other health providers outlined as subject to the Law, Regis University self-designated parts of the University to be considered “covered” under HIPAA because of the expansion of services to the other populations mentioned above. In addition, Regis University students and faculty are provided with access to protected health information (PHI) for patients they encounter in clinical settings for which the students are expected to comply with HIPAA. Thus, as of June 1, 2013, Regis University became a hybrid covered entity, and thereby compliant with the law in both areas of privacy and security.

HIPAA Compliance

Students of Regis University must adhere to the standards of HIPAA compliance and assume full personal and professional responsibility for maintaining those standards. This Policy applies to any student in any course, internship, practicum, volunteer activity, or Regis sponsored activity, any student in a Service Learning activity, and other students who may be performing internships and/or volunteer activities in a health care facility or another “covered entity” under HIPAA as part of a Regis University class in any of the University's Colleges, and will be enforced according to the policies and procedures contained in this Policy.

Violations of the Policy by faculty, staff or other Regis University employees or representatives will be handled by the Privacy & Security Oversight Committee and Human Resources.

Definitions:

Student: any individual currently enrolled at Regis University at the time of the incident and participating in a course, program, internship, Service Learning experience, other educational experience, or is participating as a student in a Regis sponsored event

Breach: the acquisition, access, use or disclosure of protected health information (PHI) in a manner not permitted which compromises the security or privacy of the PHI

Covered entity: Under HIPAA, a covered entity is a health care provider or facility, health plan, health care clearinghouse or other provider that transmits personal health information in electronic form.

Hybrid Covered Entity: Under HIPAA, entities can designate themselves as a hybrid entity when only part or some of their activities are subject to the law. These areas are specified in the declaration of the Hybrid Entity status

PHI: (Protected health information) Information on an individual transmitted or maintained in any form that contains demographic, physical or mental health, payment of health care information or other identifiers that identifies an individual or may reasonably lead to the identification of the individual

Sanction: any corrective action taken following a violation of HIPAA or the Regis University HIPAA Privacy Policy

Need to know: Access to patient information on treatment, payment, and/or operations that is directly related to and reasonably necessary for the performance of an individual's role/job responsibilities

Authorization: Written consent from patient(s)/legally authorized decision maker(s) and institution(s) to disclose information for uses outside of treatment, payment, and operations. Authorization procedures must be consistent with institutional policies/procedures

Negligent (as applied to HIPAA): An action taken without reasonable care that results in harm or potential harm, but without the intent to cause harm. Negligence may be due to carelessness, oversight, ignorance, or poor decision-making and is considered **unintentional**

Purposeful (as applied to HIPAA): An action taken knowingly and/or maliciously with complete disregard to HIPAA standards and is considered **intentional**

Responsibility

It is the responsibility of each individual student, faculty, and other employees such as internship coordinators or Service Learning representatives to be able to recognize and refrain from any violation of the HIPAA privacy policy and to report observed violations. **A reporting form is available [here](https://imagenow.regis.edu/imagenowforms/webform/711ebada-9fe0-4ca9-a9e1-df1cb8276c0e/).**

Numerous web-based resources addressing the HIPAA privacy policy are available on the Auxiliary and Business Services Web Page (<https://in2.regis.edu/sites/rmi/HIPAA/default.aspx>). It is the responsibility of each student to review all aspects of the course syllabus or other appropriate course documents relating to the course, program, internship or other educational experience, including the HIPAA Privacy Policy. In doing so, students acknowledge that they agree to adhere to these practices and procedures.

All violations of the Regis University HIPAA privacy and security policies are taken very seriously. Violations will be reported to the Regis University HIPAA Privacy Board (HPB) to determine whether a violation has occurred, the extent of the violation, and appropriate sanctions to be applied, where necessary. If a violation occurs in an outside facility separate and apart from the University, the appropriate parties there must be notified by the clinical preceptor/faculty or faculty of record. The HPB may serve as a resource for the faculty member in the reporting process.

Regis University HIPAA Privacy Board (HPB)

The purpose of the Regis University HIPAA Privacy Board is to implement, support, monitor, and enforce student adherence to the HIPAA Privacy Policy within Regis University. The HPB performs the following functions:

- a) Determines and enforces sanctions through consultation with academic departments, schools and individual faculty to maintain consistency in violation levels and sanctions.
- b) Responds to independent concerns expressed by students and faculty regarding the HIPAA Privacy Policy and other privacy issues.
- c) Reports all violations of the HIPAA Privacy Policy immediately to the Regis University HIPAA Privacy Officer.
- d) Forwards an appeal to the HIPAA Privacy & Security Oversight Committee.
- e) Reviews all notifications of violations of the HIPAA Privacy Policy, maintains a database of violations, and reports such violations and sanctions to the Regis University HIPAA Privacy & Security Oversight Committee on a quarterly basis.
- f) Revises the HIPAA Privacy Policy and related policies and procedures as needed.
- g) Identifies training needs of Regis University students related to HIPAA and the HIPAA Privacy Policy.
- h) Collaborates on the creation and maintenance of educational training and resources for Regis University students related to the HIPAA Privacy Policy.

The HPB is comprised of:

- Regis University HIPAA Privacy Officer (non-voting member)
- One faculty from each of the major clinical disciplines in the Rueckert-Hartman College for Health Professions (RHCHP) (Pharmacy, Nursing, Physical Therapy, Health Service Education, Counseling and Family Therapy)
- One member from Service Learning or BioMed Department
- One member from Student Life

Members serve a three year minimum term to ensure continuity. At the end of the three-year term, members may renew service for an additional one to three years (no more than three years) based on agreement between the member and the member's supervisor. A Chair is elected by the Board members. The Chair serves a minimum one year term in this position. The Chair-elect will serve a minimum of one year as Chair-elect, then a minimum of one year as Chair. The Regis University Information Security Officer will be available on an as needed basis for technical consultation. The HPB reports to the HIPAA Privacy and Security Oversight Committee of Regis University and will meet annually or more frequently on an as needed basis.

A quorum is required to convene a formal HPB meeting. A quorum consists of a majority of members being present at the meeting. Meetings are scheduled on an as needed basis, but not fewer than twice per year. The HPB is a voting committee. A minimum of 75% majority is required to carry the vote.

The HPB's HIPAA Privacy Violation Database

The HPB is responsible for the creation and maintenance of a database containing all documented instances of a violation of the HIPAA Privacy Policy. The purpose of the database is to:

- Document a pattern of repeat violations for individuals
- Provide aggregate data for annual reports that identify trends, assess the level of compliance with the Policy, and support modifications to the Policy

- Identify the need for further education or resources

The written documentation of the HIPAA Privacy Policy Violation is submitted to the Chair of the HPB for placement in the database within 14 days after an incident is first reported. All violations are entered into the database, which is maintained by the Office of the Academic Dean of RHCHP. The Dean's Assistant, the HPB Chair, the HIPAA Privacy Officer, or other senior University administrators with a need to know are the only parties with access to the database.

Sanctions for Violations of Privacy Policy

The sanction process is intended to ensure compliance with the HIPAA Privacy and Security Law. The purpose of sanctions is to ensure that the student adheres to the HIPAA Privacy and Security Law to:

- Protect the public, patients, students, faculty, staff, and Regis University
- Ensure the high standard of care and best practices expected of our students
- Fulfill the professional obligation of each student to provide competent patient care

The level of sanction depends on a number of factors including the nature and severity of the violation, whether it is a first offense, and other circumstances noted by the reporter of the violation. If a violation results in a sanction that requires action by the student, the resolution of the sanction is contingent upon the student adequately meeting expectations of the HPB. Expectations of each sanction will be dependent on the sanction and will be clearly written for the student. Failure to satisfactorily complete the sanction will result in further sanctions.

Categories of Violations:

The following categories describe potential violations of the Regis University HIPAA Privacy Policy. A violation will be further delineated as negligent (unintentional) or purposeful (intentional) per the Definitions section of the policy. Violations are further considered in terms of the potential or actual harm invoked by the incident.

Acquisition/Access

Violations of *acquisition* or *access* deal primarily with the circumstances in which PHI is obtained and handled including its location and format. Violations of access also include failure to prevent improper access through inadequate safeguarding, storage, and transit, regardless of the media on which the information resides.

Examples (these examples do not represent all possible violations of this Policy):

- Taking or making copies of records containing PHI
- Removing copies of records containing PHI from the facility
- Inappropriate use of staff identification or access to unauthorized areas of a facility
- Leaving a record containing PHI in a public space
- Accessing records containing PHI without a need to know (including one's own records or those of family members)
- Taking photos/videos of patients without authorization
- Leaving PHI on a printer, desk, or other unsecure workspace

Use/Disclosure

Violations of *use and disclosure* include handling of PHI for purposes other than treatment, payment and routine health care operations without authorization. *Use* involves the unauthorized sharing, employment, application, utilization, examination, or analysis of PHI for purposes internal or external to the health care facility and may or may not include release to a third party. *Disclosure* is the release, transfer, provision of access to, or divulging in any other manner of PHI to persons or organizations outside of the facility holding the information.

Example (these examples do not represent all possible violations of this Policy):

- Use of patient identifiers for scholarly papers and presentations
- Use of clinical test results (radiology scans, pathology reports, etc.) in class for scholarly papers or presentations without it being de-identified OR without obtaining appropriate authorization from the patient and the Health Information Management (HIM, or Medical Records) department.
- Misuse of PHI for personal use.
- Sale of PHI
- Faxing PHI to the incorrect fax number
- Talking about patients within an inappropriate area (elevators, hallways, etc.)
- Failure to provide a private environment to discuss PHI
- Inappropriate disclosure of PHI to an unauthorized individual without authorization (family, friends, students, vendors, patients and other healthcare professionals without a need to know).
- Texting or sending PHI via email; inappropriately forwarding an email containing PHI.
- Posting information about patients or photos of patients on social media sites or blogs
- Making comments on social media sites or blogs that contain inappropriate PHI
- Not properly verifying individuals by phone, in person, or in writing before providing PHI
- Leaving detailed PHI on a phone answering machine without patient authorization
- Engaging in personal relationships or dating patients or their family members which can lead to sharing of PHI

Technology Security

A violation of technology security (security incident) involves the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

Examples (these examples do not represent all possible violations of this Policy):

- Leaving oneself logged onto the computer and walking away
- Loading data on unprotected devices or networks (phones, fax machines, computers, flash drives, and other media)
- Careless handling of username or passwords
- Allowing another person to access any systems using one's password
- Connecting unapproved devices to a facility computer or network
- Deliberately compromising electronic record security measures

Destruction/Disposal

A violation of destruction or disposal involves the improper destruction or disposal of PHI.

Examples: (these examples do not represent all possible violations of this Policy):

- Disposing of records containing PHI in an unsecured trash receptacle
- Failure to follow organizational policy regarding shredding of paper records

Levels of Violations:

All potential HIPAA Privacy Policy violations require consultation with a Regis University HIPAA Privacy Board member. The Board member will review the alleged violation with the reporting individual or entity to determine if there is a violation of the Regis University HIPAA Privacy Policy. The Board member refers the report of the violation to the Board for review. The HPB will determine whether a violation has occurred, the level of the violation and sanction. All instances of HIPAA privacy violations will result in notification of the student's academic advisor, and the University Privacy & Security Oversight Committee. In addition, a report will be filed with the School/Division Dean, the HPB and entered in the permanent HPB database within the RHCHP Dean's Office.

The circumstances surrounding each violation will be considered by the HPB and will determine the level of the violation. Sanctions may include:

Level One: A negligent violation or one due to lack of education and training (not including non-compliance with training requirements)

- Reduction of graded assignment
- Review of HIPAA module and training materials at facility or university/department training modules
- Failure of an assignment
- Notification of academic advisor
- Reflection

Level Two: Purposeful disregard of policies without personal gain or malicious intent; purposeful failure to follow the minimum necessary standard. Sanctions may include:

- Failure of an assignment
- Failure of clinical rotation
- Course failure
- Mandatory HIPAA training at College Level
- Mandatory HIPAA Security training
- Notification of academic advisor

Level Three: Blatant misuse of information in following standards, willful disregard of a known risk, purposeful disregard with personal gain or malicious intent. Sanctions may include:

- Course failure
- Program dismissal
- University expulsion

- Mandatory HIPAA training at College level
- Mandatory HIPAA Security training
- Academic probation and ongoing surveillance of HIPAA compliance

Additional considerations for sanction:

- Impact
- Mitigating circumstances (e.g., coercion, intent)
- Previous infractions

The final level of violation and corresponding sanction is the decision of the HPB and will include consultation with the reporting faculty/unit. See the Table in Appendix A for examples of violations, sanctions, and remediation by level.

Repeat Violations

A repeat violation may result in a more serious sanction. For example, if two Level One Violations have occurred, the HPB may enforce a Level Two Violation Sanction.

Procedures

1. The reporting faculty or staff member identifies a violation of the HIPAA Privacy Policy and notifies the appropriate supervisor. The following steps are then completed (Note: if the violation occurred at a clinical agency, the appropriate agency representative/contact should be notified):
 - a. The reporting faculty or staff member notifies his/her respective division/school HPB representative of the incident. The faculty or staff member completes the Notification of HIPAA Policy Violation form (available on Web Advisor).
 - b. The HPB representative reports the incident to the HPB Chair and the Regis University HIPAA Privacy Officer immediately.
 - c. The representative HPB member of the reporting division/school conducts an initial meeting with the student to notify the student of the violation report and describe the HPB review process.
 - d. The student is notified in writing that a potential violation has occurred. This notification must also inform the student that s/he may submit a written response to the HPB within five business days after receiving notice of the violation. The student may be removed from the class and/or clinical placement pending an investigation.
 - e. The HPB then investigates the violation, which may include, but is not limited to, consultation with the individual reporting the violation and the student involved in the violation.
 - f. The faculty and student follow any specific requirements for investigation, including specified timeframes determined by the HPB and the clinical agency (or outlined in affiliation agreements).
 - g. The HPB determines if a violation has occurred, the level of violation, and determines the sanction.
 - h. The faculty and/or supervisor will be notified of the decision by the Chair of the HPB. The HPB informs the student in writing of the HPB's decision and, if applicable, the sanction with a copy to the reporting faculty and program director or Dean. The student is also informed of the appeal process.

- i. The HPB Chair enters the violation information into the HPB database.
 - i. The Imagenow database holds the initial report and final decision information. Imagenow only available to view by Chair and Co-Chair. Secure access.
 - ii. The secure database Office 365 will hold the specific documents/details regarding each case. This database is secure and accessible only by HPB members given access by Chair.
- j. If the violation is Level II or III and affects the student's progression in a program or results in course failure, correspondence will be initiated by the appropriate Dean or Director. (A violation at Level II may cause a course failure and in some programs, this may affect progression).

Note that in some cases, the HPB may work in tandem with the clinical agency in determining whether a violation occurred and in determining an appropriate sanction. Sanctions may also be applied by the agency apart from those applied by the HPB.

Appeals of HIPAA Privacy Policy Sanctions

HIPAA Privacy Appeals Board

Because of the adjudicatory function of the HPB, the case and surrounding evidence will have previously been reviewed by the HPB. For this reason and to provide fundamental fairness to the student appeal process, appeals will be heard by the University HIPAA Privacy & Security Oversight Committee acting in the role of an Appeals Board. This Committee, required by the HIPAA Privacy & Security Law for Covered Entities is comprised of representatives from University Legal Counsel, Risk Management, Human Resources, Regis Neighborhood Health, Student Health Services and the University HIPAA Privacy & Security Officers. For purposes of any appeal, University Legal Counsel will not participate as a member of the Appeals Board but may be consulted for legal advice and guidance. Additionally, when an appeal is heard, the current Chair of the HPB will be invited to serve on the Appeals Board.

The Appeals Board will meet on an as needed basis to hear an appeal. All decisions rendered by the Appeals Board will be final. University Legal Counsel may be consulted as necessary for adherence to the process and application of the law.

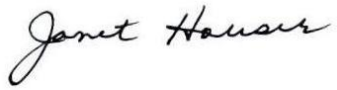
Students may only appeal the *level* of a violation; not whether a violation has occurred.

Student Appeals Process

1. The student submits a written appeal to the Chair of the HPB within seven days after receiving notification of the sanction, which must include the student's rationale and reason for the appeal.
2. The HPB Chair notifies the Privacy & Security Oversight Committee to convene the Appeals Board, which reviews all documentation forwarded by the HPB and conducts further investigation if warranted. The Appeals Board renders a decision and notifies the student of that decision with a copy to the HPB, generally within three working days after the Board's decision.
3. The possible decisions are as follows:
 - a. Student appeal is denied, sanction is upheld.
 - b. Student appeal is successful; sanction is modified
4. The School or Department completes any additional documentation and notification processes necessary related to carrying out the sanction such as notification to the Registrar.
5. The decision of the Privacy & Security Oversight Appeals Board is final.

NOTE: The HPB appeal process is limited to consideration of the specific violation(s) of the HIPAA Privacy Policy. Other aspects of student academic performance or related violations of the Student Code of Conduct

must be handled according to the normal processes outlined in the University Bulletin and the relevant student handbook.

A handwritten signature in cursive script that reads "Janet Houser".

Janet Houser, PhD
Provost
Regis University
July 5, 2018

Appendix A

Level One Examples	Possible Sanctions
<ul style="list-style-type: none"> ● Misplacing or leaving patient care sheets or notes with PHI in public areas ● Leaving a workstation without logging off ● Talking about patients in an inappropriate or public area such as elevators, cafeteria, break rooms ● Failure to provide a private area to discuss PHI ● Texting or sending PHI via email ● Forwarding an email containing PHI ● Responding to a phishing attempt 	<p>Reduction of graded assignment Failure of an assignment Review HIPAA module and training materials at facility or University/department training modules Review of HIPAA violation cases Reflection paper</p>
Level Two Examples	Possible Sanctions
<ul style="list-style-type: none"> ● Any level one, that is shown to have knowledge, intent, or a repeat offense. ● Using diagnostic results or other sensitive PHI in class for papers, presentations, etc. without de-identification or obtaining consent through facility channels ● Leaving unprotected PHI on phones or other media ● Inappropriate use of staff identification or access to unauthorized areas of a facility ● Posting PHI and/or pictures of patients on social media or other sites or in any aspect of a class without de-identification or appropriate permissions ● Taking pictures of data, patients or facilities ● Connecting unapproved devices or media to a facility network ● Inappropriate disclosure of confidential information to an unauthorized individual without permission ● Disclosing information that could harm a patient ● Disclosing a password to another person ● Leaving PHI on an answering machine or phone without permission 	<ul style="list-style-type: none"> ● Failure of an assignment ● Failure of clinical rotation ● Course failure ● Mandatory HIPAA training at College Level ● Mandatory HIPAA Security training
Level Three Examples	Possible Sanctions
<ul style="list-style-type: none"> ● Accessing records/PHI without need to know (intentional) ● Intentional distribution of PHI ● Sale of PHI ● Theft of PHI ● Inappropriate and purposeful destruction of PHI 	<ul style="list-style-type: none"> ● Course failure ● Program dismissal ● University expulsion ● Mandatory HIPAA training at College Level ● Mandatory HIPAA Security training ● Academic probation and ongoing surveillance of HIPAA compliance

<ul style="list-style-type: none">● Taking and sharing of pictures of patients, data and/or facilities (intentional)● Engaging in personal relationships that involve disclosure of PHI● Misuse of PHI for personal use/gain● Deliberately compromising electronic record security measures● Removing PHI in any form from a facility without express permission● Repeated previous offenses.	
--	--

Revised: July 5, 2018

HIPAA Privacy Board Approved: February 2018