HIPAA Privacy & Security Reminder

The goals for maintaining rigorous adherence to HIPAA compliance requirements within all Regis University-sponsored programs, projects and activities are designed to:

- Ensure the security and confidentiality of PHI and ePHI as covered by HIPAA;
- Protect against any anticipated threats or hazards to the security or integrity of such information, and
- Protect against unauthorized access, use or disclosure of such information.

Each student should have completed the necessary training on how to comply with the policies and procedures for maintaining HIPAA compliance. If you have not received or completed your HIPAA training at Regis University, you must inform your instructor.

Reminders

Protected health information is any information that allows you associate a person's identity with their health care information. This applies to all forms of media including: paper documents, electronic files and data, course notes, research papers, video and sound recordings, photos, charts, etc. As it pertains to Regis University-sponsored programs, project and activities, the following are reminders of common privacy and security practices for protected health information that must be followed:

- Any personal documents and notes in any form that contains individually identifiable health information on patients you come into contact with as a result of Regis University-sponsored training must be properly protected and its confidentiality must be maintained.
- Regis University students who are training at partner health provider organizations are prohibited from removing documents that contain individually identifiable health information without a written and signed authorization from the health care provider's Health Information Management (HIM) Department or authorized representative ***and*** the proper patient authorization.
  Special note on minors—in most cases, minors cannot legally consent or authorize the release of their protected health information.
- Regis University students participating in Regis University-sponsored health care training and research activities must only use de-identified information or limited data sets in any presentations or publications outside of the health care provider organization. (See Appendix A on 'How to de-identify individual health information'.)
- For Regis University students participating in Regis University-sponsored health care training and research activities, the following activities involving individually identifiable health information are explicitly prohibited:
  - Sending such information through unsecure email,
  - Posting such information on any social networking site—regardless of the user account used by the Regis University student, faculty or staff to post the information, and
  - Disclosing such information during classroom discussions and/or presentation.

Policy compliance and sanctions

It is the responsibility of each student to review all aspects of the course syllabus including the Regis University HIPAA Privacy & Security Reminders. In doing so, the student acknowledges that he or she agrees to adhere to these practices. Furthermore, I agree not to divulge the contents of or to provide access to any student documents in my possession that contain PHI or IIHI to another student during the current or ensuing semesters.

All violations of the Regis University HIPAA privacy and security policies and practices are taken very seriously. All violations will be reported to the Regis University HIPAA Privacy & Security Committee for review to determine the extent of the violation and the appropriate sanctions to be applied, where necessary.

Sanctions may include sanctions may include notification of the student's advisor with a note in the student's advising file, reductions in the grade for the course up to and including failure, termination from the program or other remedial actions as directed by the Regis University HIPAA Privacy & Security Committee.

Reporting requirements
In the event that any Regis University staff, faculty or student becomes aware of the unauthorized use or disclosure of PHI or ePHI that is under the control and protection of Regis University, the incident must be reported within 5 days of discovery to:

Sheila Carlon, HSA Division Director
Regis University
3333 Regis Blvd.
Denver, CO 80221
303 458 4108
PrivacyOfficer@Regis.edu

With a copy to:
Susan Layton,
Associate Vice President
Regis University
3333 Regis Blvd.
Denver, CO 80221
slayton@regis.edu

Appendix A: How to de-identify individual health information

Health information must be stripped of all of the following elements that identifies the individual, his or her relatives, employers, or other household members

- Names;
- Social Security numbers;
- Telephone numbers;
- All specific geographic location information such as subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code, if, according to the current publicly available data from the Bureau of the Census: (1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000;
- All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
- Fax numbers;
- Electronic mail addresses;
- Medical record numbers;
- Health plan beneficiary numbers;
- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers;
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) address numbers;
- Biometric identifiers, including finger and voice prints;
- Full face photographic images and any comparable images; and
- Any other unique identifying number, characteristic, or code (note this does not mean the unique code assigned by the investigator to code the research data).