

Declaration statement

The primary function of Regis University is to educate men and women of all ages at the graduate and undergraduate level. In the course of providing educational and research learning experiences to Regis University health care students and staff, certain departments and programs may include activities that fit the definition of the activities of a covered entity and involve the use and handling of PHI and ePHI. When organizations have some healthcare components and some non-healthcare components, the entire organization is subject to HIPAA unless it declares itself to be a "hybrid entity." As allowed by 45CFR164.103 and 45CFR164.105(a)(2)(iii)(C), Regis University is designating itself as a "Hybrid Entity" for the purposes of HIPAA compliance.

Designation of covered components

The Regis University components covered under the designation of hybrid entity is limited to the following:

In the College for Professional Studies, the following programs are covered:

- M.A. Counseling
- M.A. Marriage and Family Therapy

In the Rueckert-Hartman College for Health Professions, the following programs are covered:

- Division of Health Services Administration
- Loretto Heights School of Nursing
- School of Pharmacy
- School of Physical Therapy
- Clinical Care Areas

Compliance requirements for designated hybrid entity components

It is the responsibility of the chairperson of any department or program that is not listed above to notify the Regis University HIPAA Privacy & Security Committee if any of its students, staff or faculty are:

- Signatory to a Business Associate Agreement or other Data Use Agreements that covers a Regis University-sponsored program, project or activity;
- A participant in a Regis University-sponsored program, project or activity covered by a Business Associate Agreement or other Data Use Agreements, or
- A participant in a Regis University-sponsored program, project or activity that involves the use, access or handling of PHI or ePHI as defined in HIPAA that is not covered by a Business Associate Agreement or other Data Use Agreements.

Departments and programs identified as a hybrid entity component are required to follow the applicable requirements of the HIPAA Privacy & Security Rules in accordance with the University's HIPAA policies and procedures. It is the policy of Regis University to:

- Ensure the security and confidentiality of PHI and ePHI as covered by HIPAA 45 CFR Parts 160 and 164;
- 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.

If other departments need to access protected health information in the course of providing support to a covered component, the covered component is responsible for ensuring the appropriate HIPAA training has been completed by the personnel that will be accessing the protected health information.

If a third-party has access to the PHI or ePHI under the control of a Regis University covered component, that third part must agree in writing to comply with the applicable HIPAA privacy and security requirements.

Reporting requirements in the event of a suspected breach

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

Policy compliance and sanctions

Systems, resources, user activities and processes will be monitored to verify proper operation of the university's HIPAA privacy and security practices. All violations of the Regis University HIPAA information security program, its policies and associated practices shall be reported to the Regis University HIPAA Privacy & Security Committee.

Serious or repeat violations will, when appropriate, be reported to the Human Resources Department or Legal Department for follow-up.