HIPAA FAQs

Q. WHAT IS HIPAA?

HIPAA stands for "Health Insurance Portability and Accountability Act of 1996." It is a set of federal rules designed in part to protect the privacy of a person's health care information.

Q. HIPAA, HIPPA, or HIPPO?

H-**I**-**P**-**A**-**A** (with two **A**'s not two P's) Unfortunately, HIPAA is commonly misspelled on the internet.

Q. DO GEORGIA'S CONFIDENTIALITY AND PRIVACY LAWS STILL APPLY?

Yes. Georgia's laws protect the confidentiality and privacy of patient health information to the extent these laws are more stringent than HIPAA Rules, Georgia also has an Identity Theft Law which requires the appropriate destruction of records containing directly identifiable data.

Q. WHAT DOES HIPAA'S PRIVACY RULE DO?

The Privacy Rule establishes patient rights to privacy and sets the requirement to protect individually identifiable health information.

Q. WHAT IS PROTECTED HEALTH NFORMATION?

Protected health information (PHI) is any information in the medical record or designated record set that can be used to identify an individual and that was created, used, or disclosed in the course of providing a health care service such as diagnosis or treatment. It applies to PHI in any form: electronic or paper records; x-rays; schedules; medical bills; dictated notes, dental casts, conversations and more.

Health information + Directly Identifiable Data = PHI

Q. WHAT DATA ARE “DIRECTLY IDENTIFIABLE”?

Names; All geographical subdivisions smaller than a State; All elements of dates (except year) for dates directly related to an individual, except that such ages and elements may be aggregated into a single category of age 90 or older; Phone numbers; Fax numbers; Electronic mail addresses; Social Security numbers; 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 data).

Q. DO HIPAA RULES APPLY TO HEALTH INFORMATION CONTAINING NO PERSONAL IDENTIFIERS?

No. After removing all identifiers, the data are de-identified and HIPAA regulations no longer apply.

Q. WHAT ARE SOME RIGHTS HIPAA GIVES TO PATIENTS?

Patients have the right to:

- Receive our Notice of Privacy Practices (NPP)
- Access and copy medical billing records
- Request an amendment of PHI or other record
- Request an accounting for some disclosures
- Request for restrictions on uses and disclosures of their PHI
- Request the use of alternate channels of communication of PHI (e.g. use a different telephone number, different address, etc.)
- Report to us or to the federal Department of Health and Human Services about a HIPAA violation

Q. WHAT DOES THE PRIVACY RULE REQUIRE?

The Privacy Rule limits use and disclosure of PHI to the "minimum necessary." It also requires safeguards be taken to prevent improper disclosure of PHI. Access must be limited to those with a work-related “need-to-know.”

Q. WHAT IS "USE"?

Use" is accessing PHI to perform treatment, payment or health care operations (TPO) or other authorized tasks. Use of PHI must be kept to the "minimum necessary" to complete the task. However, broader use is granted for treatment purposes.

Patients can authorize the use of their PHI for research or instructional purposes. Alternatively, Georgia Regents University’s (GRU) Institutional Review Board (IRB), may waive patient authorization for certain research activities. Patients may also authorize use of their PHI for marketing, fundraising or other specific purposes.

Q. WHAT IS "DISCLOSURE"?

"Disclosure" means sharing PHI outside Georgia Regents enterprise. Patients have a right to request an accounting of such disclosures outside of TPO purposes. Waivered research authorization must be noted into the HIMS Disclosure Log.

Q. WHAT IS MY RESPONSIBILITY UNDER THE PRIVACY RULE?

Your job is to make reasonable efforts to limit the use and disclosure of PHI to the minimum necessary to accomplish the task. It is also your responsibility to report violations of the privacy rule to the enterprise privacy officer, Christine Adams at (706) 721-5631 or chradams@gru.edu

Q. WHAT DOES HIPAA PROHIBIT?

Access, use and disclosure of PHI for those without a work-related are considered to be unauthorized. Georgia Regents’ policy does not permit individuals to access personal or family members' medical records or appointments.

Some disclosures cannot reasonably be prevented such as patient/provider conversations in hospital rooms or signing in at the front desk. The key is to make reasonable efforts to limit incidental uses and disclosures. Such disclosures need not be entered into the disclosure log.

Q. WHAT DOES THE SECURITY RULE DEMAND?

The HIPAA Security Rule sets safeguards for electronic devices which access, store or transmit PHI. This applies to entity owned and personally owned computers, laptops, networks, and mobile devices used for these purposes.

Administrative safeguards include auditing access to electronic records, providing training about security requirements, and having a disaster recovery plan. Physical precautions include posting guards at building entrances, logging off, and placing servers in locked rooms. Technical safeguards are measures such as using strong passwords and encrypting transmitted data.

Q. WHAT SECURITY MEASURES CAN I TAKE TO BE MORE RESPONSIBLE?

- Pick complex or hard-to-guess passwords
- Use encryption on all electronic devices which store or transmit PHI
- Do NOT share computer log-in accounts or passwords, not even with your supervisor
- Do NOT email PHI outside the gru.edu domain without encryption

Q. DO HIPAA RULES APPLY WHEN I WORK OFF-CAMPUS?

Yes. When working remotely, use the same security safeguards (encryption, updated anti-virus and malware, firewalls, authenticated access, etc.) on your mobile devices as on your office computer. Never allow family or friends access to PHI. Never leave devices unsecured in vehicles or out of your sight during travel.

Q. HOW DO I REPORT SUSPECTED SECURITY BREACHES?

Report suspected security breaches to security officer at 706-721-1577 or ITSERVICE@gru.edu Security incidents occur when confidentiality, integrity or availability of the data has been inappropriately changed, abused, or compromised.

Examples of security breaches include:

- Accessing electronic health records without authorization
- Sharing passwords or log-in information
- Accessing PHI without authorization or a work-related need
- Emailing unencrypted PHI outside the gru.edu domain
- Losing an unencrypted USB drive containing PHI
- Misdirected emails or faxes containing PHI

Q. WHO DOES HIPAA AFFECT?

HIPAA affects workforce, student, and volunteers involved in clinical, instructional and research operations.

Business associates are required to comply with HIPAA regulations as well. Business associates are vendors or service providers who must access PHI in order to provide service.

Q. WHY IS IT ALLOWABLE TO SHARE PHI BETWEEN THE UNIVERSITY AND THE HEALTH SYSTEM?

Under the guidance of the HIPAA rule, GRU and the GR Health System formed an Organized Health Care Agreement (OHCA). OHCAs permit PHI to be shared between covered entities which are clinically integrated. Included in our OHCA are the Medical College of Georgia, the College of Nursing, the College of Allied Health Sciences, The Graduate School, GR Medical Center, and the GR Medical Associates. The Enterprise Privacy Officer and Information Security Officer oversee the HIPAA compliance aspects for all entities.

Q. CAN GRU'S COLLEGE OF DENTAL MEDICINE, STUDENT HEALTH SERVICES, GEORGIA WAR VETERANS NURSING HOME, and GEORGIA CORRECTIONAL HEALTH CARE SHARE PHI?

No. Although these entities must comply with the HIPAA rule but they are not included in the OHCA because these records are not clinically integrated. Nor do they share a common "Notice of Privacy Practices." Only members of the OHCA may share PHI.

Q. HOW AND WHEN DO I RECEIVE HIPAA TRAINING?

GRU and GR Health System trains all workforce and students, regarding the proper use and disclosure of patients' health information. Training is appropriate for the level of staff duties and may include both general training and advanced training. The Division of Human Resources is responsible for administering and documenting the training program for employees upon hire and then annually. The college in which a student is enrolled is responsible for ensuring that students are trained as part of orientation and annually. HIPAA Refresher training will be assigned periodically and will be communicated through email, The GReport, and other intercampus communications.

Q. DOES GRU/GR HEALTH SYSTEM HAVE AN ANONYMOUS HOTLINE?

Yes. You may report illegal, unethical and noncompliant behavior to the Compliance Hotline at 1-800-576-6623. The hotline is available 24 hours a day, seven days a week for workforce, students and other members of the enterprise community, including patients and visitors. Callers may remain anonymous.

Q. IF I HAVE MORE QUESTIONS ABOUT PRIVACY OR SECURITY RULES, WHO SHOULD I CONTACT?

- Christine Adams, Enterprise Privacy Officer, Compliance and Enterprise Risk Management Office, FY-103, 706-721-5631 or chradams@gru.edu
- Walt Ray, Interim Information Security Officer and Director for Client Services, located in library room AB-153, 706-721-1577 or wray@gru.edu
- Privacy and Security Policies: https://gru.policytech.com/
- The Office of Civil Rights of the Department of Health and Human Services offers excellent guidance on the HIPAA Rules. http://www.hhs.gov/ocr/privacy/