



## HIPAA Frequently Asked Questions

### 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) There are a number of misspellings throughout MCG's intranet, as well as the internet. MCG's intranet errors are currently being addressed. As for the internet, well...

### 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 Georgia law is more stringent than HIPAA Rules, Georgia law applies.

### Q. WHAT DOES HIPAA'S PRIVACY RULE DO?

The Privacy Rule sets standards to protect health care information. Specifically, it regulates health care information that can be linked with a person.

Health care information is any data relating to a person's past, present or future health, or the payment for health care. Health care information linked with personal identifying information is called Protected Health Information (PHI).

### Q. WHAT IS PERSONAL IDENTIFYING INFORMATION?

Name, address, birth date, social security number and medical record number are personal identifiers. So are phone numbers, fax numbers, e-mail addresses, and health plan beneficiary numbers. Think of PHI as puzzle pieces. Whenever enough pieces of the puzzle are linked together so that a patient may be identified – those personal identifiers are considered PHI.

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

No. Removing all personal identifiers from PHI makes it "de-identified". De-identified health data is not governed by HIPAA.

### Q. DOES IT MATTER WHAT FORM PHI IS IN?

No. The Privacy Rule applies to PHI in any form. This includes computer and paper files, x-rays, physician appointment schedules, medical bills, dictated notes, conversations and more.

### Q. WHAT DOES THE PRIVACY RULE DEMAND?

The Privacy Rule limits **use and disclosure** of PHI to the "minimum necessary." It also demands that "reasonable" safeguards be taken to prevent improper use or disclosure of PHI. The Rule imposes civil and criminal sanctions for non-compliance.

## **Q. WHAT IS "USE"?**

"Use" is sharing PHI with others to perform treatment, payment or health care operations (TPO). Use should be kept to the "minimum necessary." However, broad use is granted for treatment purposes. PHI may also be used for certain "public purposes" (e.g. law enforcement, public health, or courts).

Patients can authorize the use of their PHI for research. Alternatively, MCG's Human Assurance Committee (HAC), also known as an Institutional Review Board (IRB), may waive patient authorization for access PHI for certain research activities. Patients can authorize use of their PHI for marketing, fundraising or other specific purposes.

## **Q. WHAT IS "DISCLOSURE"?**

"Disclosure" means giving PHI to others for reasons other than TPO. Disclosures also must be kept to the minimum necessary. HIPAA gives patients the right to know who received a copy of their PHI. Unlike "uses", HIPAA mandates an accounting for all disclosures.

## **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 MCG's HIPAA privacy officer, Christine Adams at (706) 721-2661 or [chradams@mcg.edu](mailto:chradams@mcg.edu).

## **Q. WHAT DOES HIPAA PROHIBIT?**

Use or disclosure of PHI is prohibited unless it is authorized by the patient, permitted by law or granted through an HAC waiver. HIPAA prohibits leaving PHI in public view. Discarding unneeded medical records in the trash (as opposed to shredding them) is a HIPAA violation. Unless you are the provider on record, accessing your own record or family members' medical records is considered a privacy violation. Verifying your family's appointments through the IDX system is also considered unauthorized, unless verifying appointments is related to your job.

Some uses and disclosures cannot reasonably be prevented. Conversations that might be overheard or PHI accidentally seen are examples. The key is to make reasonable efforts to limit incidental uses and disclosures.

## **Q. WHAT DOES THE SECURITY RULE DEMAND?**

The HIPAA Security Rule sets safeguards for data systems and networks that store, process or transmits PHI. The Rule follows the best security practices used in industry and government.

Administrative safeguards include auditing computers for signs of misuse, reminding employees to follow security rules, and having a disaster recovery plan. Physical precautions include posting security 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.

Each member of our workforce is responsible for following best practices in applying safeguards to electronic information.

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

- Pick complex or hard-to-guess passwords
- Use passwords on PDAs and other portable devices

- Do NOT share computer log-in accounts or passwords, not even with your supervisor
- Use a screen saver that automatically locks or logs off after a period of inactivity

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

Yes. Regardless of location, you must protect the security and privacy of PHI. When working from home, for example, use the same security precautions (anti-virus, software updates, password-protected screen saver, VPN, etc.) on your home computer as on your office computer. Do not let household members access PHI.

#### **Q. DO I HAVE A RESPONSIBILITY TO REPORT SUSPECTED SECURITY BREACHES?**

Yes. Report suspected security breaches to MCG's security officer, Mark Staples, at 706 721-1577 or [mstaples@mcg.edu](mailto:mstaples@mcg.edu). A security incident is when the Confidentiality, Integrity and Availability of the information has been inappropriately changed, abused, or compromised.

Examples of security breaches include:

- Unauthorized access or use of electronic protected health information
- Unauthorized access to sensitive or confidential electronic information
- Sharing passwords or log-in information to MCG accounts
- Someone attempting to access MCG information without authorization
- Sending confidential data insecurely through email, FTP, or Web
- Loss or theft of electronic sensitive or confidential information
- Accessing an account not assigned to the person.

#### **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
- An accounting for some disclosures
- Ask 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. WHO DOES HIPAA AFFECT?**

HIPAA affects everyone in the MCG Health System. HIPAA Privacy and Security rules clearly apply to MCG's clinical operations.

Medical researchers often rely on PHI. HIPAA insists that researchers get patient authorization and HAC approval before using or disclosing PHI. PHI is also used and disclosed when teaching medical and other health professions students.

Business associates are outside individuals or firms that provide services for MCG and may work with or have access to PHI. Business associates are also affected by HIPAA, even though they are not part of the MCG's workforce.

## **Q. HOW IS HIPAA IMPLEMENTED AMONG OUR HEALTH SYSTEM – THE MEDICAL COLLEGE OF GEORGIA, MCG HEALTH, INC., AND PHYSICIAN PRACTICE GROUP?**

Under the guidance of the HIPAA rule, the Medical College of Georgia, MCG Health, Inc., and Physician Practice Group formed an Organized Health Care Agreement (OHCA). An OHCA allows PHI to be shared between entities which are clinically integrated. Each entity is responsible for complying with HIPAA. Privacy and Security Officers oversee compliance and training for each entity.

## **Q. WHAT MCG ENTITIES ARE INCLUDED IN OUR HEALTH SYSTEM'S OHCA?**

The Medical College of Georgia's OHCA includes the School of Medicine, the School of Nursing, the School of Allied Health Sciences, and Graduate Studies.

## **Q. CAN MCG'S SCHOOL OF DENTISTRY, STUDENT HEALTH SERVICES, GEORGIA WAR VETERANS NURSING HOME, and GEORGIA CORRECTIONAL HEALTH CARE SHARE INFORMATION?**

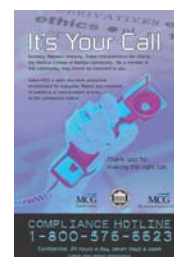
These entities must also comply with the HIPAA rule; however, they are not included in the MCG Health System's OHCA, as they do not share a clinically integrated record or a common "Notice of Privacy Practices." Only members of the MCG Health System OHCA may share PHI.

## **Q. HOW AND WHEN DO I RECEIVE HIPAA TRAINING?**

MCG will train all members of its workforce including employees, faculty and students, regarding the proper use and disclosure of patients' health information. Training will be appropriate for the level of staff and their 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. The schools in which a student is enrolled are responsible for ensuring that their students have been trained as part of orientation. New HIPAA training will be assigned periodically and will be communicated through email, beeper and other intercampus communications.

## **Q. DOES MCG HAVE AN ANONYMOUS HOTLINE?**

Yes. You may report illegal, unethical and noncompliant behavior to MCG's Compliance Hotline at 1-800-576-6623. The hotline is available 24 hours a day, seven days a week for employees, students and other workforce members of MCG, MCGHI, PPG as well as other members of the MCG 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, Compliance and Privacy Coordinator, HIPAA Privacy Officer, Office of Institutional Audit and Compliance, HS -3135, 706-721-5631 or [chradams@mcg.edu](mailto:chradams@mcg.edu).
- Walter Ray, Director of Security Information, ITSS Security Administration, HS- 2125, 706-721-1577 or [wray@mcg.edu](mailto:wray@mcg.edu).
- MCG "Privacy of Health Information" Policy: <http://www.mcg.edu/policies/9002.html>
- MCG Security Policies: <http://www.mcg.edu/itss/sa/>
- MCGHI Privacy Policies (6.01-6.30): <http://hi.mcg.edu/aboutus/policies.htm>
- 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/hipaa/>