

# AAMC's HIPAA Frequently Asked Questions – #1

## **The Impact of the HIPAA Privacy Rule\* on Medical Students and Residents — Frequently Asked Questions\*\***

The HIPAA Privacy Rule has raised a number of issues concerning its impact on the training of residents and medical students. This document represents the AAMC's understanding of answers to the questions that have been frequently brought to our attention. Ensuring that the Privacy Rule does not become an impediment to education requires institutional policies and training directed at residents and students. It also requires that all entities that train individuals have a common understanding of the Rule's requirements. It is hoped that this document will help achieve these goals.

## **Q 1 How Does the HIPAA Privacy Rule Affect the Training of Medical Students and Residents?**

### **A. TRAINING RESIDENTS AND STUDENTS (MEDICAL STUDENTS AND OTHERS) AS PART OF HEALTH CARE OPERATIONS**

The training of residents, medical students, nursing students, and other medical trainees is part of "health care operations" under the Privacy Rule. Activities that fall under the categories of treatment, payment, or health care operations (TPO) require the patient to sign an acknowledgment of privacy practices (see b. for more information). This is the only document the patient has to sign for any TPO activity under the Privacy Rule.

The Privacy Rule defines health care operations as "any of the following activities of the covered entity to the extent that the activities are related to covered functions: ... (2) ... conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers." [45 CFR 164.501]

### **B. NOTICE OF PRIVACY PRACTICES**

Patients must receive a Notice of Privacy Practices (NoPP) [45 CFR 164.520], and either sign a consent or an acknowledgement of the covered entity's privacy practices. The NoPP should inform patients that training of medical students and residents is part of the institution's health care operations.

### **C. INSTITUTIONAL PRIVACY POLICIES AND ACCESS TO PATIENT INFORMATION**

The HIPAA Privacy Rule does not prohibit medical trainees from gaining access to patients' information. However, the information is subject to the "minimum necessary

\* A complete copy of the Privacy Rule, guidance and other information is available on the Web at [www.hhs.gov/ocr/hipaa](http://www.hhs.gov/ocr/hipaa).

\*\* This paper represents the views of the AAMC and is not intended as legal advice.

standard,” so that each covered entity that trains residents, medical students and others, should develop policies that address how much information (up to the entire medical record) should be made available to trainees. (OCR Guidance, December 3, 2002, p. 25).

#### D. TRAINING IN HIPAA PROCEDURES: GENERAL


HIPAA requires that a covered entity provide training to all members of its workforce about the institution’s “privacy policies and procedures with respect to protected health information...as necessary and appropriate for the members of the workforce to carry out their function within the covered entity.” [45 CFR 164.530(b)(1)] The Rule does not specify the method of training, but requires the covered entity to document that training has been provided. [45 CFR 164.503(b)(2)(ii)].

The Privacy Rule defines “workforce” as “employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.” [45 CFR 160.103] “Trainees” includes residents, medical and other health professions students.

## Q2

### Medical Students And Residents Rotate Among Various Sites. Do They Need To Undergo HIPAA Training At Each Site?

There is no provision in the current HIPAA Privacy Rule, or in guidance that HHS has issued on the Rule, that would allow one site to meet the obligation to train members of its workforce about the institution’s privacy practices and procedures by accepting training that was provided elsewhere. This means that a rotation site could require that a medical student or resident undergo the HIPAA training that it specifies, even though the student may have received HIPAA training elsewhere.

 **Suggested strategy:** Small sites should be reminded that they can meet their HIPAA training obligations by providing much less training than would be needed at larger sites (see, OCR Questions and answers at [www.hhs.gov/ocr/hipaa](http://www.hhs.gov/ocr/hipaa), Answer ID 189, April 30, 2003). OCR has suggested that policies and procedures will vary among providers, depending on the volume of health information maintained and the number of interactions with those within and outside of the health care system. Therefore, the training requirement at a small physician’s practice (and likely at a small rural clinic) may be satisfied by providing each new member of the workforce with a copy of its privacy policies and documenting that new members have reviewed them. A large provider might need to provide training through live instruction, video presentations, or interactive software programs.

If you have web-based HIPAA Privacy Rule training, offer it to sites (particularly smaller sites) to which students and residents rotate. The sites can use it to train their own workforce. Once a rotation site uses your HIPAA training program or materials, it may be willing to accept the HIPAA training that you provide to medical students and residents and not require additional training for those individuals.

Affiliation agreements between sponsors and sites should address the responsibilities of each entity if a resident or student is accused of violating the HIPAA Privacy Rule, and if such accusation is found to be true.

Q3

**If residents and students rotate to various clinical sites, is a business associate relationship created between the sending institution and the rotation sites?**

**No.** A business associate relationship exists only “where the provision of the service involves the disclosure of individually identifiable health information from the covered entity.” [45 CFR 160.103] The rotation site is accepting your residents or students for training purposes, and is not your business associate. When residents or students rotate to a site for medical training, they become part of the workforce of the site to which they have rotated. Specifics about the medical training that occurs at the rotation site are not governed by the Privacy Rule.

Q4

**My institution, including all training sites, is organized as an Organized Health Care Arrangement. Residents and students rotate among sites within my OHCA. Does this affect any of the HIPAA requirements?**

**Yes.** If you are organized as an OHCA, then the training in HIPAA compliance and privacy procedures is only needed once, not at each rotation site.

Q5

**As part of the interview process for residency positions, fourth year medical students accompany our physicians and residents on rounds as observers. Does the HIPAA Privacy Rule prevent this practice from continuing or restrict what these observers may do?**

**No.** Fourth year medical students who follow physicians on rounds as part of the interview process can be considered part of the institution’s workforce and are engaged in an activity that falls under the institution’s health care operations. Other individuals who are on-site for a day or less (for example, a physician who comes to observe or teach a new surgical technique), also can be thought of as part of the workforce and should be treated in the same way.



**Suggested strategy:** All fourth year medical students who participate in rounds as part of the interview process for a residency position should be given a copy of your Notice of Privacy Practices, a very brief synopsis of the Privacy Rule, and be required to sign a confidentiality agreement by which they agree not to disclose any protected health information (PHI) to which they are exposed during rounds. Reasonable efforts should be made to limit the amount of PHI to which fourth year medical students and others who are on-site briefly are exposed.

Q6

**Residents and medical students often enter protected health information into their PDAs. Is this a violation of the HIPAA Privacy Rule?**

Allowing PHI to be entered into PDAs (such as Palm Pilots) which are easily portable and generally do not allow the information in them to be protected is a cause for concern. Every institution must develop policies to address the use of PHI in relation to PDAs, whether it be by physicians, residents, medical students, or any other staff.

*If you have further questions, please forward them to Ivy Baer ([ibaer@aamc.org](mailto:ibaer@aamc.org)) or Rina Hakimian ([rhakimian@aamc.org](mailto:rhakimian@aamc.org)).*

## Glossary of Relevant HIPAA Privacy Rule Terms:

- Business Associate [45 CFR 160.103]: performs activities on behalf of a covered entity that involves uses or disclosures of individually identifiable health information.
- Business Associate Agreement [45 CFR 164.504(e)(1)]: contract between the covered entity and the business associate that specifies the ways in which PHI that is provided to the business associate will be used and disclosed.
- Covered Entity [45 CFR 160.103]: a health plan, health care clearinghouse or health care provider who transmits any health information in electronic form in connection with a transaction covered by this Rule. The provisions of the Privacy Rule apply only to covered entities and business associates.
- HIPAA [42 USC 1301]: Health Insurance Portability and Accountability Act of 1996. The law that provides the Department of Health and Human Services with the authority to implement the Privacy Rule.
- “Minimum necessary” [45 CFR 164.502(b)]: standard that when using or disclosing PHI, or requesting it from another entity, a covered entity must make reasonable efforts to limit the PHI to the minimum necessary to accomplish the intended purpose.
- NoPP: Notice of Privacy Practices [45 CFR 164.520]: A document written in plain language that is given to every individual that provides notice of the uses and disclosure of protected health information that may be made by the covered entity, and of the individual’s rights and the covered entity’s legal duties with respect to protected health information.
- OCR: Office of Civil Rights, the HHS agency charged with primary responsibility for interpreting and enforcing the HIPAA Privacy Rule
- OHCA: Organized Health Care Arrangement [45 CFR 164.501]: a clinically integrated care setting in which individuals typically receive health care from more than one provider; an organized system of health care in which more than one covered entity participates, and in which the participating entities: (1) hold themselves out to the public as participating in a joint arrangement; and (2) participate in joint activities that include at least one of the following: utilization review, quality assessment and improvement activities, or payment activities.
- PHI: Protected Health Information [45 CFR 165.501]: individually identifiable health information that is transmitted by electronic media, or transmitted or maintained in any other form or medium.