

ACGME HIPAA FAQs – March 2005

Introduction

The compliance date for the HIPAA Security Regulations (45 CFR Part 160 and Part 164, Subparts A and C) is April 20, 2005. One of the requirements of these regulations is that, for the electronic transmission of protected health information (PHI), a business associate agreement (BAA) must provide that the business associate will -

- Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic PHI that it creates, receives, maintains, or transmits on behalf of the covered entity;
- Ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it;
- Report to the covered entity any security incident of which it becomes aware;
- Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract.

To comply with these requirements, it is necessary for ACGME to amend the BAAs that it has signed with sponsoring institutions, and in some cases (as discussed below) with clinical sites. The amended BAA retains the provisions of the original BAA, and includes new provisions to comply with the Security Regulations. The amended BAA with a covered entity will supercede any earlier BAA between ACGME and that covered entity.

The following FAQs are meant to provide further information about what ACGME will be doing to reach compliance by April 20, 2005, and what sponsoring institutions and clinical sites may need to do. These questions expand upon earlier FAQs that were directed at the Privacy Regulations' requirements for BAAs.

1. What will ACGME do to ensure that its BAA complies with the Security Regulations?

It is ACGME's intention to amend its BAA in a manner that will cause as little disruption as possible to sponsoring institutions and clinical sites. By April 20, 2005, ACGME intends to enter into amended BAAs with sponsoring institutions that are covered entities. An amended BAA can be found on the ACGME website. This amended BAA may also be used between ACGME and a sponsoring institution's clinical sites.

Some clinical sites have entered into BAAs with the ACGME. Those sites may want to take this opportunity to evaluate whether they need to have a BAA with the ACGME, or whether a BAA with the sponsoring institution is sufficient. This is discussed in more detail in FAQ 2 below. Whatever the decision, a BAA with ACGME must comply with the HIPAA Security requirements by the April deadline.

The ACGME also will amend its current BAA with VHA and the Department of Defense to comply with the Security Regulations.

2. Is it true that it may be unnecessary for a clinical site to have a BAA with ACGME?

Yes. Many sponsoring institutions that are covered entities maintain a single BAA with ACGME, and their clinical sites do not have separate BAAs with ACGME. For these institutions, clinical sites disclose PHI to ACGME as a business associate of the sponsoring institution (per the BAA between ACGME and the sponsoring institution). See 45 CFR §160.103 (definition of business associate).

HHS maintains a set of FAQs on its website addressing issues under the Privacy and Security Regulations. Here is one such FAQ relevant to this topic:

Question: May a covered entity share protected health information directly with another covered entity's business associate?

Answer: Yes. If the HIPAA Privacy Rule permits a covered entity to share protected health information with another covered entity, the covered entity is permitted to make the disclosure directly to a business associate acting on behalf of that other covered entity.

United States Department of Health and Human Services Office for Civil Rights' Frequently Asked Questions, Answer ID 241, available at www.hhs.gov/ocr/hipaa.

3. Is enough PHI submitted to ACGME electronically to require ACGME to amend its BAA?

Yes. If a covered entity transmits any PHI to ACGME electronically, the Security Regulations are implicated, and the ACGME BAA must be amended.

The Security Regulations do not apply to PHI transmitted orally or by paper, FAX or voicemail. They do apply to PHI transmitted by email, although very little PHI is transmitted to ACGME by email. They also apply to PHI transmitted through the ACGME website to the Resident Case Log System ("System"). Most of the information transmitted to the System is not PHI, but there is some. As of July 1, 2005, 591 of the 698 ACGME sponsoring institutions will sponsor at least one program which either is required to submit case data to the System, or will have the System available. In the next several years, ACGME expects that programs in additional specialties will be required to submit case data to the System.

4. What documents should my sponsoring institution send to ACGME? What documents should my sponsoring institution maintain?

Sponsoring institutions that are HIPAA-covered entities should send to ACGME an executed amended sponsoring institution/ACGME BAA. Each covered entity sponsoring institution should maintain a copy of (1) its executed amended sponsoring institution/ACGME BAA; (2) its signed Representation (it need not execute a new one); and (3) each ACGME/clinical site BAA.

5. My sponsoring institution is a covered entity, but it does not think that it and/or its clinical sites give PHI to ACGME. Therefore, it does not believe that a BAA with ACGME is necessary. How should my organization proceed?

It is up to the covered entity to determine whether the information provided to ACGME is PHI. ACGME encounters PHI orally and in documents in various contexts in the performance of its accreditation function: (1) during site visits following submission of accreditation applications and reapplications; (2) during site visits to investigate issues raised by complaints about residency programs; (3) in the Resident Case Log System; (4) in complaints relating to residency programs (sometimes); (5) in applications and reapplications for accreditation (rarely); and (6) in information sent by programs to ACGME between applications and reapplications (rarely).

If the lack of a BAA from a sponsoring institution or clinical site impedes ACGME in its ability to perform its accreditation function, relating to a site visit or otherwise, the RRC or IRC, as appropriate, will consider the extent and nature of the impediment, and will determine the course of action to take, up to and including adverse accreditation action, just as it would if there were an impediment for reasons unrelated to HIPAA compliance.

6. Once April 20, 2005 is past, does the sponsoring institution need to maintain an ACGME/clinical site BAA with each new clinical site?

It is the duty of the sponsoring institution to ensure that information required by ACGME in the performance of its accreditation activities is made available to ACGME. The need for a BAA is determined by the "covered entity" as defined by HIPAA regulations. 45 CFR §160.103. Under the definition in the HIPAA Privacy Regulations, most clinical sites are "covered entities." It is up to the sponsoring institution to work with clinical sites to determine which clinical sites require a BAA with ACGME in order for ACGME to access clinical site PHI as part of its accreditation function. If the sponsoring institution and the clinical site(s) determine that the information can be provided to ACGME without the use of an ACGME/clinical site BAA, then ACGME does not require that one be maintained. See FAQ 2, above.

7. In its role as a sponsoring institution or clinical site, my organization is not a "covered entity" under the HIPAA regulations. Does my organization need to sign a BAA with ACGME?

No. A sponsoring institution or clinical site may determine that, in such role, it is not a covered entity under HIPAA regulations. Examples may include coroners, medical examiners, clinical sites outside the United States, and others.

8. Will ACGME need access to ACGME/sponsoring institution and ACGME/clinical site BAAs during every site visit for every program?

No. ACGME will ask to verify the maintenance of these documents during institutional site visits. They will only be needed during program site visits if requested information is not provided and HIPAA is the reason given for not providing it.

9. What will happen if, because of HIPAA, ACGME is refused access to information that it deems necessary to perform its accreditation function during a site visit or otherwise?

ACGME has always required sponsoring institutions to ensure that ACGME has accreditation access to program related information in the control of the sponsoring institution and clinical sites, subject to the confidentiality and other provisions of ACGME policies and procedures. The HIPAA Privacy and Security Regulations introduce new requirements, the satisfaction of which may be necessary to accomplish this.

If this ability to access information needed to appropriately perform the accreditation function is impeded for any reason during a site visit or otherwise, the RRC or IRC, as appropriate, will consider the extent and nature of the impediment, and will determine the course of action to take, up to and including adverse accreditation action, just as it would if there were an impediment for reasons unrelated to HIPAA compliance.

10. Must each sponsoring institution sign the Representation?

Yes, but it does not need to sign a new Representation.

11. Must the DIO sign the amended BAA?

It is up to the "covered entity" to determine who is authorized to bind the covered entity to the BAA. Some sponsoring institutions require the CEO, some the DIO, the HIPAA Privacy Officer, or others. ACGME does not mandate who the signatory must be.

12. Must a covered entity use the ACGME amended BAA or can it send the ACGME its own?

The BAA is between the "covered entity" and ACGME. As ACGME maintains a large number of BAAs, and the language and form of its amended BAA have been accepted and recognized as sufficient for HIPAA-compliance by the VHA (through the facilities of which tens of thousands of resident physicians circulate annually), the United States

Department of Defense, and others, ACGME requests that the "covered entity" use ACGME's amended BAA.

13. Can the sponsoring institution or the clinical site modify the ACGME amended BAA?

The language of the ACGME amended BAA has been accepted and recognized as sufficient for HIPAA-compliance by the VHA, the United States Department of Defense, and others, and ACGME requests that it not be modified.

14. Can the sponsoring institution use the ACGME amended BAA for its BAA with its clinical sites, so it has one BAA for both purposes?

No. However, the sponsoring institution may use the ACGME amended BAA as a model to create its own BAA for its own purposes, as it may deem appropriate.

15. I have more questions. Whom should I contact?

Please email questions to hipaa@acgme.org. Responses will be sent as soon as possible.