CAP Ten HIPAA Compliance Questions

Responding to concerns about the threat to confidentiality of patient information posed by the development of health information systems, Congress enacted the privacy provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Final regulations implementing these provisions were issued on August 23, 2002. This list of questions attempts to address ten of the most commonly asked questions about the effect of the HIPAA privacy regulations on pathology practices and laboratories ("pathologists").

1. Do HIPAA Requirements Apply To Pathologists?

Pathologists must comply with HIPAA standards if they (or their billing company or any other third party acting on their behalf) transmit patient identifiable "protected health information' ("PHI") electronically. If any PHI is transmitted electronically, the HIPAA privacy requirements apply to all PHI in the possession of the pathologist – including PHI that is not transmitted electronically. PHI has a very lengthy definition. In essence, however, it is any information created or received by a physician or other health care provider which identifies an individual in any way and which relates to the individual's health or to payment for the individual's care.

2. When Do Pathologists Have To Comply?

There are two major HIPAA deadlines with which pathologists must comply. The first is the Transaction and Code Sets Standards, originally dated Oct. 16, 2002. Recently, however, the HHS issued a guidance document authorizing a contingency plan for compliance to these standards. A CAP STATLINE article published October 16, 2003 explains this HIPAA compliance contingency plan. Pathologists will have to ensure that all electronic billing and claims filings are formatted in accordance with HIPAA requirements.

The second important deadline is the Privacy Rule compliance date of April 14, 2003. By that date, pathologists must have appropriate policies in place, must obtain authorization for disclosure of PHI where necessary, and (with certain limited exceptions) must otherwise be in full compliance with all HIPAA requirements. In addition, HIPAA has a number of components and a number of separate deadlines.

A summary of the HIPAA components and deadlines for compliance can be found at http://www.hipaadvisory.com/regs/compliancecal.htm.

3. Does My Group Have To Designate A Privacy Official?

Each pathology group and laboratory must designate a privacy official. This person is responsible for the development and implementation of HIPAA privacy rule policies and procedures. Moreover, this person must make sure that the group or laboratory is in compliance with all applicable requirements. In large laboratories, the privacy official position could take up much of the person's time. In smaller practices, the privacy official may be a person with many other tasks, e.g., the office manager.

4. Is Any Training in HIPAA Issues Required?

All pathologists and employees must be trained on applicable policies and procedures with respect to PHI. Each new employee of the group or laboratory must be trained within a reasonable period after being hired. There must be documentation that the training has been provided.

5. What Sort Of Policies and Procedures Must Be Implemented?

A pathologist must develop and implement policies and procedures to govern how the laboratory and its employees and other agents use and disclose PHI. The general rule is that a pathologist may not use or disclose PHI except as specifically permitted or required in the HIPAA privacy regulations. You may use the Administrative Checklist to ensure you meet all requirements.

6. Do Pathologists Have To Require HIPAA Compliance By Other Entities?

The HIPAA privacy regulations require covered entities to enter into written agreements with so-called "Business Associates." These are persons or entities that have access to PHI as a result of providing service to or for a covered entity. Business Associate agreements are intended to ensure that a Business Associate will provide the same privacy protections to PHI as the covered entity would.

For example, a pathologist's billing service will be a Business Associate of the pathologist. Similarly, attorneys, accountants or consultants who provide services to a pathologist may be Business Associates of the pathologist if such individuals have access to PHI. The College may be a Business Associate of a laboratory if it has access to PHI in the process of inspecting that laboratory.

In certain circumstances, a pathologist or laboratory may be the Business Associate of another Covered Entity. For example, when a pathologist directs a hospital laboratory, the pathologist is also providing services to the hospital and will have access to information about the hospital's patients. In these circumstances, the pathologist likely will be a Business Associate of the hospital.

In general, required Business Associate agreements must be in place by April 14, 2003. However, if the pathologist already has a contract with an entity to which the Business Associate requirements apply, a Business Associate agreement need not be obtained until the current contract renews or April 14, 2004 – whichever occurs first. Therefore, each pathologist must determine which of the individuals or entities providing services to the pathologist will need to sign a Business Associate agreement. In addition, the pathologist should identify which hospitals, laboratories or other covered entities for which the pathologist or laboratory provides services will ask the pathologist or laboratory to sign such a contract.

A sample business associate agreement can be found at http://www.hhs.gov/ocr/hipaa/contractprov.html. A detailed memo on this topic is available from the College, as well – Business Associate Requirements.

7. What Safeguards for PHI Should A Pathologist Consider?

The HIPAA privacy regulations require covered entities to establish certain "administrative," "technical," and "physical" safeguards to protect the privacy of PHI they maintain. Administrative safeguards may include the performance of periodic audits to analyze the effectiveness of privacy protections that are in place. Technical safeguards may include the use of password protection on computer systems so that those who do not need access to test results and other private information will not be able to access that information. Physical safeguards may include the backing up of computer systems or the preparation of a disaster emergency plan in order to protect the integrity of patient information.

8. How Does HIPAA Relate To CLIA?

HIPAA allows for the communication of test results to the patient as allowed by CLIA. CLIA permits labs to provide test results only to "authorized persons" as defined primarily by state law. In most cases, this will be the ordering physician, not the patient. If state law allows for test results to be communicated directly to the patient, the pathologist will be a direct treatment provider for that patient and must try to

obtain an acknowledgement that the patient has received the pathologist's notice of privacy practices. Of course, the pathologist must safeguard the confidentiality of any PHI.

9. What Compliance Resources Are Available?

In addition to the tools and resources available from the College, there are a number of valuable sources of information on the Internet. The Web Site Links page of this resource lists some of the most commonly used sites.