

*Frequently Asked Questions on*

*HIPAA and Clinical Trials*

The following questions were answered by Lawrence H. "Doc" Muhlbaier in his book *HIPAA in Clinical Trials, A Practical Guide for Research Compliance*. To purchase a copy of the book or any of HCPro's other HIPAA products call 800/650-6787 or go to [www.hcmarketplace.com](http://www.hcmarketplace.com).



# FREQUENTLY ASKED QUESTIONS ON HIPAA AND CLINICAL TRIALS

## **1. What is HIPAA? What are the various parts of HIPAA?**

HIPAA is the Health Insurance Portability and Accountability Act of 1996, also known as the Kassebaum-Kennedy Act. HIPAA is divided into three portions: portability, accountability, and administrative simplification. Two of the most important parts for researchers — privacy and security — fall under the rubric of “administrative simplification.” The privacy and security regulations govern the way medical and research professionals handle PHI. HIPAA evolved because health care providers were asking for a unified billing format. Providers received what they asked for and much more. Although the privacy and security portions of the bill weren’t immediately viewed as serious, they became the buzz of the health care industry and everyone will find out just how serious the regulations are beginning on April 14, 2003, when they’re required to comply with the privacy portion.

## **2. Who is required to comply with HIPAA? What is a “covered entity”? How can I tell whether I’m a covered entity?**

There are three types of organizations that are required to comply with HIPAA: Health care providers who engage in electronic billing, health care clearinghouses, and health care (insurance) plans. April 14, 2003, is the date by which all of these entities, except for small health plans, must be in compliance with the majority of the regulations under HIPAA. Note that the group that is the exception to the rule includes small health plans, rather than providers. Small health plans are by no means exempt from HIPAA. They must comply with the rules by April 14, 2004.

## **FREQUENTLY ASKED QUESTIONS ON HIPAA AND CLINICAL TRIALS**

Once a health care entity is considered a covered entity, then any individually identifiable health care information is considered protected. That means that pieces of health care information that are not used for billing purposes are still protected, including PHI for individuals for whom the covered entity has not submitted bills. Similarly, individually identifiable health information is protected even if the covered entity does not have a treatment relationship with the individual (i.e., a research study on healthy individuals in which blood test results are included). Don't be fooled into thinking that because you do not submit bills by computer you will be exempt. If you have health practitioners on staff and/or treat patients or conduct human research you are almost certainly a "covered entity." Besides, the HIPAA standards for privacy and security will quickly become the community standard for care and research. Please check with legal counsel who understand HIPAA to see if you are one of the very few entities not covered by HIPAA.

### **3. What is the difference between consent and authorization? How is a HIPAA authorization different from those authorizations now in use?**

Under HIPAA, consents are used solely for treatment and are optional. If a covered entity chooses to use a consent, a notice of privacy practices does not have to be provided. An authorization is an individual's approval for the covered entity to use his or her PHI for a particular purpose during a particular time period. The authorization is for uses other than treatment, payment, or operations.

The HIPAA authorization for research is very similar in intent to a research consent and therefore is allowed to be combined with a research consent. The benefit of this is that one document then satisfies HIPAA, the Common Rule, and FDA requirements.

### **4. What is assent?**

Assent used in HIPAA is different from assent used under the Common Rule. Though both refer to minors who are not emancipated, under HIPAA the parent assents to the minor receiving PHI confidentially (e.g. without the parent being able to see the PHI) from the health care provider. This is different than the definition under the Common Rule, in which the minor agrees ("assents") to the study.

Assent is applied to research under the Common Rule or under the FDA regulations in addressing consent or authorization by minors. In general it means that the consent or authorization would be signed by one or more parents, but assent would be sought of the minor child. This is typically done for children between the ages of 7 and 12 years.

### **5. What is a notice of privacy practices?**

A notice of privacy practices is a document drafted by a covered entity that can mean the difference between conducting research and not conducting research. The document must spell out all the activities in which a covered entity is allowed to participate. A notice of privacy practices must be provided by a covered entity to all of its patients, research participants, or customers. In addition to making a good-faith effort to provide patients with a copy of the notice, employees must also document that effort. However, a notice does not have to be presented in order to conduct the study as long as there is an assurance that one exists and it covers the project about to be conducted. The notice can be presented after the treatment has begun, unlike a research consent, which has to be obtained before a study can begin.

### **6. What is the minimum necessary rule and what are its requirements?**

The “minimum necessary” is the rule within HIPAA that says health care workers and research personnel should rely on the smallest possible amount of individually identifiable health information in order to carry out their duties. Minimum necessary is required of all HIPAA-regulated activities, except for provider activities related to the direct treatment of patients or for de-identified information.

HIPAA does not give any guidance on what “minimum necessary” means for particular activities, but instead relies on covered entities to make that ruling for themselves. There are some examples of minimum necessary in the preamble to the regulation.

Minimum necessary is an example of how HIPAA is largely a compliance activity rather than a technology activity. For example, billing professionals may not be able to see all the details of a patient’s treatment and nursing staff may not be able to see the specifics of a patient’s bill; these would be considered good practices with or without HIPAA.

### **7. Do research participants have any right to see research records or results? How about clinical patients who are also research subjects?**

Research subjects have no more or less rights than clinical care patients to see records. In particular, they might not see research-specific documents depending on the study. Under HIPAA a patient is allowed to see information in the “designated record set.” Information in a research record typically is often a duplication of a designated record set and therefore would be accessible in most cases. They typically would not see the randomization of a treatment in a blinded study, as that would compromise the integrity of the study and is also not part of the designated record set. Commercial sponsors of research would be quite alarmed if patients/subjects could look at proprietary information, thus the limits on the “right to see”.

## **FREQUENTLY ASKED QUESTIONS ON HIPAA AND CLINICAL TRIALS**

For example, study-related laboratory tests are frequently not recognized by the hospital because they are conducted by an outside lab. Because they are not recognized, they don't usually make it into the designated record set and therefore covered entities are not required to allow patients to see this information.

### **8. If a trial sponsor asks a physician to recruit his or her patients for the study, does he or she need to obtain patient authorization before releasing their names to the sponsor?**

Yes and no. If the patients who are recruited for the study sign an authorization, that authorization must state that their names will be given to the sponsor. However, the IRB or Privacy Board is expected to only allow reasonable information to be given to the sponsor. Often an IRB will consider the name unreasonable and unnecessary. In the situation of pre-screening or case-finding in which written authorization is not obtained, the name would likely not be available to the sponsor as minimum necessary explicitly applies.

### **9. What is protected health information (PHI)?**

PHI is individually identifiable health information in the possession of a covered entity that has ever been in any form—paper or electronic; it may or may not have been used in an electronic transaction. It merely has to have been in electronic form at some point. Exceptions to PHI include education records covered by the Family Education Rights and Privacy Act, or employment records held by the covered entity in its role as employer.

### **10. To what extent will the privacy rule provision of HIPAA chill or hinder research by making researchers apprehensive about releasing PHI for fear of ramifications?**

The privacy rule explicitly allows methods of sharing research information between covered entities or between a covered entity and other persons. For instance, under a waiver of authorization, the sharing could be authorized by the IRB. Under a limited data set or a de-identified data set, the data could be shared with more or less restriction on what people can do with it. However, the full-extent of any chill is not yet known. Stay tuned!

### **11. Why would a covered entity use a Privacy Board?**

A Privacy Board must be used by a covered entity that does not have or is not eligible for an IRB. In order to be eligible for an IRB, a covered entity must conduct research that is funded by the NIH or participate in research that must be reported to the FDA. A Privacy Board is constituted similarly to an IRB, but has a more limited scope.

Covered entities that are eligible for an IRB can either use their IRB or a Privacy Board to address the waiver and alteration issues allowed under HIPAA. Reasons to include a Privacy Board are often business- or operations-related within the covered entity, such as the IRB not having enough staff to meet the additional privacy responsibility. Another reason would be that an IRB could determine that additional privacy issues could be picked up by the covered entity's compliance office. A company that uses an external IRB may wish to institute a Privacy Board to simplify its waiver activities.

### **12. Is genetic information covered under HIPAA?**

Human tissue and bodily fluids are not covered under HIPAA. However, information about them is covered by HIPAA. So a tube of blood is not covered by HIPAA, but the label on the tube of blood is. DNA information about that blood, when linked to the label, is also covered by HIPAA.

### **13. We don't send any information by electronic means. What parts of HIPAA do we have to comply with, if any?**

If a covered entity does not send information by electronic means, it is not covered by HIPAA. If a covered entity does not do any electronic billing, it is not covered by HIPAA. However, once covered by HIPAA, then PHI is any information that has ever existed about an individual's health, whether or not it was sent. Once an entity is covered, then everything is covered. People have tried to say that some individuals' information is not covered because they did not send an electronic bill for a particular person, but it does not work that way. Again, check with HIPAA-aware legal counsel. Don't assume you are not covered.

### **14. Is patient or subject authorization required for health care providers to use patient records for retrospective studies? Can outside researchers have access?**

Not generally. If the data are on the shelf, as one would expect with most retrospective studies, then the IRB or Privacy Board could waive the authorization. This can be done whether or not the researcher is inside or outside of the covered entity. Waivers apply to both uses and disclosures.

### **15. Do I have to account for all disclosures or are there any exceptions?**

A covered entity only has to account for disclosures that are done for reasons other than TPO and are done without written authorization. In the research setting, this typically means that a covered entity has to account for disclosure under reviews preparatory to research, waiver or alteration, or research on decedent PHI.

## **FREQUENTLY ASKED QUESTIONS ON HIPAA AND CLINICAL TRIALS**

One addition that may affect researchers is that reporting of adverse events to a drug or device manufacturer is a disclosure that has to be tracked for accounting, if the researcher did not state that disclosure in the authorization.

### **16. How much access does a research subject have to his or her records?**

Research subjects have no access to their research records, as such. However, as individuals have received treatment from the health care provider, they have access to whatever information is included in the designated record set. This designated record set may include some research information, or it may not. This is determined by whether the research information is actually used to make treatment decisions about the individual.

An example of research information that would not be in the designated record set is a laboratory test obtained only for the research project and not reported to the individual's health care provider. Similarly, an x-ray done at the health care facility and included in the medical record would be available to the individual, whether or not the research project paid for it, as it would be available to the health care provider to make decisions about the patient. Typically, the treatment randomization in a blinded clinical trial is not available to the individual.

### **17. Can a parent sign a HIPAA research authorization for a teenager?**

Generally, yes. Typically a parent could sign and would be required to sign a research authorization for a teenager. The teenager would also be asked to sign (that piece is generally a requirement under the Common Rule or FDA regulations). One caveat to this is that the age at which the parent's signature is no longer required depends on the age of the majority in the state in which the authorization is obtained. Some states have different laws that determine the age at which a person is no longer a minor. HIPAA makes no mention of ages and that is therefore left to the state law to determine who is an adult and who is a minor.

### **18. IRB documents do not involve any form of patient identifiers, but with new HIPAA regulations, I am wondering whether my IRB needs to revisit the issue. Are there any regulations regarding this issue?**

Documents sent to the IRB do not have patient identifiers. The informed consent or authorization clearly does, as it includes the patient's signature. However, the signed authorizations are not provided to the IRB. They are kept by the researcher or the medical records department depending on the circumstances of

the study and covered entity practice. Of note here is that an NIH-issued Certificate of Confidentiality can further modify who is allowed to see or keep a research consent or HIPAA authorization document.

### **19. What items need to be “de-identified” to get an IRB waiver?**

None. An IRB waiver can use any information about the patient, including identifiers, that is needed for the study. Waivers are subject to the minimum necessary requirements of HIPAA, so there needs to be a scientific requirement for including identifiers.

### **20. What is a HIPAA waiver and how do I get one?**

A HIPAA waiver allows one to forego obtaining authorization or to obtain a modified authorization. The waiver can only be used for research. Waivers are obtained through the IRB or the Privacy Board and are addressed more thoroughly in Chapter 5.

### **21. What are the penalties for violating the HIPAA regulations?**

Penalties range from \$100 for a single violation to 10 years in jail and \$250,000. For inadvertent violations, it should be noted that the HHS has stated it intends to work with entities to correct deficiencies rather than use penalties as the first source of corrective action.

### **22. I know that hospitals and health practitioners can share PHI necessary for TPO—treatment, payment and health care operations—is this also true for researchers?**

Generally, no. A researcher can share PHI if that sharing is allowed in the authorization signed by the patient, or is done under a waiver of authorization provided by the IRB or Privacy Board, or is necessary for the emergency care of the patient.

### **23. Can I have a research participant sign-in sheet?**

Yes. The HHS made it clear in the August 14, 2002, final privacy regulations that sign-in sheets are allowed and considered an incidental disclosure not subject to accounting or penalty. One should note that the sensitivity of some research activities may preclude the use of sign-in sheets.

### **24. How does HIPAA affect abuse reporting?**

Generally not at all. Abuse reporting is still mandated or required under most state laws and can be done. It is, however, subject to limited disclosure accounting. Abuse reporting is subject to state law and professional judgment. HIPAA requires that the individual who is the subject of the report be notified promptly, unless that would place the individual at risk of serious harm. If a researcher has questions about abuse in the context of the research rather than in the context of treatment, he or she should speak with the local IRB chair or compliance officer about how to address it.

### **25. Does a patient or subject's lawsuit against the researcher void the HIPAA privacy rule?**

No. The HIPAA privacy rule has specific requirements for what can be disclosed under a subpoena or a lawsuit. Further, if the patient's concern is about a privacy violation under HIPAA, there is no right of private action. He or she can complain to the OCR or to a local person as described in the notice of privacy practices. A notice of privacy practices must include the mention of a local authority to whom patients can make complaints.