BNA, INC.

MEDICAL RESEARCH LAW & POLICY

BNA Employee-Owned Since 1947

REPORT

Following is one in a series of analyses by experts in the health care field on the practical aspects of implementing various HIPAA requirements that apply to medical research.

HIPAA Compliance Steps for Commercial Research Sponsors

BY MARK BARNES, GREGORY J. GLOVER, AND CLINTON HERMES

The Health Insurance Portability and Accountability Act of 1996 and related privacy and security regulations (collectively, ''HIPAA'') directly apply only to ''covered entities,'' *i.e.*, health plans, health care clearinghouses, and certain health care providers. As a result, much of the attention given to HIPAA's effect on research has been focused on how hospitals, physician practices, and other covered entities will be allowed to use and disclose protected health information (''PHI'') for research purposes, and what covered entities should do to ready their research operations for HIPAA's compliance dates.[1,2] Research sponsors, such as pharmaceutical companies and medical device manufacturers, however, are not covered entities simply by virtue of sponsoring clinical research and therefore are not directly regulated by HIPAA as research sponsors.[3] Still, research sponsors cannot afford to ignore HIPAA, for various compelling legal reasons.

Virtually all of the research information needed by research sponsors is created by covered entities, which will be prohibited from disclosing that information to research sponsors without either a HIPAA-compliant authorization from each data subject specifically permitting the disclosure or an exception to that prohibition (*e.g.*, for a review preparatory to research, or pursuant to an Institutional Review Board or Privacy Board waiver of the authorization requirement). If a research site fails to comply with these requirements, research sponsors either will be denied access to critical data, or will receive data that have been disclosed to them wrongfully and without authority. If a sponsor is denied access to critical data, this could be catastrophic, particularly if the research site is responsible for a large percentage of the study's subjects or if the research

Mark Barnes is an attorney with the law firm of Ropes & Gray, New York, Gregory J. Glover is an attorney with the firm's Washington, D.C., office, and Clinton Hermes is an attorney with the firm's Boston office.

[1] *See, e.g.*, Mark Barnes and Clinton Hermes, *Clinical Research After the August 2002 Privacy Rule Amendments*, 1 BNA MED. RES. L. & POL. REP. 406 (9/18/02); Jennifer Kulynych, *Privacy Rule Creates New Compliance Obligations for Research Involving Human Subjects*, FDLI UPDATE (November/December 2002), at 8.

[2] The Standards for Privacy of Individually Identifiable Health Information (45 C.F.R. Parts 160 and 164) require compliance by April 14, 2003, for most covered entities. The Security Standards (45 C.F.R. Parts 160, 162, and 164) will be published as a final rule in the Feb. 20 *Federal Register*, with an effective date of April 21, 2003, and a compliance date, for most covered entities, of April 21, 2005.

[3] Research sponsors may be directly regulated by HIPAA in other ways, *e.g.*, by selling or dispensing a drug, device, equipment, or other item pursuant to a prescription and electronically billing for the sale, or by sponsoring an employee benefit plan that pays for health care.

 ISSN 1539-1035

sponsor is depending on the data generated in order to respond to Food and Drug Administration (''FDA'') requirements. On the other hand, if a sponsor receives data that have been disclosed by the investigators without HIPAA authority to do so, the consequences to the research sponsor currently are difficult to determine, but could range from a civil lawsuit against the research sponsor (if the sponsor attempts to use the data) to, in egregious cases, a refusal by FDA to accept the data to support an FDA application (such as a New Drug Application or a Premarket Approval Application).

Because HIPAA compliance therefore can be as important to the research sponsor as it is to the research sites that HIPAA directly regulates, research sponsors should begin preparing for HIPAA now, if they have not already done so. This article sets out nine steps that each research sponsor should consider taking in that endeavor.

Recommendations

1. *Representations and Warranties.* Sponsors should include in their clinical trial agreements with research sites various representations and warranties from the sites relating to the sites' HIPAA compliance in order to protect the research sponsors' access to study data. Specifically, research sites should represent and warrant that they will comply with HIPAA and any other state and federal laws relating to the confidentiality, privacy, and security of health information so that they can continue to provide sponsors with completed case report forms,[4] access to source data, and all other information required by the protocol. For interventional trials, sites also should represent and warrant that they will have appropriate HIPAA authorizations in place for each subject (which must list as recipients and users of the data the sponsor and the sponsor's contractors, including any contract research organization (''CRO'')), as well as any other consents required under state law. Further, sponsors may consider amending the clinical trial agreement to provide that the site will indemnify the sponsor for any loss resulting from the site's (and/or investigator's) negligent failure to comply with state or federal privacy laws, including HIPAA.

At the same time, sponsors should expect that sites and investigators will use HIPAA as an opportunity to amend clinical trials agreements. A typical amendment offered by a medical center will require the sponsor (and all the sponsor's agents and contractors) to use and disclose patients'/subjects' data only for purposes of the study and for interaction with regulatory authorities. Such amendments represent hospitals' attempts to safeguard subjects' information, are entirely appropriate, and should be agreed to by sponsors. Some hospitals may overreach, however, and may attempt to bind sponsors with ''business associate'' contracts, by which sponsors would voluntarily subject themselves to HIPAA requirements. Since sponsors are not typically ''business associates'' under HIPAA rules—sponsors do not perform activities for or on behalf of HIPAA-covered entities—sponsors should decline to sign any such business associate agreements.

2. *Notice of Privacy Practices.* HIPAA requires that covered research sites distribute a Notice of Privacy Practices (a ''Notice'') to patients (including study subjects) no later than the date of the first service delivery after April 14, 2003. The Notice must provide ''adequate notice of the uses and disclosures of protected health information that may be made by the covered entity,'' and covered entities are specifically prohibited from using or disclosing information in a manner inconsistent with the Notice.[5] If the Notice states that patient authorization will be obtained for all uses and disclosures except those specifically mentioned,[6] and fails to describe adequately any possible research uses and disclosures, the covered entity will be prohibited from disclosing PHI to the sponsor regardless of any representations to the contrary and regardless of any IRB or Privacy Board waiver or other HIPAA exception. An insufficient Notice therefore can cost the sponsor valuable data. Moreover, because the Notice is the most visible manifestation of a covered entity's HIPAA compliance, an insufficient Notice carries a relatively high degree of complaint and enforcement risk against the covered entity as well as a risk of possible civil liability.[7] As a result, it is in the sponsors' interest to ensure that the Notice distributed by research sites to their patients/subjects describes possible research uses and disclosures of PHI (*e.g.*, that PHI may be disclosed for research purposes pursuant to an authorization, or pursuant to a waiver of authorization, reviews preparatory to research, etc.).

3. *Research Authorization.* HIPAA requires that an authorization describe, among other things, the persons authorized to make the requested use or disclosure and the persons to whom the covered entity may make the requested use or disclosure. While this requirement seems simple at first blush, it can be a complicated task in, for example, a large, Phase III clinical trial. For example, in a multi-site study, the parties that might need identifiable data and therefore must be listed on the authorization form as possible data disclosers/users/recipients include: all the research sites, any other health care providers who might interact with the subject in connection with the study (*e.g.*, a primary care physician performing a monthly blood draw and sending the sample to a research site), laboratories and data analysis centers, CROs, site management organizations, the research sponsor, the research staff, IRBs and Data Safety Monitoring Boards, and many others. Any omissions could be costly, since failure to list a person or entity as a legitimate recipient and/or user of subjects' data would mean that such ''unlisted'' persons or entities could not legitimately receive and/or use the data.

Because the research sponsor best understands all aspects of the study's information flow, it may be wise for the research sponsor to offer a research authorization to be used at each site for the study. Sponsors therefore should attach to the clinical trial agreement

[4] While case report forms often omit direct subject identifiers such as names, they often will contain treatment dates, subject initials, and other information that might be ''identifiable'' for HIPAA purposes.

[5] 45 C.F.R. § 164.502(i).

[6] Indeed, this is likely how most Notices will be structured because HIPAA requires a statement in the Notice that ''other uses and disclosures will be made only with the individual's written authorization.'' 45 C.F.R. § 164.520(b)(1)(ii)(E).

[7] While HIPAA does not create a private right of action, many have speculated that courts will look to HIPAA as a benchmark for a negligence or reasonableness standard.

  MRLR ISSN 1539-1035

they send to research sites a HIPAA authorization template, tailored to the information flow for the specific protocol, to ensure that the authorization adequately permits disclosure of identifiable information to (and use of that information by) all the parties that need access to it (and/or use of it) for the study. Since research sponsors already attach an informed consent form template for study sites to use (subject to IRB review and approval), this addition should be easily absorbed into existing processes.

4. *The Protocol.* Research protocols currently explain the informed consent form provided by the sponsor and how to use the form in the informed consent process. Protocols similarly should explain the HIPAA authorization form sent by the sponsor (or other form of authorization used by the site or investigator) so that the investigator understands the importance of the form, implements the form properly, and is able to answer any questions about it accurately.

5. *Site Monitors.* FDA regulations require research sponsors to oversee the conduct of their clinical investigations.[8] To fulfill this requirement, sponsors send monitors to research sites to ensure that the investigators, research staff, and IRBs are meeting their regulatory responsibilities and conducting the study in accordance with the protocol. As of April 14, 2003, part of site monitors' regular audit responsibilities should include verifying that subjects have signed HIPAA authorizations and that those authorizations permit disclosure to the sponsor, the CRO, and any other contractors of the sponsor. In addition, leading up to the Security Standards' compliance date of April 21, 2005, research sponsors should begin to consider to what extent it is possible or appropriate for them to begin monitoring for some aspects of security compliance by their researchers or research sites. The site monitors should be trained in how and why to audit for these limited aspects of HIPAA compliance, so that they understand these changes to their monitoring activities.

6. *Training of Investigators.* Research sponsors generally host investigator meetings near the beginning of a study in order to help investigators and their research staffs better understand specific aspects of the protocol. Sponsors should train investigators in HIPAA compliance as part of this investigators' meeting. The HIPAA training should emphasize the importance of securing each subject's HIPAA authorization in interventional trials and should help investigators complete HIPAA waiver requests for registry or database studies at sites that require local IRB or Privacy Board approval of HIPAA waiver applications.[9] Educating investigators and their research staffs in HIPAA compliance will be particularly important in the first year of HIPAA enforcement (*i.e.*, after April 14, 2003, for the privacy regulations, and after April 21, 2005, for the security regulations), since many investigators may yet not understand how HIPAA will affect the conduct of a study, and many hospitals and physician practices may not be educating these investigators about HIPAA compliance obligations in the context of clinical research.

7. *CRO Agreements.* Research sponsor contracts with CROs, central laboratories, and any other entities receiving identifiable data either from the sponsor or directly from the sites should require such entities to keep patient information confidential, except for (1) uses and disclosures necessary for study purposes, and (2) uses and disclosures required as part of the entity's interaction with federal authorities. While such contracts often require the confidentiality of trade secrets or proprietary information, many do not specifically protect patient information. Although HIPAA does not specifically require such contractual provisions unless the data were received or disclosed as part of a ''limited data set'' or pursuant to a business associate agreement,[10] subjects are promised a high degree of confidentiality during the informed consent process, and such promises can only be ensured by contractually restricting data recipients' use and disclosure of patient information. Moreover, the advent of HIPAA will raise the public's privacy awareness and provides a good opportunity to improve current privacy practices, in order for sponsors to avoid any civil liability for violation of subjects' privacy.

8. *Existing Studies.* In studies for which a clinical trial agreement already is in place, research sponsors have two options to ensure their continued access to data after April 14, 2003: they can send to the sites either (1) an amendment to the existing agreement that contains the representations, warranties, and other provisions described above, or (2) a letter confirming that the existing agreement requires the site to abide by all applicable laws,[11] that the site will comply with HIPAA as of April 14, 2003, and that HIPAA compliance includes obtaining an authorization for each research subject (or waiver of authorization). If the existing clinical trial agreement does not specifically require compliance with applicable laws, an amendment may be more appropriate.

Note that special rules apply to studies that were started prior to April 14, 2003, but for which the research sites must continue to use or disclose PHI after that date.[12] Specifically, if informed consent was not waived for a study (*e.g.*, for interventional research), subjects who have signed an informed consent form before April 14, 2003, need not sign a HIPAA authorization form, but subjects enrolled after that date must ex-

[8] 21 C.F.R. § 312.50; 21 C.F.R. § 812.40.

[9] HIPAA does not require that a waiver be granted by any particular IRB or Privacy Board in order for a covered entity to release data in reliance on the waiver. For example, an academic medical center with an affiliated IRB could release data under a waiver granted by an unaffiliated commercial IRB or Privacy Board, or by another institution's affiliated IRB. As a result, sponsors technically may prepare a waiver request and submit the request to a central IRB or Privacy Board without assistance from the investigators. Nevertheless, many institutions' research policies may require local IRB or Privacy Board approval of a waiver request in some or all circumstances.

[10] Note that research sponsors and others performing research-related functions almost never will be business associates of a covered entity because research is not a ''covered function'' under HIPAA. *See* 67 Fed. Reg. 53182, 53252 (Aug. 14, 2002); Department of Health and Human Services, *Standards for Privacy of Individually Identifiable Health Information* (Dec. 3, 2002), at http://www.hhs.gov/ocr/hipaa/guidelines/guidanceallsections.pdf, p. 43.

[11] While most clinical trial agreements contain such provisions, legal counsel should verify this in each instance.

[12] Note that for studies for which informed consent was waived, the covered entity must obtain a HIPAA authorization if informed consent is sought from the individual after April 14, 2003.

ecute HIPAA authorizations.[13] Any limitations on the use and disclosure of PHI contained in the informed consent form must be honored. For these studies, sponsors may wish to (1) clarify sites' obligations in the amendment or letter mentioned above, and (2) ensure that site monitors understand that the documentation that should be in the study file will depend on each subject's enrollment date.

9. *Policies and Procedures*. Sponsors' internal policies and procedures must be amended to encompass the processes described above.

Conclusion

While HIPAA does not directly regulate commercial research sponsors as such, HIPAA could substantially restrict research sponsors' access to PHI if investigators and sites do not implement HIPAA fully or accurately. There is much sponsors can do, however, to ensure investigators' and sites' HIPAA compliance. Specifically, sponsors can incorporate HIPAA compliance (and other privacy protections) into their agreements with research sites and others, and they can educate and monitor those who must implement HIPAA on the ground. Not only are these steps important to protecting sponsors' access to important research data, but they also are good research practice. Safeguarding the privacy of research subjects is, after all, part and parcel of the ethical conduct of research. With the oft-cited mistrust of clinical research by the public,[14] commercial research sponsors will be well-served by using HIPAA as an opportunity to examine and improve their own privacy practices and those of the researchers and companies that handle patient information on their behalf.

---

[13] If informed consent has been waived for a study before April 14, 2003 (*e.g.*, for retrospective chart reviews), covered entities may continue indefinitely to use and disclose the subjects' PHI in connection with the study without obtaining a HIPAA authorization from the subjects and without an IRB or Privacy Board waiver.

[14] *See*, *e.g.*, Daniel D. Federman et al., eds., *Responsible Research: A Systems Approach to Protecting Research Participants* INSTITUTE OF MEDICINE, at 14-15 (2002).

  MRLR ISSN 1539-1035