PALMER & DODGE LLP
111 HUNTINGTON AVENUE AT PRUDENTIAL CENTER
BOSTON, MA 02199-7613

HIPAA Issues for Biotech and Life Science Companies: On the Frontier of Science and on the Edge of HIPAA

by

Mark E. Schreiber
617-239-0585
mschreiber@palmerdodge.com

and

Patrick J. Concannon
617-239-0419
pconcannon@palmerdodge.com

Introduction

Most biotech and life sciences companies are not directly covered by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). Yet biotechs must collect and make use of de-identified or occasionally individually identifiable patient health data from clinical studies to sustain themselves, requiring that they work closely with HIPAA-covered entities. HIPAA's standards *are* being imposed indirectly on biotech, medical device and testing companies even where the companies are not covered entities or business associates under HIPAA, principally through clinical trial agreements ("CTA's"). Clinical researchers and research study sponsors increasingly need to be sensitive to and savvy about HIPAA standards that their partner researchers, physicians or health care providers live with day to day.

Are medical device companies covered entities?

Medical device companies clearly can be HIPAA covered entities. "Health care" under HIPAA means care, services or supplies related to the health of an individual and includes, but is not limited to, "preventative, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body" and also "sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription."[1]

A medical device company meets the HIPAA's definition of "health care provider" if it is a provider of medical or health services (as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s). See Appendix A for HHS' comments in the December 2000 Notice of Proposed Rulemaking about this definition. The definition of "provider of medical or health services" under 1861(s) is quite broad. The term "medical and other health services" means any of the following items or services (among others):

[1] See 45 C.F.R. § 160.103.

(2)(C) diagnostic services which are—

(i) furnished to an individual as an outpatient by a hospital or by others under arrangements with them made by a hospital, and

(ii) ordinarily furnished by such a hospital (or by others under such arrangements) to its outpatients for the purpose of diagnostic study;

(2)(P) prostrate cancer screening tests;

(2)(R) colorectal cancer screening tests;

(13) screening mammography;

(14) screening pap smear; screening pelvic exam.

The above-referenced sections of the definition may apply to certain medical device companies.

The next question is whether a medical device company that is a health care provider, as defined, also transmits health information in certain electronic billing or claims transactions. If so, such a medical device company may be a covered entity under HIPAA. Note that only one isolated billing email containing health information is required for a health care provider to trigger covered entity status.

A relatively small number of device manufacturers bill for their equipment on a per use basis or submit Medicare or health insurance reimbursement claims electronically relating to such uses. Those that do are the most obvious candidates for medical device HIPAA-covered entities.

Many medical device companies provide detailed training and servicing in connection with their products, and in the course of providing such services their employees may encounter individually identifiable health information, or "protected health information" ("PHI"). Some entities now are considering disabling the PHI access component of the device to limit HIPAA exposure. Yet other medical device manufacturers will have summarily dismissed the question of possible HIPAA applicability based upon a belief that they do not engage in any electronic billing transactions; this conclusion may be reached without sufficient inquiry into the flow of PHI in the organization and the possibility that PHI is used for billing, claims or insurance purposes on occasion by their organization's accounts receivable group. It is easy for the best intentioned regulatory team engaged in a HIPAA compliance assessment to inadvertently fail to ask, or have others ask, the right questions of the people in their organization, including in accounts receivable.

Are medical device companies business associates?

In some cases, yes. A small number of medical device manufactures may review the PHI of covered entities in the course of performing a quality review function listed under the "business

associate" definition in the HIPAA regulations.[2] For example, a manufacturer of an imaging instrument might be called upon to review patient-specific images and provide feedback to the technician, physician or others at a HIPAA covered entity. Such device manufacturers may qualify as business associates under HIPAA.

Additionally, where the business helps de-identify records or create a limited data set for a covered entity, these are recognized business associate functions.

For guidance as to when medical device companies are deemed covered entities or business associates, see the HHS FAQ Answer included at Appendix B.

Are clinical study sponsors business associates under HIPAA?

Generally speaking, no. Sponsors and sponsors' contract research organizations ("CRO's") typically do not perform any HIPAA-defined service functions or activities on behalf of the research facilities. Some research facilities will nonetheless refer to a study sponsor as a business associate and/or impose PHI handling obligations on sponsors in their standard CTA's that are tantamount to business associate agreement obligations. Research sites should require that sponsors agree to *reasonable* limitations on sponsors' use of study data. Sponsors should, however, strongly resist unnecessarily being characterized as a business associate or agreeing to overbroad or inapplicable PHI handling obligations similar to those of business associates. Some sponsors hope to make use of study data for purposes other than research or scientific purposes, and resist provisions that tie their future use of study PHI to research or scientific purposes.

A model letter from a CRO to a study site that explains that the CRO is not a business associate under HIPAA is included at Appendix C.

Can a HIPAA authorization be drafted so as to authorize future specified research uses beyond the primary research study?

The answer is "no." HIPAA's regulations require that research authorizations specify "each purpose" for the use and disclosure.[3] As it is virtually impossible at any given time to describe the purpose of a future, yet to be conceived study, an authorization form that purports to authorize the use and disclosure of PHI for future, unspecified research studies is likely to be HIPAA non-compliant.[4] An exception is an authorization for PHI use in a registry or database for unspecified future research, which HHS indicates is acceptable.

---

[2] *Id*.

[3] See 45 C.F.R. § 164.508(c)(iv).

[4] For a useful discussion of the interplay between research facilities, investigators, and sponsors with respect to HIPAA authorizations for clinical studies, see "The 'Future Uses' Dilemma: Secondary Uses of Data and Materials by Researchers and Commercial Research Sponsors," by Mark Barnes & Kate Gallin Heffernan, BNA Medical Research Law & Policy Report, Vol. 3, No. 11, June 2, 2004, pp. 440-50.

Sponsors should pay close attention to appropriate HIPAA authorization language, as noted below, and also the drafting of CTA's. Sponsors are almost never HIPAA covered entities and thus generally need not comply with HIPAA standards upon receiving PHI pursuant to a valid HIPAA authorization. The most significant limits on a sponsor's use of PHI from clinical studies are imposed by CTA's, including proposed uses and disclosures, and possibly exclusions for marketing purposes.

Sponsors should also be sufficiently familiar with state privacy laws that might impact the sponsors' future PHI usage options. Finally, it is obvious that a business associate agreement erroneously entered into between a facility and a sponsor can have a dramatic impact of the sponsor's ability to use and disclose PHI from a given study in the future.

Should clinical study sponsors insist on having a say as to the contents of HIPAA authorizations?

The answer is "yes." As mentioned above, study sponsors are generally not covered entities under HIPAA. Sponsors nonetheless have compelling interests in ensuring that authorizations used in clinical studies are HIPAA-compliant due to the sponsor's dependency upon the proper disclosure of the data resulting from studies. (It may not be in the sponsor's interests to "push the envelope" of excessively broad wording of HIPAA authorizations for this same reason.) If months after authorizations were entered into by study participants in a given study, and after the study was underway, it was determined that the authorizations were HIPAA non-compliant, the sponsor likely could not or legally should not receive the participants' PHI under those circumstances. If the authorizations were determined to be defective only after the sponsor had received PHI from the study, the sponsor could face civil exposure if it were to use the PHI.[5] Risks to sponsors aside, as a practical matter the sponsor is typically in a good position to anticipate the various classes of persons to whom PHI must be disclosed throughout the clinical process.

Study sponsors should insist on representations and warranties in clinical trial agreements that sites will comply with HIPAA, obviously including HIPAA's authorization requirements, and take a hands-on approach to ensure the required core elements in a study's authorization before participants begin to sign the authorizations. Study facilities will often insist upon authorization drafts that reflect the concerns of their IRBs. Study sponsors, which typically fund studies, should nonetheless have sufficient leverage to require that authorizations are HIPAA compliant from their perspective and worded in an appropriate, reasonable fashion.

The following hypothetical example is roughly on point. A researcher moves from Facility A to Facility B. Facility A expresses reluctance to transfer medical records that it disclosed to the researcher out of concern for whether the purpose as described in the combined informed consent/HIPAA authorization allowed for such a transfer. If the sponsor then takes the position that one of the HIPAA-required statements arguably was not included in the informed consent/HIPAA

[5] It has been further suggested that the FDA may refuse to accept data in an FDA application where PHI was improperly disclosed, but the FDA, we are informed, would as a practical matter be loath to make such a determination or otherwise entangle itself in HIPAA issues over which HHS, and not FDA, has jurisdiction.

authorization, this might give rise concerns by the sponsor about it's ability to use study data that had been disclosed to it and possibly have a disruptive effect on the study. These concerns may be avoided if more attention is paid to the authorization language at the outset.

Finally, it should be noted that a site's Notice of Privacy Practices, if not carefully drafted, can have a limiting effect on the ability of a site to disclose PHI for research purposes, so sponsors should also review a copy of the privacy notice as part of their diligence in preparation for a study.

Confidentiality agreements between a medical center and a Sponsor or CRO

Health care facilities often require that sponsors or their CRO's enter into standard confidentiality agreements with the centers before the medical center sites will allow access to study participant PHI. These confidentiality agreements broadly restrict the use and disclosure of PHI. CRO's must review such agreements carefully and consider revising them before signing so that it is clear that the agreements allow for use and disclosure of PHI for study monitoring purposes and for uses pursuant to valid HIPAA authorizations.

Accounting for Research Disclosures

HIPAA-covered study facilities often use and disclose PHI for research purposes pursuant to patient authorizations. HIPAA's regulations carve out disclosures made pursuant to authorizations as a type of disclosure for which covered entities need not provide accountings to patients.[6] Facilities should be mindful that disclosures made pursuant to IRB waivers *must* be accounted for in response to a patient's request for an accounting of PHI disclosures. As public awareness of privacy issues grows and HIPAA enforcement activities by HHS increase, such requests will undoubtedly occur more frequently. It is important for HIPAA-covered facilities to have disclosure documentation procedures in place, and which are adhered to in practice.

\- -

Mark E. Schreiber is Chair of Palmer & Dodge LLP's Privacy Group in Boston and is a partner in the Labor and Employment Group.

Patrick J. Concannon is an Associate in the Business Law Group of Palmer & Dodge LLP in Boston.

[6] See 45 C.F.R. § 164.528(a)(1)(iv).

Appendix A

Health Care Provider Definition

from 65 Fed. Reg. 82,477-78 (2000)

Health Care Provider

We proposed to define health care provider to mean a provider of services as defined in section 1861(u) of the Act, a provider of medical or health services as defined in section 1861(s) of the Act, and any other person or organization who furnishes, bills, or is paid for health care services or supplies in the normal course of business.

[[Page 82,478]]

In the final rule, we delete the term ``services and supplies,'' in order to eliminate redundancy within the definition. The definition also reflects the addition of the applicable U.S.C. citations (42 U.S.C. 1395x(u) and 42 U.S.C. 1395x(s), respectively) for the referenced provisions of the Act that were promulgated in the Transactions Rule.

To assist the reader, we also provide here excerpts from the relevant sections of the Act. (Refer to the U.S.C. sections cited above for complete definitions in sections 1861(u) and 1861(s).) Section 1861(u) of the Act defines a ``provider of services,'' to include, for example, a hospital, critical access hospital, skilled nursing facility, comprehensive outpatient rehabilitation facility, home health agency, hospice program, or, for purposes of section 1814(g) (42 U.S.C. 1395f(g)) and section 1835(e) (42 U.S.C. 1395n(e)), a fund.'' Section 1861(s) of the Act defines the term, ``medical and other health services,'' and includes a list of covered items or services, as illustrated by the following excerpt:

(s) Medical and other health services. The term ``medical and other health services'' means any of the following items or services:

(1) Physicians' services;

(2) (A) services and supplies . . . furnished as an incident to a physician's professional service, or kinds which are commonly furnished in physicians' offices and are commonly either rendered without charge or included in the physicians' bills; (B) hospital services . . . incident to physicians' services rendered to outpatients and partial hospitalization services incident to such services; (C) diagnostic services which are-- (i) furnished to an individual as an outpatient by a hospital or by others under arrangements with them made by a hospital, and (ii) ordinarily furnished by such hospital (or by others under such arrangements) to its outpatients for the purpose of diagnostic study; (D) outpatient physical therapy services and outpatient occupational therapy services; (E) rural health clinic services and federally qualified health center services; (F) home dialysis supplies and equipment, self-care home dialysis support services, and institutional dialysis services and supplies; (G) antigens . . . prepared by a physician . . . for a particular patient, including antigens so prepared which are forwarded to another qualified person . . . for administration to such patient, . . . by or under the supervision of another such physician; (H)(i)

services furnished pursuant to a contract under section 1876 (42 U.S.C. 1395mm) to a member of an eligible organization by a physician assistant or by a nurse practitioner . . . and such services and supplies furnished as an incident to his service to such a member . . . and (ii) services furnished pursuant to a risk-sharing contract under section 1876(g) (42 U.S.C. 1395mm(g)) to a member of an eligible organization by a clinical psychologist . . . or by a clinical social worker . . . (and) furnished as an incident to such clinical psychologist's services or clinical social worker's services . . .; (I) blood clotting factors, for hemophilia patients . . .; (J) prescription drugs used in immunosuppressive therapy furnished, to an individual who receives an organ transplant for which payment is made under this title (42 U.S.C. 1395 et seq.), but only in the case of (certain) drugs furnished . . . (K)(i) services which would be physicians' services if furnished by a physician . . . and which are performed by a physician assistant . . .; and (ii) services which would be physicians' services if furnished by a physician . . . and which are performed by a nurse . . .; (L) certified nurse-midwife services; (M) qualified psychologist services; (N) clinical social worker services . . .; (O) erythropoietin for dialysis patients . . .; (P) prostate cancer screening tests . . .; (Q) an oral drug (which is approved by the Federal Food and Drug Administration) prescribed for use as an anti-cancer chemotherapeutic agent for a given indication, and containing an active ingredient (or ingredients) . . .; (R) colorectal cancer screening tests . . .; (S) diabetes outpatient self-management training services . . .; and (T) an oral drug (which is approved by the federal Food and Drug Administration) prescribed for use as an acute anti-emetic used as part of an anti-cancer chemotherapeutic regimen . . .

(3) diagnostic X-ray tests . . . furnished in a place of residence used as the patient's home . . .;

(4) X-ray, radium, and radioactive isotope therapy, including materials and services of technicians;

(5) surgical dressings, and splints, casts, and other devices used for reduction of fractures and dislocations;

(6) durable medical equipment;

(7) ambulance service where the use of other methods of transportation is contraindicated by the individual's condition . . . ;

(8) prosthetic devices (other than dental) which replace all or part of an internal body organ (including colostomy bags and supplies directly related to colostomy care), . . . and including one pair of conventional eyeglasses or contact lenses furnished subsequent to each cataract surgery . . . [;]

(9) leg, arm, back, and neck braces, and artificial legs, arms, and eyes, including replacements if required . . . ;

(10) (A) pneumococcal vaccine and its administration . . . ; and (B) hepatitis B vaccine and its administration . . . , and

(11) services of a certified registered nurse anesthetist . . . ;

(12) . . . extra-depth shoes with inserts or custom molded shoes with inserts for an individual with diabetes, if . . .;

(13) screening mammography . . . ;

(14) screening pap smear and screening pelvic exam; and

(15) bone mass measurement . . . (etc.)

Appendix B

FAQ from HHS Website (Answer ID 490)

Question: When may a covered health care provider disclose protected health information, without an authorization or business associate agreement, to a medical device company representative?

Answer: In general, and as explained below, the Privacy Rule permits a covered health care provider (covered provider), without the individual's written authorization, to disclose protected health information to a medical device company representative (medical device company) for the covered provider's own treatment, payment, or health care operation purposes (45 CFR 164.506(c)(1)), or for the treatment or payment purposes of a medical device company that is also a health care provider (45 CFR 164.506(c)(2), (3)). Additionally, the public health provisions of the Privacy Rule permit a covered provider to make disclosures, without an authorization, to a medical device company or other person that is subject to the jurisdiction of the Food and Drug Administration (FDA) for activities related to the quality, safety, or effectiveness of an FDA-regulated product or activity for which the person has responsibility. See 45 CFR 164.512(b)(1)(iii) and the frequently asked questions on public health disclosures for more information.

In certain situations, a covered health care provider may disclose protected health information to a medical device company without an individual's written authorization only if the medical device company is a health care provider as defined by the Rule. A medical device company meets the Privacy Rule's definition of "health care provider" if it furnishes, bills, or is paid for "health care" in the normal course of business. "Health care" under the Rule means care, services or supplies related to the health of an individual. Thus, a device manufacturer is a health care provider under the Privacy Rule if it needs protected health information to counsel a surgeon on or determine the appropriate size or type of prosthesis for the surgeon to use during a patient's surgery, or otherwise assists the doctor in adjusting a device for a particular patient. Similarly, when a device company needs protected health information to provide support and guidance to a patient, or to a doctor with respect to a particular patient, regarding the proper use or insertion of the device, it is providing "health care" and, therefore, is a health care provider when engaged in these services. See 65 FR 82569. By contrast, a medical device company is not providing "health care" if it simply sells its appropriately labeled products to another entity for that entity to use or dispense to individuals.

The following are some examples of circumstances in which a covered provider may share protected health information with a medical device company, without the individual's authorization:

- A covered provider may disclose protected health information needed for an orthopaedic device manufacturer or its representative to determine and deliver the appropriate range of sizes of a prosthesis for the surgeon to use during a particular patient's surgery. (This would be a

treatment disclosure to the device company as a health care provider. Exchanges of protected health information between health care providers for treatment of the individual are not subject to the minimum necessary standards. 45 CFR 164.502(b).)

- The device manufacturer or its representative may be present in the operating room, as requested by the surgeon, to provide support and guidance regarding the appropriate use, implantation, calibration or adjustment of a medical device for that particular patient. (This would be treatment by the device company as a health care provider. As noted in the prior example, treatment disclosures between health care providers are not subject to the minimum necessary standards.)

- A covered provider may allow a representative of a medical device manufacturer to view protected health information, such as films or patient records, to provide consultation, advice or assistance where the provider, in her professional judgment, believes that this will assist with a particular patient's treatment. (This would also be a treatment disclosure and minimum necessary would not apply.)

- A covered provider may share protected health information with a medical device company as necessary for the device company to receive payment for the health care it provides. (This would be a disclosure for payment of a health care provider and subject to minimum necessary standards.)

- A covered provider may disclose protected health information to a medical device manufacturer that is subject to FDA jurisdiction to report an adverse event, to track an FDA-regulated product, or other purposes related to the quality, safety, or effectiveness of the FDA-regulated product. (This would be a public health disclosure and subject to minimum necessary standards.)

A business associate agreement would not usually be required for the disclosures noted above. For example, a business associate agreement would not be needed for disclosures between health care providers for the treatment of the individual (45 CFR 164.502(e)(1)(ii)(A)). Likewise, a medical device company would not be a business associate of a covered provider with respect to public health disclosures to a device company that is subject to FDA jurisdiction or disclosures to a device company as a health care provider for that company's payment purposes, as in neither case is the device company performing a function or activity on behalf of, nor providing a specified service to, the covered provider. See 45 CFR 160.103. In other circumstances, however, a business associate agreement may be required even if the disclosure were permitted without an authorization. For example, a business associate agreement would be required if a covered entity asked the medical device company to provide an estimate of the cost savings it might expect from the use of a particular medical device; and to do so, the device company needed access to the covered entity's protected health information. In this case, the medical device company is performing a health care operations function (business planning and development) on behalf of the covered provider, which requires a business associate agreement even though the disclosure is permitted without an authorization.

Appendix C

Sample "We're not a BA" letter for CROs

DATE

ADDRESS

Re: STUDY/PROTOCOL #

Dear NAME:

This letter is in response to your recent request that Contract Research Organization ("CRO") execute the attached Business Associate Agreement.

CRO is a Contract Research Organization that has been contracted by Pharma Co ("SPONSOR") to monitor the above referenced study in which your site participated.

CRO is not a Business Associate of your organization as the provider under the Privacy Rule of the Health Insurance Portability and Accountability Act of 1996 ("the HIPAA Privacy Rule"). Under the HIPAA Privacy Rule, a business associate is defined as an entity that provides services *on behalf of* a covered entity. CRO has not been retained to provide services on behalf of you as the covered entity. Our services are on behalf of and pursuant to our contractual agreement with the Sponsor of the Study.

As CRO is neither a business associate nor a covered entity, we are not directly subject to the requirements of the Privacy Rule. However, contractually, we are required to protect the confidentiality and privacy of all patient information, and to use patient information only for the study-related purposes set forth in our contract with the Sponsor. Further, to the extent applicable to CRO, we are required to maintain the confidentiality and privacy of patient information consistent with federal and state law.

If you have any concerns or questions, please feel free to contact me at 202-555-1212.

Sincerely,

CRO