

## What Every Lawyer Needs to Know About the HIPAA Privacy Regulations

By *Jennifer A. Stiller*<sup>\*</sup>  
*Law Offices of Jennifer A. Stiller*

New Federal regulations concerning healthcare privacy rights and privacy practices can impinge upon legal practice in a number of ways. This article is an effort to highlight what legal practitioners generally need to know for purposes of ordinary legal practice.

### *Background*

In 1996, as part of the Health Insurance Portability and Accountability Act, or “HIPAA” (Pub. L. 104-191), Congress enacted 42 U.S.C. chapter 7, which was designed to improve the efficiency and effectiveness of the health care system by facilitating the electronic exchange of information with respect to certain financial and administrative transactions. At the same time, in recognition of the challenges to the confidentiality of health information presented by advances in health information technology and communications, Congress directed the Secretary of Health and Human Services (“HHS”) to adopt regulations to protect the privacy of individually identifiable health information.<sup>1</sup>

Those regulations were adopted August 14, 2002<sup>2</sup> and became effective April 14, 2003. They are codified at 45 C.F.R. §§ 160.101 – 160.312 and 164.102 – 164.534.

### *The HIPAA Privacy Regulations*<sup>3</sup>

Although the privacy regulations impose obligations only on “covered entities,” they affect those accustomed to obtaining information from such entities. The regulations apply to all forms of “protected health information,” whether maintained electronically or otherwise.

The HIPAA privacy regulations impose direct obligations only on three types of person or entity – health plans, healthcare providers, and healthcare clearinghouses. The regulations set forth detailed rules governing these covered entities’ internal use and external disclosure of protected health information, including complicated rules for when a patient authorization is required for use and disclosure and when it is. Where release of information is pursuant to a signed patient authorization, there are specific requirements for that document.

---

<sup>\*</sup> Jennifer A. Stiller is a solo practitioner in Haverford whose practice is limited to health law (for a description of what that is, see <http://www.healthregs.com/HealthLaw.shtml>). She was formerly chair of the Healthcare Practice Group at Montgomery, McCracken, Walker & Rhoads, LLP.

“Protected health information” is defined to mean individually identifiable health information, written or oral, maintained or transmitted in any form or medium. Information that does not identify an individual, and with respect to which there is no reasonable basis to believe an individual can be identified, is not “individually identifiable health information” and therefore is not PHI.

The regulations also create new individual patient rights, most notably the right to inspect and copy their own PHI, request amendments of erroneous or incomplete information, and obtain an accounting of disclosures of their information.

There is no private cause of action under HIPAA; enforcement is chiefly through complaints filed with the Office of Civil Rights (OCR) in the Department of HHS. OCR may impose civil penalties of \$100 per violation, with no covered entity subject to a penalty of more than \$25,000 in any one year. Any person who knowingly obtains another person’s individually identifiable health information or discloses it to someone else, is subject to criminal penalties, with the basic violation carrying a fine of \$50,000 and/or imprisonment for one year.<sup>4</sup>

For lawyers not involved in counseling covered entities about the obligations under HIPAA, the regulations present three main issues:

- What constitutes a valid patient authorization for release of PHI.
- Disclosures in connection with judicial proceedings.
- “Business associate” obligations.

#### *Valid Patient Authorizations*<sup>5</sup>

In order for a patient’s authorization to release his or her protected health information to be valid, it must be in writing, written in plain language, not combined with another document, and contain at least the following Core Elements:

- (1) A description of the information to be used or disclosed that identifies the information *in a specific and meaningful fashion*. (Emphasis added.)
- (2) The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure.
- (3) The name or other specific identification of the person(s), or class of persons, to whom the covered entity may make the requested use or disclosure.
- (4) A description of each purpose of the requested use or disclosure.

- (5) An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure.
- (6) Signature of the individual and date.<sup>6</sup>

A copy of the signed authorization must be provided to the individual who signed it.

In addition to the Core Elements, a HIPAA-compliant authorization must contain certain “required statements.” These are statements adequate to place the individual on notice of all of the following:

- (1) That the patient has a right to revoke the authorization in writing, and either:
  - The exceptions to the right to revoke and a description of how the patient may revoke the authorization; or
  - To the extent that such exceptions are set forth in the covered entity’s Notice of Privacy Practices, a reference to that Notice.
- (2) The ability or inability of the covered entity to condition treatment, payment, enrollment or eligibility for benefits on the authorization, by stating either that:
  - The covered entity may not condition treatment, payment, enrollment or eligibility for benefits on whether the individual signs the authorization (if none of the exceptions specified in 45 C.F.R. § 164.508(b) (4) applies); or
  - The consequences to the individual of a refusal to sign the authorization when one of the exceptions to 45 C.F.R. § 164.508(b)(4) permits the covered entity to condition treatment, enrollment in the health plan, or eligibility for benefits on failure to obtain such authorization.
- (3) The potential for information disclosed pursuant to the authorization to be subject to redisclosure by the recipient and no longer protected by the HIPAA privacy regulations.

An authorization is invalid if it does not contain a Core Element, if its expiration date has passed or expiration event has occurred, if it has been revoked, or if it is combined with another document to create a compound authorization. It is also invalid if the patient’s signature on it was required in order for the patient to receive treatment, payment, enrollment in the health plan, or eligibility for benefits, or if the covered entity to whom the authorization is directed knows any material information on it to be false.

### *Disclosures in Connection with Judicial Proceedings*<sup>7</sup>

A covered entity may disclose PHI in connection with a judicial or administrative proceeding in response to a court or administrative order, but only such PHI as is authorized by such order.

If the information is sought by subpoena, discovery request, or other lawful process, the covered entity may disclose the PHI without an authorization only if the covered entity has received *satisfactory assurances* from the party seeking the PHI that the patient has been given notice of the request; or that such party has made a reasonable effort to obtain a “qualified protective order” (unless the covered entity itself makes reasonable efforts to provide notice to the patient or to seek a qualified protective order).

A “qualified protective order” is a court or administrative order, or a stipulation of the parties, that:

- Prohibits the parties from using or disclosing the PHI for any purpose other than the proceeding for which it was requested; and
- Requires that the PHI be returned to the covered entity or destroyed when the litigation is over.

Given that the second bullet point may prove problematic for many lawyers, it would seem that providing satisfactory assurance of notice to the patient is likely to be the best approach for most attorneys. “Satisfactory assurances” of notice to the patient requires a good faith effort to send written notice to patient (notice to the last known address), containing sufficient information to permit the patient to raise an objection before the tribunal. The time for filing objections must have lapsed without any objections having been filed (or, alternatively, the tribunal must have resolved any objections, and information sought is consistent with that decision).

### *Business Associates*<sup>8</sup>

The HIPAA privacy regulations allow a covered entity to disclose PHI to a business associate (“BA”), and allow the BA to create or receive PHI on covered entity’s behalf, if the covered entity has a written contract with the BA that establishes the permitted and required uses and disclosures of PHI by the business associate.<sup>9</sup> Disclosure of PHI to a business associate may only be for the purpose of helping the covered entity to carry out its healthcare functions – not for the BA’s independent use or purposes. The contract may not authorize the business associate to use or further disclose the information in a manner that would violate the requirements of the HIPAA privacy regulations if done by the covered entity.

If a covered entity authorizes a BA to create, receive, maintain or transmit

electronic PHI on the covered entity's behalf, the BA must also provide satisfactory assurances that it will safeguard the information in accordance with the HIPAA security regulations.<sup>10</sup> In the event of a material breach of BA agreement, the covered entity must terminate the relationship or, if that is not feasible, it must report the breach to OCR.

For outside counsel, it is important to note that the definition of “business associate” specifically includes anyone who provides legal services to or for a covered entity, where the provision of the service involves the disclosure of individually identifiable health information from the covered entity or from another of its business associates, to the lawyer.<sup>11</sup> Keeping this definition in mind:

- A defense lawyer who represents a physician in a malpractice claim *is* a business associate of the physician, and must have a business associate agreement with him.
- The plaintiff’s lawyer suing the physician *is not* a business associate of the physician.
- The plaintiff’s lawyer who wishes to obtain her client’s medical records from health care providers who are not defendants in the litigation *is not* a business associate of such providers (because she is not providing legal services to them).
- The commercial litigator who represents a hospital in a dispute over a failed real estate deal *is not* a business associate of the hospital because the representation does not involve access by the lawyer to individually identifiable health information.

In conclusion, it should be noted that once individually identifiable health information is in the possession of a person who is neither a covered entity nor the business associate of a covered entity, that information is no longer PHI, and the HIPAA regulations do not apply to it. There may, of course, be other legal obligations, such as those created by contract or other laws regarding privacy, that attach to such information, but those are beyond the scope of this article.

## ENDNOTES

---

<sup>1</sup> 42 U.S.C. § 1320d-2 note.

<sup>2</sup> 67 Fed. Reg. 53181 (Aug. 14, 2002).

<sup>3</sup> It should be emphasized that the HIPAA privacy regulations are complex and often confusing. This summary description of the regulations is of necessity considerably less detailed than the regulations themselves, and should be taken as nothing more than a very broad overview.

<sup>4</sup> If the offense is committed under false pretenses, the penalties are \$100,000 and/or five years imprisonment. If the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, the penalties are \$250,000 and/or ten years imprisonment.

<sup>5</sup> 45 C.F.R. § 164.508.

<sup>6</sup> If the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual must also be provided.

<sup>7</sup> 45 C.F.R. § 164.512(e).

<sup>8</sup> 45 C.F.R. § 160.504(e).

<sup>9</sup> For specific requirements for such BA agreements, see 45 C.F.R. § 164.504(e).

<sup>10</sup> See 68 Fed. Reg. 8333 (Feb. 20, 2003).

<sup>11</sup> See 45 C.F.R. § 160.103 (definition of "Business Associate").