The Health Insurance Portability and Accountability Act ("HIPAA") Privacy Rule[1]

by Susan H. Pauley, Esq.
Steptoe & Johnson PLLC

Background. On November 3, 1999, the U.S. Department of Health and Human Services ("HHS") published a proposed HIPAA Privacy Rule.[2] On December 28, 2000, the Rule was finalized, in a somewhat modified form. On April 14, 2001, despite a change in administration, the HIPAA Privacy Rule became effective. On August 14, 2002, modifications to the HIPAA Privacy Rule were published. The compliance deadline for all covered entities (defined below), except small health plans, was April 14, 2003. Small health plans were given an additional year to come into compliance.

Significant modifications to the HIPAA Privacy Rule (as well as the HIPAA Security Rule) were included in the Health Information Technology for Economic and Clinical Health (HITECH) Act (and its implementing regulations) within the American Recovery and Reinvestment Act ("ARRA"), which was enacted on February 17, 2009 (Pub. L. No. 111-5). In general, the effective date for the modifications and new requirements imposed by the ARRA was February 17, 2010. This effective date did not, however, apply to all of the new requirements.

Preemption. Except in certain circumstances, HIPAA preempts state law when HIPAA requirements are "contrary to" state law. One of the most noteworthy circumstances in which HIPAA does not preempt state law is where state privacy laws are more stringent than HIPAA.

Key Defined Terms. The HIPAA Privacy Rule regulates covered entities' use and disclosure of protected health information.

"Covered entities" is defined to mean: (1) health plans; (2) health care clearinghouses; and (3) health care providers who transmit health information electronically in connection with a covered transaction.

"Protected health information" or "PHI" is broadly defined as individually identifiable health information that is transmitted or maintained electronically or in any other form.[3]

"Individually identifiable health information" is information that –

- Is created or received by a health care provider, health plan, employer, or health care clearinghouse;

---

[1] Due to the length and complexity of the HIPAA Privacy Rule, this article does not provide a comprehensive review of the HIPAA Privacy Rule. Instead, the article highlights certain key issues. The author would like to thank Michael Nissim-Sabat for his assistance in updating this article.

[2] The HIPAA Privacy Rule is found at 45 C.F.R. Part 160 and Subparts A and E of Part 164.

[3] On a related note, the HIPAA Security Rule, which may be found at 45 C.F.R. Part 160 and Subparts A and C of Part 164, regulates the use and disclosure of electronic PHI – that is PHI that is transmitted or maintained in electronic form (*e.g.*, records on CD-Rom or floppy disk, email, scanned records).

- Relates to an individual's past, present, or future health; the provision of health care to an individual; or the past, present, or future payment for health care to an individual; and
- Identifies an individual (or for which there is a reasonable basis to believe that the information may be used to identify the individual).

It is important to note that PHI does not include individually identifiable health information contained in certain categories of records such as, for example, employment records maintained by a Covered Entity in its role as employer and education records covered by the Family Educational Rights and Privacy Act.

Permitted Uses and Disclosures of PHI. In general, the HIPAA Privacy Rule permits Covered Entities to use and/or disclosure of PHI in the following circumstances:

- For treatment, payment and health care operations purposes without an authorization;
- For the following other purposes without an authorization:
  - Uses/disclosures required by law.
  - Uses/disclosures for public health activities.
  - Disclosures about victims of abuse, neglect, or domestic violence.
  - Uses/disclosures for health oversight activities.
  - Disclosures for judicial and administrative proceedings.
  - Disclosures for law enforcement purposes.
  - Uses/disclosures about decedents (coroners, medical examiners, funeral directors).
  - Uses/disclosures for cadaveric organ, eye, or tissue donation.
  - Uses/disclosures for research purposes.
  - Uses/disclosures to avert a serious threat to health or safety.
  - Uses/disclosures for specialized government functions.
  - Disclosures for worker's compensation (*i.e.,* Covered Entities may disclose PHI as authorized by and to the extent necessary to comply with state worker's compensation laws).
- Pursuant to a HIPAA-compliant authorization.

Use and Disclosure of PHI in Litigation. In the litigation context,[4] PHI is typically obtained in one or more of the following of the following ways:

- Voluntarily from the record subject (*i.e.*, in response to a request for production of records).
- Pursuant to a HIPAA-compliant authorization.
- Pursuant to a court order/Qualified Protective Order.
- Pursuant to a subpoena meeting the requirements of the HIPAA Privacy Rule.

[4] The Supreme Court of Appeals of West Virginia has noted that "'discovery of protected health information is permitted so long as a court order or agreement of the parties prohibits disclosure of the information outside the litigation and requires the return of the information once the proceedings are concluded.'" *State ex rel. State Farm Mut. Auto. Ins. Co. v. Bedell*, 719 S.E.2d 722, 742 (W. Va. 2011), *cert. denied*, *State Farm Mut. Auto. Ins. Co. v. Bedell*, 132 S. Ct. 761 (2011) and *Luby v. Bedell*, 132 S. Ct. 776 (2011) (internal citations omitted).

Components of a HIPAA-compliant Authorization. In order to be compliant with the HIPAA Privacy Rule, an authorization must contain the following core elements:

- A description of the information to be used/disclosed.
- The name or class of persons permitted to make the use/disclosure.
- The name or class of persons permitted to use the authorization and receive the disclosures.
- A description of the purpose of the use/disclosure.
- An expiration date or the naming of an event that will cause the authorization to expire.
- A statement advising the individual of his/her right to revoke the authorization, along with an explanation of how to revoke the authorization and an address to which a revocation may be sent.
- The signature of the individual consenting to the authorization and the date. If the authorization is executed by a representative of the record subject (*e.g.*, parent, guardian), a description of the relationship is required.
- A statement regarding the ability/inability to condition treatment, payment, enrollment, or benefits on the execution of the authorization.
- A statement that information released pursuant to the authorization may no longer be protected and may be subject to re-disclosure.

Authorizations are defective if the expiration date has passed or the Covered Entity providing information pursuant to the authorization knows that the expiration event has occurred; the authorization has not been completed; the Covered Entity providing information pursuant to the authorization knows that the authorization has been revoked; or the Covered Entity providing information pursuant to the authorization knows that material information in the authorization is false.

Disclosure of PHI in Response to a Subpoena or a Qualified Protective Order. Pursuant to 45 C.F.R. § 164.512(e), a Covered Entity may disclose PHI in response to a subpoena (unaccompanied by a court order) as long as the Covered Entity either (1) receives satisfactory assurance (*e.g.*, written statement and accompanying documentation demonstrating that the requesting party has made a good faith attempt to provide written notice to the record subject; that the notice includes sufficient information about the litigation/proceeding to allow the record subject to raise an objection; the time for any such objection has passed; and no such objection was made or any objection raised has been resolved and any disclosures are consistent with the resolution) from the party seeking the PHI that such party has made reasonable efforts to ensure that the record subject has been given notice of the record request or (2) receives satisfactory assurance from the party seeking the information that such party has made reasonable efforts to secure a qualified protective order meeting the HIPAA Privacy Rule requirements.

The HIPAA Privacy Rule requires that in order for a Covered Entity to disclose PHI pursuant to a qualified protective order, the qualified protective order must prohibit the parties from using or disclosing the PHI for any purpose other than the litigation or proceeding for which the PHI was requested; and requires that the PHI be returned to the Covered Entity or destroyed upon the conclusion of the litigation or proceeding.

Representation of Covered Entities.

In-house legal counsel. Covered Entities that employ in-house legal counsel may share PHI with their in-house legal counsel as part of their "health care operations." "Health care operations" are activities of a Covered Entity related to the Covered Entity's covered functions (*i.e.*, functions that make the entity a health plan, health care provider, or health care clearinghouse) such as, for example, conducting quality assessment and improvement activities; reviewing health care professionals' competence or qualifications; underwriting and premium rating; conducting or arranging for medical review, legal services, and auditing functions (*e.g.*, fraud and abuse detection); business planning and development; and business management and general administrative activities.

Outside Legal Counsel/Business Associates. If the representation of a Covered Entity by outside legal counsel, in a litigation or non-litigation context, requires the use and/or disclosure of PHI, a Business Associate Agreement must be executed. In general, a "Business Associate" is a person who performs or assists in the performance of (but not in the capacity of a member of the Covered Entity's workforce) a function or activity involving the use or disclosure of individually identifiable health information (*e.g.*, claims processing, billing) or provides (but not in the capacity of a member of the Covered Entity's workforce) legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for the Covered Entity and the provision of such service(s) involves the disclosure of individually identifiable health information from the Covered Entity (or a Business Associate of the Covered Entity) to the person. Business Associates are required to provide a written assurance (*e.g.*, written contract or other written agreement) that they will appropriately safeguard PHI disclosed to them by a Covered Entity.

It is important to note that the HITECH Act appears to codify the Business Associate Agreement requirement. In addition, the HITECH Act's additional privacy requirements must be incorporated into Business Associate Agreements. The HITECH Act also makes Business Associates subject to HIPAA's civil and criminal penalties.

Minimum Necessary Standard. Except in certain situations (*e.g.*, disclosures for treatment purposes, uses/disclosures to the record subject, uses/disclosures pursuant to a HIPAA-compliant authorization, uses/disclosures required by law, disclosures to the HHS Secretary for enforcement purposes, and uses/disclosures required for compliance with the HIPAA Administrative Simplification Rules), whenever a Covered Entity uses or discloses PHI or requests PHI from another Covered Entity, the Covered Entity is required to make reasonable efforts to limit PHI to the minimum amount necessary to accomplish the intended purpose.

Under the HITECH Act, which modified the Minimum Necessary Standard, the Minimum Necessary Standard will only be met if the use, disclosure, or request of PHI is limited

to a "limited data set" (most direct identifiers have been removed), or, if needed, to the minimum amount necessary to achieve the intended purpose. This provision was supposed to be, but has not yet been, replaced by guidance from the Secretary of the U.S. Department of Health and Human Services (which was supposed to have been issued within 18 months of the HITECH Act's enactment).

Individuals' Rights Under the HIPAA Privacy Rule. Not only does the HIPAA Privacy Rule address Covered Entities' uses and disclosures of PHI, but the HIPAA Privacy Rule also creates certain individual rights such as the following:

- Except in limited circumstances, the right to receive access to or a copy of PHI about themselves which is maintained by a Covered Entity. The ARRA added language to allow individuals to obtain a copy of their health information in electronic format if the information is maintained electronically.
- The right to request an amendment of his/her PHI.
- The right to receive an accounting of disclosures of PHI.[5]
- The right to receive a copy of a Covered Entity's Notice of Privacy Practices, upon request.

Enforcement and Penalties for Noncompliance. There is no express private right of action in HIPAA or the HIPAA Privacy Rule.[6] Instead, the U.S. Department of Health and Human Services ("HHS"), Office of Civil Rights ("OCR"), is responsible for enforcement. Penalties may be in the form of civil monetary penalties and/or criminal penalties. The ARRA modified HIPAA's enforcement provisions.[7] In particular, the HITECH Act strengthened the enforcement of the rules under HIPAA by creating four categories of violations reflecting increasing culpability levels, and four corresponding tiers of penalties with higher minimum penalties and a maximum penalty of $1.5 million per calendar year for all violations of an identical requirement (for violations occurring on or after February 18, 2009). Further, the HITECH Act eliminated the affirmative defense for violations in which the Covered Entity had no knowledge of the violation and, in exercising reasonable diligence, should not have known about the violation – that situation is now punished under the lowest tier of penalties. Also, the HITECH Act prohibited the imposition of penalties for any violation that is corrected within a 30-day time period unless the violation was due to willful neglect.

In addition to civil monetary penalties, criminal penalties may be imposed in certain situations. Criminal prosecutions for violations of the HIPAA Privacy Rule are handled by the United States Department of Justice. Criminal penalties may be imposed in those situations in which a person knowingly and wrongfully does the following: (1) uses or causes to be used a

---

[5] In May, 2011, as required by the Health Information Technology for Economic and Clinical Health (HITECH) Act, HHS issued a Notice of Proposed Rulemaking to modify the accounting of disclosure requirement. *See* 76 Fed. Reg. 31425.

[6] In the Southern District of West Virginia, it has also been determined that HIPAA does not provide a basis for federal question jurisdiction. *See Fields v. Charleston Hosp., Inc.*, 2006 WL 2371277, at *5 (S.D. W. Va.) (mem. op. & order) (HIPAA does not create a federal cause of action).

[7] For further information, see HIPAA Administrative Simplification: Enforcement Interim Final Rule; Request for Comments, 74 Fed. Reg. 56123 (October 30, 2009).

unique health identifier; (2) obtains individually identifiable health information relating to an individual; or (3) discloses individually identifiable health information to another person. Criminal penalties range from fines of up to $50,000 and/or imprisonment up to one year -- to fines of up to $250,000 and/or imprisonment for up to ten (10) years for those situations in which the violation was committed with the intent to sell, transfer, or use the information for commercial advantage, personal gain, or malicious harm.

With the enactment of the HITECH Act, state attorneys general may bring civil actions on behalf of residents to enjoin further violations and to obtain damages up to $25,000 per calendar year for violations of an identical requirement or prohibition. In addition, in those actions, attorneys' fees may also be awarded. The HITECH Act also clarified that non-Covered Entities (such as employees of Covered Entities) may be found to have violated HIPAA if the non-Covered Entity obtains or discloses individually identifiable health information maintained by a Covered Entity without authorization.

Under the HITECH Act, OCR was also required to perform periodic audits to ensure compliance by Covered Entities and Business Associates with the HIPAA Privacy Rule, the HIPAA Security Rule, and the Breach Notification requirements. OCR began a pilot audit program of 115 audits in November 2011. The pilot program is slated to conclude in December 2012.

On a Related Note . . . Breach Notification Requirements. In August, 2009, pursuant to the HITECH Act, OCR issued its interim final rule requiring notification of breaches of unsecured PHI. In the event of a breach of unsecured PHI, a Covered Entity must notify each individual whose unsecured PHI it believes has been or is reasonably believed to have been accessed, acquired, used, or disclosed as a result of the breach. Subject to certain exceptions, "breach" is the acquisition, access, use, or disclosure of PHI (in any format, not just electronic PHI) in a manner that is not permitted by the HIPAA Privacy Rule and that "compromises the security or privacy of the PHI" or, more specifically, in a manner that "poses a significant risk of financial, reputational, or other harm to the individual."

In the event that the breach involves the PHI of more than 500 residents of a state or jurisdiction, a Covered Entity is required to promptly (and, in any event, no later than 60 days) notify prominent media outlets serving the state or jurisdiction. The interim final rule also requires notification to the HHS Secretary. Specifically, in the event that the breach involves 500 or more individuals, the Covered Entity must notify the HHS Secretary. For breaches involving less than 500 individuals, the Covered Entity must maintain a log/documentation of the breach(es) and within 60 days of the end of each calendar year, notify the HHS Secretary.

The notification is to include:

- A brief description of the breach, including the date of the breach and the date that the breach was discovered, if known;
- A description of the types of unsecured PHI involved in the breach;
- Any steps that individuals should take to protect themselves from potential harm;

- A brief description of the Covered Entity's efforts to investigate the breach, to mitigate harm to individuals, and to protect against future breaches; and
- Contact information (*i.e.,* toll-free telephone number, e-mail address, web site, or postal address) for individuals to obtain additional information.

HHS developed a final breach notification rule, which it submitted for review to the Office of Management and Budget in May 2010. HHS later withdrew its final Security Breach Notification Rule from review by OMB to allow for further consideration. Until a new final rule is promulgated, the interim final rule is in effect.

HIPAA Omnibus Rule. In March, 2012, OCR submitted its omnibus HIPAA rule, which includes regulations on enforcement, breach notification, health plan use of genetic information, application of the HIPAA Security Rule to Business Associates and subcontractors, and using patient health information for marketing activities, to OMB for review. OMB, however, has delayed its release of the Rule.

Additional Information Available. While there are many sources of additional information regarding the HIPAA Privacy Rule, the U.S. Department of Health and Human Service's website (www.hhs.gov), and particularly the fact sheets and frequently asked questions included therein, are a good starting place to obtain additional information regarding the HIPAA Privacy Rule.

This article should not be construed or relied upon as legal advice or legal opinion on any matter. The content is intended for general information purposes only. You should consult with your own lawyer for legal advice or a legal opinion on the specific facts and circumstances of your own situation.