JW | Health e-Alert

An important health care law update from the law firm of Jackson Walker.

January 22, 2013

Resources

JW Health Care Practice Area

JW Health Care Attorneys

JW HealthBrief Newsletter

Contact JW

www.jw.com

Offices

Austin
100 Congress Avenue
Suite 1100
Austin, TX 78701

Dallas
901 Main Street
Suite 6000
Dallas, TX 75202

Fort Worth
777 Main Street
Suite 2100
Fort Worth, TX 76102

Houston
1401 McKinney Street
Suite 1900
Houston, TX 77010

San Angelo
301 W. Beauregard Avenue
Suite 200
San Angelo, TX 76903

San Antonio
112 E. Pecan Street
Suite 2400
San Antonio, TX 78205

Texarkana
6004 Summerfield Drive
Texarkana, TX 75503

The HIPAA Omnibus Rule: Incremental Revisions and a Few Big Pops

By **Jeff Drummond**

Nearly two years after the first anticipated publication date, the U.S. Department of Health and Human Services ("HHS") has finally published the "Omnibus" Final Rule implementing many changes to HIPAA called for by the Health Information Technology for Economic and Clinical Health Act ("HITECH") and finalizing other regulations that were previously issued in proposed form. The Omnibus Rule will officially be published Friday, January 25, 2013, with an "effective date" of March 26, 2013; however, HHS will not enforce most of the new provisions until September 23, 2013, thereby giving covered entities six months to implement fixes.

While the regulations are voluminous, the most important changes relate to a few specific areas: breach notifications; business associates and subcontractors; fundraising and marketing; "hybrid" entities; deceased patients; school immunization records; "notice of privacy practices" revisions; and the "hide" rule.

Breach Notification Changes: The biggest change wrought by the Omnibus Rule is the replacement of the "no harm" standard with a "probability that data was compromised" standard. The "no harm" standard stated that an improper disclosure of protected health information ("PHI") is not a "breach" that must be reported unless there is a "significant risk of financial, reputational, or other harm to the individual" whose data was exposed. This was judged to be too subjective a standard, even though most commentators argued for its continued inclusion. Under the new regulations, an improper disclosure need not be treated as a breach if the covered entity can demonstrate "that there is a low probability that the PHI in question has been compromised." HHS provides four factors for considering whether there is a low or high probability of compromise: the nature of the PHI (focusing on whether the data includes identifying information such as social security numbers instead of the sensitivity of the type of data, like mental health or STD data); who used or received the PHI; whether the PHI was actually acquired or viewed; and mitigation efforts.

HHS stated that the change was required to make the determination less subjective. However, HHS does not define what is meant by the data being "compromised." Therefore, it is hard to see how this has reduced the subjectivity in determining whether a data breach has occurred. The change also seems to focus the determination on what happens to the data itself, rather than whether the incident is likely to harm an individual such that the individual would need to protect himself. This will certainly result in more breaches being reported, since entirely harmless incidents will have to be reported because the data itself may have been exposed.

HHS has also made clear that any possible breach incident, including a breach of the minimum necessary rule (such as

providing more information than absolutely necessary in an otherwise HIPAA-compliant release), should trigger a risk analysis by the covered entity or business associate dealing with the matter. The risk analysis will have to address the four factors outlined by HHS and will drive the determination of whether there is a low probability of the data being compromised.

Of course, only breaches of "unsecured" PHI are required to be reported, and encryption is the only way to "secure" such data. Ultimately, the revised breach notification requirements should drive more covered entities to investigate and adopt encryption strategies, since any loss of encrypted data will not trigger a breach notification.

Business Associates and Subcontractors: HITECH brought business associates under the direct application of HIPAA, specifically with regard to the Security Rule administrative, physical and technical safeguards, as well as certain provisions of the Privacy Rule. In the proposed regulations, HHS notes the distinction between a business associate and a subcontractor. In the Omnibus Rule, HHS states clearly that all business associates and all subcontractors (that access PHI) are subject to HIPAA as "business associates," and noted that, while a covered entity need only have a contract in place with its direct business associate, that business associate must have a contract in place with its subcontractor business associate, and so on, all the way "down the chain."

The Omnibus Rule contains changes that will have to be reflected in business associate agreements ("BAAs"). However, if a covered entity changed its BAAs to comply with the provisions of HITECH, then those changes may be sufficient. HHS also granted some leeway to entities that already have BAAs in place that were compliant to the previous regulations: if a covered entity has a BAA in place prior to January 25, 2013, that met the pre-HITECH requirements, that BAA does not have to be revised to meet the Omnibus Rule until the earlier of the BAA's renewal date (excluding evergreen renewals) or September 22, 2014. In other words, you get an extra year if your BAAs were already in place.

Fundraising and Marketing: The Omnibus Rule implements several changes required by HITECH relating to fundraising and marketing. On the one hand, covered entities may use more information about a patient for fundraising purposes, such as the department where the individual received care, the patient's treating physician, and whether the patient had a good outcome from the care given. This will allow entities to better target fundraising. However, an entity's notice of privacy practices must say that fundraising materials may be sent, and every fundraising communication must give the individual the right to opt out of receiving any more in "clear and conspicuous language."

HITECH specifically addresses marketing activities, and restricts them unless the patient specifically authorizes them. Under the proposed regulations, HHS tried to distinguish between allowable and problematic communications, based on the type of communication and whether and how the covered entity may be compensated for making the communication. Under the Omnibus Rule, if the covered entity receives financial remuneration, almost all marketing communications will require an authorization from the patient, even if the communication is for treatment or health care operations (the restriction does not prevent the covered entity from receiving non-financial remuneration, such as where a third party provides the marketing materials or conducts the mailing on the covered entity's behalf). The restriction does not apply if the covered entity is paid for something other than the communication itself, such as a research grant. A provider can still make face-to-face communications or give the patient a promotional gift, and be compensated for it, without being required to get authorization; a provider can also be compensated for giving refill reminders or communications about currently-prescribed drugs or biologics (including information on how to operate delivery devices like insulin pumps) without an authorization, as long as the subsidy is reasonably related to the cost of making the communication.

Virtually any sales of PHI will require an authorization, with some limited exceptions (including research and payment for treatment). Unlike the restriction on marketing, any remuneration to the covered entity (in cash or in kind) triggers the requirement for the authorization. The authorization must specify that the covered entity is being compensated for the disclosure.

Hybrid Entities: An entity that has covered entity operations and non-covered entity functions has always had the ability to segregate the covered entity functions and treat the segregated operations as a separate entity for HIPAA compliance. The Omnibus Rule now requires that not only must the covered entity functions be put in the segregated operations, any business associate functions must be placed there as well. The Omnibus Rule also has a good discussion of how an on-site clinic might be part of a hybrid entity or might not be a covered entity at all.

Deceased Patients: Originally, HIPAA protections applied to an individual's PHI forever. The Omnibus Rule now states that, once you've been dead for 50 years, your PHI is no longer subject to HIPAA protections. Also, HIPAA originally prevented a health care provider from communicating with a patient's family members once the patient died. While the patient is alive, friends and family may be "involved in the care" of the individual, and a covered entity may disclose PHI to them, at its discretion, to the extent of their involvement in the individual's care. However, once the patient dies, the friends and family are no longer "involved in the care." The Omnibus Rule allows a provider to continue providing information to friends and family under the same rules that were in place prior to the patient's death.

School Immunization Records: The Omnibus Rule now allows a covered entity to disclose proof of immunization to a school without being required to obtain the written authorization of the individual patient (or his/her parents), if the applicable state requires such information to be given to schools. However, the patient or parents must still give at least verbal approval.

Notices of Privacy Practices: Providers and others who changed their notice of privacy practices ("NoPP") in response to the passage of HITECH might not need to further revise them, unless one of the particular changes to the Omnibus Rule impacts them. Likewise, health plans that made changes in connection with HITECH and (as applicable) the Genetic Information Nondiscrimination Act ("GINA") may not need to further revise their NoPPs. All others will need to review their NoPPs to determine if additional revisions are required.

The "Hide" Rule: The HITECH Act includes a requirement that allows a patient to request that a provider not disclose PHI to the patient's insurance company, as long as the patient pays out of pocket, in full, for the health care services to which the PHI relates; if the patient so requests, the provider must maintain the confidentiality of that PHI. Since the clear intent of this law is to allow a patient to hide information from his or her insurer, I like to call it the "hide" rule. When HHS published the proposed regulations implementing HITECH, they recognized the trouble the Hide rule would cause, and asked for advice on how to deal with it. I don't think they got any. Instead, the Omnibus Rule imposes the obligations on providers. Providers are expected to counsel patients on the unintended consequences and take reasonable steps to obtain payment from the patient before notifying the insurer (on the basis that the patient then didn't pay in full out of pocket). Providers can still make disclosures required by law, but if a provider has a contract with a managed care company that conflicts with the patient's right to hide the information, the patient's rights supersede the terms of the managed care contract. A patient's "hide" rights must also be specified in the provider's NoPP.

The Omnibus Rule is voluminous, and may be subject to further clarification prior to the effective date. However, all entities covered by HIPAA should review their BAAs, NoPPs, and policies and procedures to ensure continued compliance with HIPAA. Any entity that touches PHI should be aware that, if it is a business associate or subcontractor business associate, it is required to comply with the

primary Security Rule provisions relating to administrative, physical and technical safeguards, as well as certain Privacy Rule requirements. That means that the entity must have done a risk analysis and adopted appropriate policies and procedures based on the results of that analysis. Failure to do so is a violation of HIPAA.

For further information on HIPAA and the Omnibus Rule, please contact **Jeff Drummond** at 214.953.5781 or **jdrummond@jw.com**.

---

*If you wish to be added to this e-Alert listing, please **SIGN UP HERE**. If you wish to follow the JW Health Care group on Twitter, please **CLICK HERE**.*

Austin Dallas Fort Worth Houston San Angelo San Antonio Texarkana

JW | JACKSON WALKER L.L.P.

Health e-Alert is published by the law firm of Jackson Walker L.L.P. to inform readers of relevant information in health care law and related areas. It is not intended nor should it be used as a substitute for legal advice or opinion which can be rendered only when related to specific fact situations. For more information, please call 1.866.922.5559 or visit us at **www.jw.com**.

901 Main Street, Suite 6000 | Dallas, Texas 75202