OCR PUBLISHES PROPOSED RULES TO IMPLEMENT HITECH ACT CHANGES TO HIPPA PRIVACY, SECURITY AND ENFORCEMENT RULES

D. Brent Wills, Esq.
Kaufman Gilpin McKenzie Thomas Weiss, P.C.
July 21, 2010

On July 14, 2010, the Department of Health and Human Services (“HHS”) Office of Civil Rights (“OCR”) published in the Federal Register a proposed rule (the “Proposed Rule”) to implement certain changes to the privacy, security and enforcement rules (the “Privacy Rule,” “Security Rule” and “Enforcement Rule,” respectively) under the Health Information Portability and Accountability Act of 1996 (“HIPAA”). OCR issued the Proposed Rule pursuant to the Health Information Technology and Economic and Clinical Health Act of 2009 (“HITECH,” or the “Act”).

The Proposed Rule includes many changes, both minor and substantial, to the HIPAA rules. This Client Alert summarizes a few of the changes most likely to impact our clients.

1. Compliance and Enforcement

Some of the Proposed Rule’s most important provisions deal with the timing of compliance and enforcement with respect to the changes to the Privacy Rule and the Security Rule mandated in the Act, particularly since it is unclear when OCR intends to issue a final rule to implement the changes (the “Final Rule”). For its part, the Proposed Rule provides that, in general, the changes (in whatever final form they take) would take effect 180 days after the effective date of the Final Rule. In addition, under the Proposed Rule, individuals and entities who are parties to business associate agreements in effect (and in compliance with the Privacy Rule) as of the effective date of the Final Rule would not be required to comply with the Final Rule until 18 months thereafter.

2. Business Associates and Subcontractors

As expected, the Proposed Rule extended most of the provisions of the Privacy Rule and the Security Rule to apply directly to business associates. Unexpectedly, however, the Proposed Rule provided that, in addition to business associates, subcontractors of business associates could also be directly liable under the Privacy and Security rules. Business associates, and not

---

1 HITECH became law in February, 2009 as part of the American Recovery and Reinvestment Act (i.e., the “stimulus bill”).
2 Please note that the extended periods for compliance established in the Proposed Rule are not binding on state attorneys general or other agencies authorized to enforce HITECH.
3 The Proposed Rule provides that (i) the definition of “subcontractor” includes any person who acts on behalf of a business associate, other than a member of the business associate’s workforce; and (ii) a business associate’s “workforce” includes employees and other person whose conduct is directly controlled by a business associate.
their HIPAA-covered entities, would be responsible for entering into appropriate business associate agreements with their subcontractors.

Significantly, OCR did not specify whether covered entities and their business associates must amend or enter into new business associate agreements to comply with the HITECH requirement to “incorporate” the changes to the Privacy Rule and the Security Rule imposed by the Act, although the extended deadline for compliance (see above) presumably contemplates that many business associate agreements will need to be renegotiated, otherwise revised, or replaced to comply.

3. Sales of PHI and Using PHI for Marketing and Fundraising Purposes

The Proposed Rule restricts the circumstances in which third parties may sell an individual’s protected health information (“PHI”), or use an individual’s PHI for marketing or fundraising purposes. Among other things, the Proposed Rule would preclude a third party from selling an individual’s PHI without the individual’s consent. In addition, any fundraising communications delivered to an individual that makes use of an individual’s PHI would have to provide the individual with a clear and conspicuous opportunity to opt of receiving future fundraising communications.

4. An Individual’s Rights to His or Her Protected Health Information

Under the Privacy Rule, an individual is currently permitted, in certain circumstances, to request that a covered entity not use or disclose the individual’s PHI to his or her health plan, but the covered entity is not obligated to agree to do so. Under HITECH and the Proposed Rule, if an individual pays a covered entity in full, out of pocket for an item or service, and the individual requests that the covered entity not disclose the transaction to his or her health plan, the covered entity would be precluded from making the disclosure.

In addition, the Proposed Rule would require a covered entity that has an electronic health record with respect to an individual (“EHR”) to provide the individual with an electronic copy of the EHR at his or her request. The Proposed Rule presumes that covered entities will have the ability to deliver electronic PHI by means of online portals, email or portable electronic media.

5. Going Forward

OCR will accept comments regarding the Proposed Rule until September 13, 2010, prior to issuing the Final Rule. OCR solicited comments on numerous provisions in the Proposed Rule, including the provisions relating to subcontractors, whether business associates must notify downstream subcontractors regarding restrictions on disclosures of PHI requested by an individual, and the particular means whereby a covered entity must be able to deliver electronic PHI to an individual.

This Client Alert is provided by Kaufman Gilpin McKenzie Thomas Weiss, P.C. for educational and informational purposes only. It is not intended to constitute legal advice. If you require legal advice, we recommend that you contact appropriate legal counsel.