PUBLICATION

Action Items For HITECH Act Compliance

December 21, 2009

This year has brought about historic and dramatic changes in federal law governing the privacy and security of health care information in the United States. The February 2009 enactment of the Health Information Technology for Economic and Clinical Health (HITECH) Act, which was part of the American Recovery and Reinvestment Act of 2009 (ARRA), created federal notification requirements for security breaches of protected health information (PHI) and added numerous provisions and amendments to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its implementing privacy and security regulations. As the year draws to a close, it is a good time to take stock of the new legal obligations imposed by the HITECH Act and assess your company's compliance status with existing and forthcoming requirements. To help you with these efforts, we are providing a list of some of the "action" items that are important for you to consider.

Action Items

- **By now** , each covered entity should have amended its business associate agreements to establish the rights and responsibilities associated with security breach notification and to require business associate compliance with other parts of the HITECH Act as they become applicable. Many covered entities have also used this opportunity to amend business associate agreements to require specified technologies that meet the breach notification "safe harbor" as discussed in our prior alert on the April 2009 guidance on this issue. Click here for the previous Baker Donelson Alert. Others have also reconsidered certain business issues, such as common law agency issues, indemnification and insurance requirements as a part of their business associate agreement amendments.
- **By now** , covered entities and business associates should have a breach notification policy or should have integrated breach notification requirements into their existing security incident policies to ensure compliance with the HHS Interim Final Breach Rule, which took effect on September 23, 2009. Click here to see Baker Donelson's Breach Notification Alert.

February 17, 2010 is the one-year anniversary of the HITECH Act and with the anniversary comes many of the Act's effective dates for compliance. For instance:

- **By February 17, 2010**, covered entities must comply with an individual's right:
  - to request that a covered entity restrict disclosure of PHI if the disclosure is to a health plan for payment or health care operations and the PHI pertains solely to an item or service for which the health care provider involved has been paid out of pocket in full.
  - to obtain a copy of PHI used or maintained in an electronic health record or request that such copy be transmitted directly to an entity or person designated by the individual.
- **By February 17, 2010**, covered entities and business associates must comply with new minimum necessary requirements. Note, however, that additional guidance on minimum necessary is not due until August 2010. We have been working with clients to modify minimum necessary policies and procedures with the understanding that additional changes may be needed later in 2010.
- **By February 17, 2010**, covered entities must comply with the new marketing and fundraising provisions of the HITECH Act. We expect additional guidance on the marketing and fundraising provisions in the new year. Thus, any amendments to policies and procedures governing marketing

and fundraising should be undertaken with the understanding that additional modifications may be needed.

- **By February 17, 2010**, business associates will need to be in compliance with requirements of the HIPAA Security Rule and with certain Privacy Rule provisions. Among other things, compliance will require business associates to implement full-blown policies and procedures and security measures that are consistent with the Security Rule.
- **By March 1, 2010**, the first annual breach notification report of breaches of unsecured PHI involving less than 500 individuals is due to the Secretary of HHS (the report is due no later than 60 days after the end of the preceding calendar year [March 1, 2010]). Covered entities should be maintaining logs so that they are well prepared to submit this report and to address questions on whether they have taken any corrective actions and mitigation on any breaches which are reported.

More Agency Guidance Expected

Prior to December 31, and possibly even before Christmas, we expect several rules to be issued, including the initial set of standards on Health Insurance Exchanges (HIEs); electronic health record (EHR) certification; and privacy and health information technology privacy issues considered by the HIT Policy Committee. The effects will likely be limited to HIEs and those with or considering EHRs; however, the manner in which those issues are considered within the HIT Policy Committee could certainly have a ripple effect on the privacy and security practices of all covered entities and business associates.

In addition, the coming year promises to continue to be an active one for legal changes in the areas of privacy and security. Additional rules and guidance are expected relative to minimum necessary standards (including the use of limited data sets), marketing, fundraising, de-identification, and restrictions on certain disclosures and sales of PHI. More significantly, the U.S. Department of Health and Human Services is required to initiate compliance audits and has been hiring staff aimed at preparing for these audits. State attorneys general have already initiated some high profile investigations related to breaches that should continue to garner media attention.

If you have questions about compliance with the HITECH Act, contact your Baker Donelson attorney.