HDJN
The health law solution.

CLIENT ADVISORY

January 31, 2013

New HIPAA Regulations Require Updates to Policies, Procedures, Business Associate Agreements and Notice of Privacy Practices

On January 25, 2013, the Department of Health and Human Services published final regulations under HIPAA, the HITECH Act and the Genetic Information Non-discrimination Act ("GINA"). These regulations will require nearly all covered entities to adopt changes to their notice of privacy practices, their policies and procedures and their business associate agreements.

What Changes Will Have the Biggest Impact on Health Care Providers?

The regulations include a number of changes that will impact most health care providers. All providers should review current policies and procedures and update those to reflect new language and standards under the regulations. Among the specific actions that will be required for most health care providers are:

Updates to Notice of Privacy Practices – The regulations will require that the notice of privacy practices specifically reference the ability of a patient to opt out of fundraising communications. The notice of privacy practices must also specifically address a patient's right to restrict disclosures to health plans for payment and health care operations of the health plan, where the patient has paid out-of-pocket in full for the services. The regulations also require that the notice of privacy practices be updated to include a statement regarding the duty of the health care provider to notify the patient in the event of a breach of the patient's protected health information.

Breach Notification – The prior federal regulations only required health care providers to notify patients of a breach of their PHI where there was a significant risk of financial, reputational or other harm. The new regulations modify this standard to require notification of a breach unless the provider demonstrates that there is a low probability "that the protected health information has been compromised based on a risk assessment". The risk assessment must include an analysis of several specific factors. The changes to the regulations will impact breach notification decisions for some providers, but nearly all providers will need to modify their breach notification policies to reflect these new standards.

Business Associate Agreements – The regulations include several new provisions that can impact business associate agreements, depending upon what terms are included in a provider's current agreement. Each provider should review its template/model business associate agreement for compliance with the new regulations. The template should be updated to reflect the new standards, and any existing business associate agreements that do not meet the new standard should be updated. The new regulations also include revisions that may require providers to establish new business associate agreements with vendors that store PHI, even if the vendor is not expected to access, use or disclose the PHI. Additional guidance on this issue is expected by March 26, 2013.

PHI of Decedents – The regulations include changes to allow providers to disclose information after a patient's death to family members and other individuals who were involved in the patient's care or payment for care prior to the patient's death. These changes offer health care providers opportunities to share additional information following a patient's death, and providers who want to allow staff to exercise that flexibility should update their policies and procedures to reflect these changes.

Research – For providers involved in research, the new regulations include changes that will allow use of a single authorization for disclosures for multiple research activities. Providers involved in research should update their policies, procedures and research-related authorization forms to benefit from these changes.

Disclosure of Immunization Records – The new regulations facilitate disclosures of immunization records by a health care provider to schools. Under the new standards, subject to state law, providers will be permitted to disclose proof of immunizations for a student or prospective student directly to a school without a written authorization if the school is required by law to maintain the information and an appropriate person agrees to the disclosure. In the case of an unemancipated minor, the appropriate person would be a parent, guardian or other person acting in loco parentis, and in other cases, the appropriate person will typically be the patient. Providers are required to document the agreement, but a formal authorization form will not typically be required. For health care providers who want to avoid requiring formal authorizations, the provider should update policies and procedures to reflect the new regulations.

When Are These Changes Effective?

The new regulations become effective March 26, 2013. The compliance date (i.e., the date by which providers will need to update policies, procedures, and other materials) is September 23, 2013. For business associate agreements in place before January 25, 2013, if the arrangement is not modified or renewed between March 26, 2013 and September 23, 2013, providers will have until the earlier of the first renewal or modification date for the arrangement or September 22, 2014 to update the business associate agreement. For any arrangements modified or renewed after March 26, 2013, the business associate agreement must be updated as necessary to comply with the new standards. Providers should review template/model business associate agreements as soon as possible, however, because any arrangements renewed or modified after March 26, 2013 will need to meet the new standards at the time of the renewal or update.

What Should Providers Do?

As outlined above, providers should begin reviewing their policies, procedures, business associate agreements and notice of privacy practices as soon as possible, in order to identify and complete required updates. Enforcement activities have increased significantly under HIPAA recently and providers are advised to be diligent in addressing these new standards. If the Office for Civil Rights continues efforts on HIPAA compliance audits after the compliance date, providers may be required to demonstrate compliance with these new standards even if there have been no breaches or complaints involving the provider. With these recent changes, this can also be a good time for an overall assessment of a provider's operational practices and documents to ensure regulatory compliance.

If you have questions, for assistance in revising policies, procedures and documents to meet these new standards, or for help with a compliance assessment relating to HIPAA practices, please contact Bill Hall or Mark Watson at (866)967-9604, or by email at bhall@hdjn.com or mwatson@hdjn.com. Additional information about Hancock, Daniel, Johnson & Nagle, P.C. is available on the firm's website at www.hdjn.com.