HEALTHCARE

THE HIPAA "OMNIBUS" FINAL RULE PART II – REVISIONS TO BUSINESS ASSOCIATE DEFINITION, LIABILITY AND OBLIGATIONS, CERTAIN INDIVIDUAL RIGHTS, AND IMPLEMENTATION OF GINA.

by Cynthia Moore, Brian R. Balow and Rodney Butler

The United States Department of Health and Human Services (the "Department" or "HHS") issued the "Omnibus" Final Rule (the "Final Rule") on January 17th, 2013. The Final Rule contains long-awaited rules and clarifications regarding the Health Insurance Portability and Accountability Act ("HIPAA") Privacy, Security and Enforcement Rules and the Health Information Technology for Economic and Clinical Health Act ("HITECH Act"). **Most of the provisions of the Final Rule are effective September 23, 2013.**

This Alert is the second part to our informative summaries of the major changes resulting from the Final Rule. You may obtain a copy of Part I, which summarized revisions resulting from the Final Rule to the breach notification rule, notice of privacy practices, and marketing and fundraising communications, at http://www.dickinson-wright.com/The-HIPAA-Omnibus-Final-Rule-01-29-2013.

Also, don't forget to "follow" our blog to receive notifications of new posts in the future: http://www.dwhealthlawblog.com/.

Expansion of the definition of a "Business Associate"

Under the HIPAA Privacy Rule, a "business associate" was defined to generally mean a person who performed functions, activities or particular services on behalf of a covered entity which involved the use or disclosure of protected health information (PHI). Consistent with changes made by the HITECH Act, the Final Rule provides that the term "business associate" is expanded to include Health Information Organizations, E-prescribing Gateways or other persons that will provide data transmission services of PHI to a covered entity that will need routine access to PHI, and persons who offer personal health records to one or more individuals on behalf of a covered entity.

Significantly, the Final Rule also expands the term "business associate" to include a subcontractor of a business associate who "creates, receives, maintains, or transmits" PHI on behalf of a covered entity. A "subcontractor" is defined as "a person to whom a business associate delegates a function, activity, or service other than in the capacity of a member of the workforce of such business associate."

Part and parcel of the conceptual changes, clarified and expanded definitions of the terms "business associate" and "subcontractors" will be the expansion of liability to those groups for specific provisions of the Privacy and Security Rules.

Expansion of Business Associate Liability

Although the HITECH Act creates direct liability for impermissible uses and disclosures of PHI by a business associate in certain situations, it does not create direct liability for business associates with regard to compliance with all requirements under the Privacy Rule (i.e., it does not treat them as covered entities).

However, the Final Rule will expand a business associate's direct liability for impermissible uses and disclosures of PHI where:

- Uses and disclosures of PHI are not in accord with its business associate agreement or the Privacy Rule;
- There is a failure to provide breach notification to the covered entity;
- A failure to provide an accounting of disclosures occurs;
- There is a failure to comply with the requirements of the HIPAA Security Rule;
- A disclosure is not made of PHI when required by HHS to do so for HHS to investigate and determine the business associate's compliance with the HIPAA Privacy and Security Rules;
- There is a failure to disclose PHI to the covered entity, individual, or individual's designee, as necessary, to satisfy a covered entity's obligations with respect to an individual's request for an electronic copy of PHI;
- A failure to make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request occurs; and
- A business associate fails to enter into business associate agreements with subcontractors that create or receive PHI on their behalf.

In addition, the Final Rule implements the HITECH Act providing that the HIPAA Security Rule's administrative, physical, and technical safeguards requirements, as well as the Rule's policies and procedures and documentation requirements apply to business associates in the same manner as these requirements apply to covered entities, and that business associates are civilly and criminally liable for violations of these provisions. While HHS recognized that there may be concern over the costs to business associates of compliance with the Security Rule, it did not agree with the materiality of those costs since it determined that previous rules had "effectively" imposed these same requirements and consequently, business associates and subcontractors should already have in place compliant security practices, any revisions that need to be made would only be "modest improvements."

HHS also recognized that certain smaller or less sophisticated business associates that access electronic PHI "may not have engaged in the formal administrative safeguards such as having performed a risk analysis, established a risk management program, or designated a security official, and may not have written policies and procedures, conducted employee training, or documented compliance as the statute and these regulations would now require." To mitigate this concern, HHS points to the availability of an estimate for compliance costs as well the resources available on OCR's website.

Changes to Business Associate Agreements

A covered entity will be permitted to disclose PHI to a business associate and will allow a business associate to create, receive, maintain, or transmit PHI on its behalf, if the covered entity obtains satisfactory assurances in the form of a written contract or other written arrangement with the business associate, that the business associate will appropriately safeguard the information and protect PHI.

HHS added a new parallel provision which allows a business associate to disclose PHI to a subcontractor. This provision allows the subcontractor to create, receive, maintain, or transmit PHI on behalf of a business associate, if the business associate obtains similar satisfactory assurances that the subcontractor will appropriately safeguard the information. Further, if the subcontractor creates, receives, maintains, or transmits electronic PHI, it must agree to comply with the Security Rule. HHS made clear in the Final Rule that a covered entity is not required to obtain satisfactory assurances from business associates that are subcontractors; rather, a business associate is required to obtain those assurances from the subcontractor.

The Final Rule do not change the parties to the contracts. For example, a covered entity may contract with a business associate (contractor) to use or disclose PHI on its behalf. The business associate may then obtain the services of, and exchange PHI with, a subcontractor (subcontractor 1), and that subcontractor may, in turn, contract with another subcontractor (subcontractor 2) for services involving PHI. The contractor and subcontractors 1 and 2 would now be defined as business associates who would have direct liability under the Privacy Rule, and who would be required to obtain business associate agreements with the parties with whom they contract for services that involve access to PHI. Note, however, that with respect to the definition of "business associate," direct liability under the Privacy Rule would attach regardless of whether the contractor and subcontractors have entered into the required business associate agreements.

Among other amendments to the rules governing business associate agreements are the following:

- HHS modified some of the specific business associate agreement provisions to provide that the agreement must require that: (1) business associates comply, where applicable, with the HIPAA Security Rule with regard to electronic PHI; (2) business associates report breaches of unsecured PHI to covered entities; and (3) business associates ensure that any subcontractors that create or receive PHI on behalf of the business associate agree to the same restrictions and conditions that apply to the business associate with respect to such information.

- A new agreement provision was added requiring that, to the extent a business associate is to carry out a covered entity's obligations, the business associate must comply with the requirements of the Privacy Rule that applies to the covered entity in the performance of such obligations. Therefore, when a covered entity delegates a responsibility under the Privacy Rule to the business associate, the business associate is contractually required to comply with the requirements of the Privacy Rule in the same manner as they apply to the covered entity. However, if the covered entity does not delegate any of its responsibilities under the Privacy Rule to the business associate, then this provision would not be applicable, and the parties would not be required to include such language. As an example, if a third party administrator, as a business associate of a group health plan fails to distribute the plan's notice of privacy practices to participants on a timely basis, the third party administrator would not be directly liable under HIPAA Rules, but would be contractually liable, for the failure. Nevertheless, even though the business associate is not directly liable under the HIPAA Rules for failure to provide the notice, the covered entity remains directly liable for the failure to provide the individuals with its notice of privacy practices because it is the covered entity's ultimate responsibility to do so despite its having hired a business associate to perform the function.

- If only a limited dataset is released to a business associate for a health care operations purpose, then a data use agreement suffices and a business associate agreement is not necessary. To make this clear, HHS added a new provision which recognizes that a data use agreement may qualify as a business associate's satisfactory assurance that it will appropriately safeguard the covered entity's PHI when the PHI disclosed for a health care operations purpose is a limited data set.

HHS has made available an updated model business associate agreement, which is posted on its website.

Under the transition provisions of the Final Rule, business associate contracts or other written agreements which were in existence at the time of the publication of the modified Privacy Rule may continue to be used until September 23, 2014, if the pre-existing contract or other written agreement (with a business associate or subcontractor) complied with the prior provisions of the Privacy and Security Rules and the contract will not be renewed or modified between March 26, 2013 and September 23, 2013. These transition provisions apply only to the requirement to amend business associate contracts; they do not affect the effective date of any compliance obligations under the Privacy and Security Rules.

Right to Request a Restriction of Uses and Disclosures

Prior to amendment by the HITECH Act, a covered entity was not required to grant an individual's request to restrict disclosure of his or her PHI. The Final Rule implements the HITECH Act by requiring a covered entity to agree to a request by an individual to restrict the disclosure of PHI about the individual to a health plan if:

- the disclosure is for payment or health care operations and is not otherwise *required by law*; and

- the PHI relates solely to a health care item or service for which the individual has paid the covered entity in full.

Covered entities are not required to create separate medical records or otherwise segregate a restricted health care item or service, but should "flag" the restricted item so that it is not inadvertently sent to a health plan.

The Preamble to the Final Rule provides helpful clarification of how the "required by law" exception operates. If a provider is required by state or other law to submit a claim to a health plan and there is no exception for an individual to pay out of pocket, then disclosure is required by law and the individual does not have the right to request a restriction of disclosure to the health plan. With regard to Medicare, which is generally subject to a mandatory claim submission rule, if a beneficiary requests a restriction and pays for the service out of pocket, the provider must agree to the restriction on disclosure as the payment amounts to a refusal to authorize the submission of a bill to Medicare for the service.

Access of Individuals to Protected Health Information

The Final Rule implements the change made by the HITECH Act which requires a covered entity to allow an individual to access an electronic health record (EHR) in electronic format. The Final Rule extends this right to any PHI maintained in electronic format in a designated record set, which must be provided to the individual in the form and format requested by the individual if it is readily producible. If the electronic information is not readily producible, then it must be provided in a readable electronic form and format as agreed to by the covered entity and the individual.

The reasonable cost-based fee that may be charged for accessing PHI may include labor for copying PHI and the cost of supplies for creating the paper copy or electronic media if the individual requests that the electronic copy be provided on portable media (such as a CD or flash drive). A retrieval fee may not be charged.

Access must generally be provided within 30 days of the request. A covered entity is allowed one 30 day extension, with written notice to the individual of the reasons for delay and the expected date on which access will be provided. Covered entities are encouraged to provide access sooner if allowed by technology.

The Genetic Information Nondiscrimination Act

The Final Rule implements changes made by the Genetic Information Nondiscrimination Act of 2008 ("GINA"). Section 105 of GINA requires the Department to clarify that genetic information is health information, and prohibits group health plans, health insurance issuers and issuers of Medicare supplemental policies from using or disclosing genetic information for underwriting purposes.

The Final Rule revises the definition of health information to explicitly state that health information includes genetic information. This change is consistent with a longstanding interpretation of the Department.

The Final Rule also adds applicable definitions from GINA, including genetic information, genetic services and genetic tests. "Genetic information" generally means (1) an individual's genetic tests, (2) the genetic tests of an individual's family members, (3) the manifestation of a disease or disorder in an individual's family members (i.e., family medical history), or (4) any request for, or receipt of, genetic services. A "genetic test" is an analysis of human DNA, RNA, chromosomes, proteins or metabolites that detects genotypes, mutations or chromosomal changes. "Genetic services" means (1) a genetic test, (2) genetic counseling or (3) genetic education.

The Final Rule clarifies that information about manifested diseases or disorders of the individual, or conditions or medical tests of the individual that do not meet the definition of "genetic test", such as an HIV test, complete blood count, or cholesterol or liver function test, are not genetic information and may be used or disclosed for underwriting purposes.

As noted above, GINA prohibits only certain types of health plans from using genetic information for underwriting purposes. The Final Rule expands the types of health plans to which the prohibition applies to include all of the health plans covered by the Privacy Rule other than issuers of long-term care policies.

The Final Rule defines "underwriting purposes" to mean:

- Rules for eligibility or benefits under the health plan;
- The determination of premium or contribution amounts under the health plan;
- The application of any pre-existing condition exclusion under the health plan; and
- Other activities related to the creation, renewal or replacement of a contract of health insurance or health benefits.

However, "underwriting purposes" does not include determinations of medical appropriateness where an individual seeks a benefit under the plan, if genetic information is relevant to the coverage decision.

If a health plan performs underwriting, it must revise its Notice of Privacy Practices ("NPP") to include a statement that it will not use or disclose genetic information for underwriting purposes. A health plan that does not perform underwriting is not required to revise its NPP.

This Client Alert is published by Dickinson Wright PLLC to inform our clients and friends of important developments in the field of healthcare law. The content is informational only and does not constitute legal or professional advice. We encourage you to consult a Dickinson Wright attorney if you have specific questions or concerns relating to any of the topics covered in here.

FOR MORE INFORMATION CONTACT:

Cynthia A. Moore, is a member and practice department manager in Dickinson Wright's Troy office. She can be reached at 248.433.7295 or cmoore@dickinsonwright. com.

Brian R. Balow, is a member in Dickinson Wright's Troy office. He can be reached at 248.433.7536.

Rodney D. Butler is an Associate in Dickinson Wright's Nashville office. He can be reached at 615.255.6538 or rbutler@dickinsonwright.com.