HEALTHCARE

THE HIPAA "OMNIBUS" FINAL RULE PART I – REVISIONS TO THE RULES ON BREACH NOTIFICATION; NOTICE OF PRIVACY PRACTICES; AND MARKETING AND FUNDRAISING COMMUNICATIONS.

by Rose J. Willis, Deborah L. Grace and Randolph F. Pistor

The United States Department of Health and Human Services (the "Department") 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 first of our summaries of the major aspects of the Final Rule. Forthcoming future alerts will summarize changes made by the Final Rule to the HIPAA Security Rule, business associate obligations, and business associate agreements, among other major provisions. We will post more in depth reviews of these significant changes in our DW Health Law Blog located at http://www.dwhealthlawblog.com/ - you may want to "follow" our blog to receive notifications of new posts.

Revisions to the Rules on Breach Notification.

The Final Rule significantly modified the HIPAA/HITECH Act breach notification rules relating to the procedures that covered entities or business associates, as applicable, must take when determining whether a breach of unsecured protected health information ("PHI") requires notification to affected individuals, the Secretary of the Department or the media.

Under the Final Rule there is now a presumption that an impermissible use or disclosure of PHI is a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised. The shift to this presumption represents a significant burden on covered entities and business associates, and as a result covered entities and business associates, as applicable, will need to document in a detailed and comprehensive fashion their risk assessment review and conclusion regarding impermissible uses or disclosures of unsecured PHI, *even if they ultimately determine that the use or disclosure was not a breach.*

The new "low probability" standard replaces the previous "harm standard" that was set forth in the Interim Final Rule (issued by the Department October 30, 2009) (the "IFR"), representing a more objective approach to the determination of whether a breach has occurred. Under the Final Rule, a covered entity's determination of whether there is a "low probability" that PHI was compromised must address, at the least, the following four factors:

- The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
- The unauthorized person who used the PHI or to whom the disclosure was made;
- Whether the PHI was actually acquired or viewed;
- The extent to which the risk to the PHI has been mitigated.

Further, after addressing each of the above stated factors, the covered entity or business associate must evaluate the overall probability that the PHI was compromised by considering all factors in combination. The Department clarified that a covered entity or business associate may choose to automatically provide the required notification following an impermissible use or disclosure of PHI without performing a risk assessment to determine if one is necessary.

The Final Rule also removed the exception to the breach notification rule that was applicable to "limited data sets" which was previously issued in the IFR. Under that exception, an impermissible use or disclosure of PHI that qualified as a limited data set but excluded dates of birth and zip codes, was not considered a "breach." Now, even in those cases the covered entity will need to conduct a risk assessment using the above-described criteria to determine whether a breach occurred.

The Final Rule addressed and clarified a number of detailed questions raised by commenters. For example, it clarified that uses or disclosures that impermissibly involve more than the minimum necessary information may qualify as breaches, even though such information if disclosed to a business associate or as an internal use within a covered entity or business associate, may have a low probability that the PHI was compromised since the information was not acquired by a third party. Further, the Department declined to in the following situation provide an explicit exception to the definition of "breach": in the event a laptop is lost and recovered and a forensic analysis shows that the PHI on the computer was not accessed (instead the covered entity would need to go through its risk assessment and may determine that as a result there is a low probability that the PHI was compromised). The Department noted that if a computer is lost or stolen, it is not reasonable to delay breach notification based on the hope that it will be recovered.

As a result of the new "low probability" standard, covered entities and business associates will need to examine and revise their breach notification policies and procedures prior to the September 23, 2013 effective date.

Revisions to the Notice of Privacy Practices ("NPP").

The Privacy Rule prescribes certain information that must be included in a covered entity's NPP, including a statement advising individuals that any use or disclosure of PHI other than those permitted by the Privacy Rule will be made only with written authorization of the individual, and that the individual has the right to revoke an authorization. The Final Rule expands a covered entity's disclosure obligations by requiring that the NPP specifically state that uses and disclosures of PHI for marketing purposes and the sale of PHI require an individual's written authorization. Also, if the covered entity records or maintains psychotherapy notes, then its NPP must include a statement that uses and disclosures of psychotherapy notes require an individual's written authorization.

Besides the specific disclosures regarding written authorization, the Final

Rule requires that a covered entity that intends to contact an individual for fundraising purposes to disclose in its NPP that it may contact the individual to raise funds, and that the individual has the right to opt out of receiving such communications. If the covered entity is a health plan and it uses or discloses PHI for underwriting purposes, then its NPP must state that the covered entity is prohibited from using or disclosing genetic information for such purposes. All covered entities must include in their NPP a statement of the right of affected individuals to be notified following a breach of unsecured PHI. Finally, for a covered entity other than a group health plan, the NPP must inform individuals of their right to restrict certain disclosures of PHI to a health plan where the individual pays out of pocket in full for the health care item or service.

The Department has determined that these changes are material, and each covered entity must take certain actions to advise the individual of the change in the NPP and make available the revised NPPs. If the covered entity is a group health plan that currently posts its NPP on its website, then it must prominently post information about the material changes or its revised NPP on its website by the compliance date, September 23, 2013, and it must provide the revised NPP or information about the material changes and how to obtain the revised NPP in its next annual mailing to the individuals covered by the plan or during the next open enrollment period. Group health plans that do not maintain customer service websites must provide the revised NPP or information describing the material changes and how to obtain the revised NPP to individuals covered by the plan within 60 days of the compliance date.

Marketing and Fundraising Communcations

Disclosures of PHI for "Marketing" Purposes.

The HIPAA Privacy Rule, at 45 C.F.R. § 164.508(a)(3) (the "Privacy Rule"), requires that covered entities obtain a valid authorization from individuals before using or disclosing PHI to "market" a product or service. The term "marketing" means "to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service" and generally excepts communications for treatment and health care operations purposes from this definition. The Final Rule's changes to the definition of "marketing" concern its exceptions, which are now dependent upon the "financial remuneration" received, if any.

The new definition specifies that "marketing" does not include a communication made to provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for the individual, but only if any financial remuneration received by the covered entity in exchange for making the communication is reasonably related to the covered entity's cost of making the communication. Falling within this exception are communications about the generic equivalent of a drug being prescribed to an individual as well as adherence communications encouraging individuals to take their prescribed medication as directed. Where an individual is prescribed a self-administered drug or biologic, communications regarding all aspects of a drug delivery system, including, for example, an insulin pump, also fall under this exception. The Department intends to provide future guidance to address the scope of this exception.

Additionally, the definition of "marketing" does not include a communication made for the following treatment and health care operations purposes, except where the covered entity receives financial remuneration in exchange for making the communication:

- For treatment of an individual by a health care provider, including case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual;
- To describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication, including communications about: the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits; or
- For case management or care coordination, contacting of individuals with information about treatment alternatives, and related functions to the extent these activities do not fall within the definition of treatment.

The Privacy Rule defines "financial remuneration" to mean "direct or indirect payment from or on behalf of a third party whose product or service is being described." The definition clarifies that "direct or indirect payment" does not include any payment for treatment of an individual. However, the term "financial remuneration" does not include non-financial benefits, such as in-kind benefits, provided to a covered entity in exchange for making a communication about a product or service. Rather, financial remuneration includes only payments made in exchange for making such communications. In addition, the financial remuneration a covered entity receives from a third party must be for the purpose of making a communication and such communication must encourage individuals to purchase or use the third party's product or service. If the financial remuneration received by the covered entity is for any purpose other than for making the communication, then this marketing provision does not apply.

Finally, permissible costs for which a covered entity may receive remuneration under this exception are those which cover only the costs of labor, supplies, and postage to make the communication. Where the financial remuneration a covered entity receives in exchange for making the communication generates a profit or includes payment for other costs, such financial remuneration would run afoul of the HITECH Act's "reasonable in amount" language.

Combining the new definition of "marketing" with the Privacy Rule's authorization requirement, it follows that for marketing communications that involve financial remuneration, the covered entity must obtain a valid authorization from the individual before using or disclosing PHI for such purposes, and such authorization must disclose the fact that the covered entity is receiving financial remuneration from a third party. Additionally, where a business associate (including a subcontractor), as opposed to the covered entity itself, receives financial remuneration from a third party in exchange for making a communication about a product or service, such communication also requires prior authorization from the individual.

Disclosures of PHI for "Fundraising" Purposes.

The Final Rule amended the fundraising provisions of the Privacy Rule, significantly expanding the PHI that may be used for fundraising purposes to include:

- Demographic information relating to the individual, including name, address, other contact information, age, gender, and date of birth;
- Dates of health care provided to the individual;
- Department of service information, which includes information about the general department of treatment (e.g., cardiology, oncology, pediatrics, etc.);
- Treating physician;
- Outcome information, including information regarding the death of the patient or any sub-optimal result of treatment or services; and
- Health insurance status.

Of course, a covered entity must still apply the minimum necessary standard to ensure that only the minimum amount of PHI necessary to accomplish the intended purpose is used or disclosed.

Concurrent with this expansion in PHI that may be disclosed, the Final Rule expanded upon the requirements of a covered entity that uses PHI for fundraising purposes. Previously, a covered entity that planned to use or disclose PHI for fundraising was required to (1) inform individuals in its notice of privacy practices that it might contact them to raise funds for the covered entity (as discussed in the following section), (2) include in any fundraising materials it sent to an individual a description of how the individual may opt out of receiving future fundraising communications, and (3) make "reasonable efforts" to ensure that individuals who did opt out were not sent future fundraising communications. Now, under the Final Rule, covered entities that use or disclose PHI for fundraising purposes are subject to the following requirements:

- PHI may not be used or disclosed for fundraising purposes unless the covered entity informs individuals in its notice of privacy practices that it might contact them to raise funds and that they have a right to opt out of receiving such communications (as discussed in the following section). Covered entities are not required to send pre-solicitation opt outs to individuals prior to the first fundraising communication.
- With each fundraising communication made to an individual, whether made in writing or over the phone, the covered entity must provide the individual with a clear and conspicuous opportunity to elect not to receive any further fundraising communications.
- Covered entities are free to provide individuals with the choice of opting out of all future fundraising communications or just campaign-specific communications. Whatever method is employed, the communication should clearly inform individuals of their options and any consequences of electing to opt out of further fundraising communications.
- The method for an individual to elect not to receive further fundraising communications may not cause the individual to incur an undue burden or more than a nominal cost. The Department encourages covered entities to consider the use of a toll-free phone number, an e-mail address, or similar opt out mechanism that would provide individuals with a simple, quick, and inexpensive way to opt out of receiving future communications, as requiring individuals to write a letter to opt out constitutes an undue burden.
- Covered entities may employ multiple opt out methods, allowing individuals to determine which opt out method is the simplest and most convenient for them, or a single method that is reasonably accessible to all individuals wishing to opt out. Requiring that individuals opt out of further fundraising communications by simply mailing a pre-printed, pre-paid postcard would not constitute an undue burden under the Final Rule and is an appropriate alternative to the use of a phone number or e-mail address.
- A covered entity may choose to provide individuals with the opportunity to select their preferred method for receiving fundraising communications. If an individual elects to opt out of future fundraising communications, then the opt out is effective for all forms of fundraising communications and the individual must be removed from all such lists.
- The covered entity may not condition treatment or payment on the individual's choice with respect to the receipt of fundraising communications.

The covered entity may not make fundraising communications to an individual where the individual has elected not to receive such communications. However, the covered entity may provide an individual who has elected not to receive further fundraising communications with a method to opt back in to receive such communications.

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:

Rose J. Willis is Of Counsel in Dickinson Wright's Troy office. Willis is a member of the healthcare group and can be reached at 248.433.7584 or rwillis@dickinsonwright.com.

Deborah L. Grace is a Member in Dickinson Wright's Troy office. Grace is a member of the employee benefits group and can be reached at 248.433.7217 or dgrace@dickinsonwright.com.