February 12, 2013

On January 17, 2013, the U.S. Department of Health and Human Services ("HHS") issued a final rule ("Omnibus Rule")[1] affecting multiple aspects of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). The Omnibus Rule becomes effective on March 26, 2013, and HIPAA covered entities and business associates must comply with its requirements by September 23, 2013 (the "Compliance Date"), which is 180 days beyond the Omnibus Rule's effective date.

The Omnibus Rule, commonly referred to by this name because of its sweeping scope, is comprised of four final rules that:

- modify aspects of HIPAA and its implementing regulations including the privacy standards located at 45 C.F.R. parts 160 and 164, subparts A and E (the "Privacy Rule"), the security standards located at 45 C.F.R. parts 160, 162 and 164, subpart C (the "Security Rule"), and enforcement standards located at 45 CFR part 160, subparts C, D, and E (the "Enforcement Rule");
- implement statutory amendments, including an increased and tiered civil money penalty structure, under the Health Information Technology for Economic and Clinical Health Act ("HITECH");
- modify the interim final rule for Breach Notification for Unsecured Protected Health Information located at 45 C.F.R. part 164, subpart D (the "Breach Notification Rule"), including replacing its harm threshold for breach notification requirements with a default presumption that an acquisition, access, use, or disclosure of PHI that violates the Privacy Rule is a breach, and supplant the Breach Notification Rule as of the Compliance Date (covered entities and business associates must continue to comply with the interim rule in the meantime); and
- modify the HIPAA Privacy Rule by implementing section 105 of Title I of the Genetic Information Nondiscrimination Act of 2008 ("GINA"), clarify that genetic information is health information, and prohibit health plans, including group health plans, health insurance issuers (including HMOs), and issuers of Medicare supplemental policies, from using or disclosing genetic information for underwriting purposes.

This client alert refers to the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules collectively as the "HIPAA Rules."

Application of the HIPAA Rules to business associates and subcontractors

The Omnibus Rule reflects the new post-HITECH reality that business associates (and any subcontractors *ad infinitum* who have access to protected health information ("PHI")) are directly regulated by the HHS Office of Civil Rights ("OCR"). Business associates must comply with the requirements of the Security Rule, in accordance with HITECH, as well as certain requirements of the Privacy Rule. Specifically, under the Privacy Rule, business associates, among other things:

- may use and disclose PHI only as permitted or required by their business associate agreements or as required by law;
- are expressly prohibited from using or disclosing PHI in a manner that would violate the Privacy Rule if done by a covered entity;
- are expressly required to use, request, or disclose only the minimum PHI necessary;
- must also disclose PHI (i) when required by the Secretary for investigation or determining compliance with the Privacy Rule, and (ii) to a covered entity or an individual in order to satisfy the covered entity's obligations with respect to an individual's request for an electronic copy of PHI; and
- are required to take reasonable steps to cure a subcontractor's breach or end a subcontractor's violation of the subcontractor's

obligations under its contract or arrangement with the business associate and to terminate the contract or arrangement if the business associate's steps are unsuccessful.

Updated definition of business associates

The Omnibus Rule expands the definition of "business associate" to include entities that transmit and need routine access to PHI (e.g., Health Information Organizations, E-Prescribing Gateways); vendors of personal health records who serve covered entities; subcontractors who create, receive, maintain or transmit PHI on behalf of business associates; and entities that, on behalf of a covered entity or organized health care arrangement ("OHCA") handle PHI for patient safety activities carried out by or on behalf of a Patient Safety Organization or a health care provider.

The following are excluded from the "business associate" definition: a health care provider who receives PHI from a covered entity for treatment purposes; a plan sponsor with respect to disclosures by a group health plans ("GHP") where general GHP requirements are met; a government agency for purposes of determining government health plan eligibility or enrollment in plan administered by another government agency; and a covered entity participating in an OCHA.

Notably, the commentary to the Omnibus Rule clarifies that the "conduit" exception previously articulated by OCR is limited such that the only conduits that are not business associates are those providing transmission services (whether digital or hard copy), including any temporary storage of transmitted data incident to such transmission. The duration, frequency, and persistent nature of handling of PHI is determinative. Thus, If an entity maintains PHI on more than a temporary basis on behalf of a covered entity (e.g., a data storage company), it is a business associate and not a conduit, even if the entity does not actually view the PHI.

Updated business associate agreement requirements for business associates and subcontractors

The HIPAA Rules previously provided that a covered entity may permit a business associate to create, receive, maintain, or transmit PHI or electronic PHI on the covered entity's behalf only if the covered entity obtains satisfactory assurances that the business associate will appropriately safeguard the information. Such satisfactory assurances must be documented in the form of a written contract—namely, a business associate agreement—or other arrangement. The Omnibus Rule adds that business associates must obtain such satisfactory assurances from their subcontractors (who must obtain the same satisfactory assurances from their subcontractors). However, covered entities are not required to obtain such satisfactory assurances from subcontractors.

Pursuant to the Omnibus Rule, business associate agreements between a covered entity and business associate must now provide, among existing requirements, that a business associate will:

- Comply with the Security Rule with respect to electronic protected health information;
- Report to the covered entity any breach of unsecured protected health information as required by § 164.410;
- Ensure that subcontractors agree to the same restrictions and conditions that apply to the business associate with respect to PHI created, maintained, or transmitted on behalf of the business associate; and
- To the extent that a business associate carries out a covered entity's obligation under the Privacy Rule, comply with the Privacy Rule requirements applicable to the covered entity in the performance of such obligation.

Further, all required elements of business associate agreements apply to contracts or arrangements between business associates and subcontractors.

Application of compliance and enforcement provisions to business associates

Because business associates are directly regulated by OCR, they are subject to compliance and enforcement by the HHS Secretary (the "Secretary"). Accordingly, the Secretary may receive, and persons have a right to file, complaints that a business associate is not complying with HIPAA's administrative simplification provisions, and the Secretary may, and if facts suggest a possible violation due to willful neglect "will": (i) investigate complaints filed against a business associate or (ii) conduct a compliance review to determine whether a business associate is complying with administrative simplification provisions. An investigation by the Secretary may include a review of policies and procedures and the circumstances of any alleged violation, and business associates must: (i) keep records and submit compliance reports as the Secretary deems necessary to determine business associates' compliance with administrative simplification provisions and (ii) comply with the Secretary's complaint investigations and compliance reviews, including by providing the Secretary access to their facilities.

Furthermore, business associates are now subject to civil monetary penalties for violations of HIPAA's administrative simplification provisions. To the extent that multiple covered entities and/or business associates have violated these provisions, the Secretary may impose civil monetary penalties against each violator. Liability attaches, in accordance with the federal common law of agency, to a covered entity for violations by its business associates and their subcontractors and to a business associate for violations by its subcontractors.

Updated civil monetary penalties provisions

Effective March 26, 2013, the Omnibus Rule updates the factors, both mitigating and aggravating, that the Secretary considers when determining the amount of a civil monetary penalty. The Secretary will apply these factors within a tiered structure of penalties depending on the violator's knowledge and willfulness. Broadly speaking, these factors include the nature and extent of the violation and the nature and extent of the harm resulting from the violation. More specifically, these include:

Nature and extent of the violation

- The number of individuals affected; and
- The time period during which the violation occurred.

Nature and extent of the harm resulting from the violation

- Whether the violation caused physical, financial, or reputational harm;
- Whether the violation hindered an individual's ability to obtain health care;
- The history of prior compliance with the administrative simplification provisions, including violations; and
- The financial condition of the covered entity or business associate.

The Omnibus Rule also updates the affirmative defenses available to avoid imposition of a civil monetary penalty. A modified set of affirmative defenses is available to both covered entities and business associates for violations occurring after February 18, 2009, as compared to affirmative defenses available to covered entities for violations occurring prior to February 18, 2009.

The applicable civil monetary penalties are unchanged from HITECH, which means they include a tiered civil money penalty structure with scalable penalties ranging from $100 to $50,000 per violation, depending on the level of knowledge and intent associated with a violation and an overall limit of $1.5 million for identical violations during calendar year.

Breach notification requirements

HITECH provided for covered entities and business associates to make mandatory notifications (from business associates to covered entities and from covered entities to individuals, the media, and/or the Secretary) in the event of a breach of unsecured

PHI. The Secretary issued the Breach Notification Rule on August 24, 2009 implementing these mandatory notifications. The Breach Notification Rule is supplanted by the Omnibus Rule as of the Compliance Date. Covered entities and business associates must continue to comply with the Breach Notification Rule in the meantime.

The Omnibus Rule: 1) codifies the Breach Notification Rule and 2) modifies certain of its provisions, most notably the definition of a "breach" requiring notification. The definition of "breach," per the interim rule, contained a harm threshold such that a breach "poses a significant risk of financial, reputational, or other harm to the individual." The Omnibus Rule replaces the harm threshold with a presumption that an acquisition, access, use, or disclosure of PHI in a manner not permitted under the Privacy Rule is a breach, *unless* the applicable covered entity or business associate demonstrates that:

> [T]here is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:
>
> 1. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
> 2. The unauthorized person who used the protected health information or to whom the disclosure was made;
> 3. Whether the protected health information was actually acquired or viewed; and
> 4. The extent to which the risk to the protected health information has been mitigated.[2]

Under the Breach Notification Rule, a non-permitted use or disclosure of de-identified information that does not include date of birth or zip code was deemed not a breach. Under the Omnibus Rule, this would be subject to the default presumption that a breach has occurred.

Authorizations for the sale of PHI and for the use and disclosure of PHI for marketing

The Omnibus Rule prohibits covered entities from selling PHI (i.e., directly or indirectly receiving remuneration from or on behalf of the recipient of the PHI in exchange for the PHI) without obtaining a valid authorization for the sale of PHI, which authorization must state that disclosure will result in remuneration to the covered entity The sale of PHI does not include disclosures:

- For public health purposes;
- For research purposes, but only with respect to cost-based fees to cover the cost to prepare and transmit PHI;
- For treatment and payment purposes;
- To a business associate (or subcontractor) where the only compensation is made by the disclosing covered entity (or business associate) to the business associate (or subcontractor) for performance of activities on its behalf;
- To an individual when requested under the Privacy Rule;
- Required by law; or
- For any other purpose in accordance with the Privacy Rule with no compensation other than a cost-based fee to cover the cost to prepare and transmit the PHI or a fee otherwise expressly permitted by law.

In addition, authorizations remain required for covered entities' use and disclosure of PHI for marketing, but the Omnibus Rule has narrowed the definition of marketing such that it does not include:

- refill reminder communications that a covered entity makes without receiving payment, directly or indirectly from or on behalf of a third party whose products or services are being described, beyond the cost of making the communication or
- communications for treatment and health care operations purposes without receiving payment, directly or indirectly from or on

behalf of a third party whose products or services are being described. Such treatment or health care operations purposes include: case management or care coordination, including recommending alternative treatments, therapies, providers, or care settings, and communications to describe a health-related product or service (or payment there for) provided by or included in the plan of benefits of the covered entity making the communication (e.g., regarding entities participating in a provider or plan network, plan changes, and valuable products or services available to plan enrollees but not included in a plan of benefits).

Disclosures of PHI for fundraising

The Omnibus Rule expands the nature of PHI that a covered entity may disclose to a business associate or to an institutionally related foundation for the purpose of raising funds for its own benefit, without a HIPAA-compliant authorization. In this context, the additional information that a covered entity may now disclose includes: department of service information, treating physician, outcome information, and health insurance status. In addition, a covered entity must include in each fundraising communication made to an individual the opportunity to elect not to receive any further fundraising communications. The method for opting out may not cause individuals an undue burden or more than a nominal cost. Furthermore, a covered entity may not condition treatment or payment on whether an individual has opted-out of receiving fundraising communications, and a covered entity may not make fundraising communications to individuals who have opted-out of receiving fundraising communications. A covered entity may allow individuals an opportunity to opt back in to receive fundraising communications.

Notice of privacy practices for PHI

In light of modifications in the Omnibus Rule, covered entities will need to update their Notice of Privacy Practices ("NPP"). NPPs now must include a description of the types of uses and disclosures of PHI that require an authorization pursuant to the Privacy Rule. They must also include a statement that the covered entity is required by law to notify affected individuals following a breach of unsecured PHI. The NPP no longer requires a separate statement indicating, where this is the case, that a covered entity intends to contact individuals to provide appointment reminders and information about treatment alternatives and other health-related benefits and services. However, the required separate statement indicating, where this is the case, that the covered entity may contact individuals to raise funds for the covered entity must now state that individuals have a right to opt out of receiving such communications. Health plans, excluding issuers of certain long-term care policies, that intend to use or disclose PHI for underwriting purposes must include a separate statement indicating that the health plans are prohibited from using or disclosing PHI that is genetic information of an individual for such purposes.

The Omnibus Rule provides the following instructions for a covered entity to make known a material change to its NPP:

1. A health plan that posts its notice on its web site in accordance with paragraph (c)(3)(i) of this section must prominently post the change or its revised notice on its web site by the effective date of the material change to the notice, and provide the revised notice, or information about the material change and how to obtain the revised notice, in its next annual mailing to individuals then covered by the plan.
2. A health plan that does not post its notice on a web site pursuant to paragraph (c)(3)(i) of this section must provide the revised notice, or information about the material change and how to obtain the revised notice, to individuals then covered by the plan within 60 days of the material revision to the notice.[3]

Expanded rights of individuals

The Omnibus Rule adds that a covered entity must agree to an individual's request to restrict disclosure of PHI about the individual to a health plan if:

1. The disclosure is for the purpose of carrying out payment or health care operations and is not otherwise

required by law; and

2. The protected health information pertains solely to a health care item or service for which the individual, or person other than the health plan on behalf of the individual, has paid the covered entity in full.[4]

The Omnibus Rule provides that if an individual requests an electronic copy of PHI that a covered entity maintains in a designated record set, the covered entity must provide the individual with access to the PHI in the electronic form and format requested by the individual. However, if the PHI is not readily producible in such form and format, the covered entity must provide the PHI in a readable electronic form and format as agreed to by the covered entity and the individual. So long as the covered entity provides *some form* of electronic copy, it is not required to purchase new software or systems to accommodate an electronic copy request. A covered entity must act on—i.e., grant or deny, in whole or in part—an individual's request for access within 30 days of receipt (and can obtain one additional 30-day extension). (Note that the fee charged by a covered entity for providing such PHI to an individual may now include supplies for creating the paper copy or electronic media if the individual requests that the electronic copy be provided on portable media.)

Additionally, the Omnibus Rule provides that if an individual requests access to PHI in a signed written document that directs the covered entity to send the individual's copy of the PHI directly to another person designated by the individual and identifies where the covered entity should send the PHI, the covered entity must provide the copy to the person designated by the individual.

Miscellaneous

The Omnibus Rule also contains the following provisions:

Compound HIPAA-compliant authorizations for research

An authorization generally may not be combined with another document to create a "compound authorization." However, the Privacy Rule provides that an "authorization for the use or disclosure of protected health information for a research study may be combined with any other type of written permission" for the same research study—and now, pursuant to the Omnibus Rule, an authorization may be combined with other written permission from another research study. This change allows covered entities to obtain a single compound authorization for broader uses beyond a single study, including combining such an authorization: (i) with another authorization for the same research study; (ii) with an authorization for the creation or maintenance of a research database or repository, or (iii) with a consent to participate in research. In addition, such a compound authorization for research may contain, so long as they are clearly distinguished, both conditioned and unconditioned components, where conditioned refers to conditioning the provision of research related treatment on the provision of an authorization. Such a compound authorization must also allow individuals an opportunity to opt in to the research activities described in the unconditioned authorization.

Provisions regarding deceased individuals

The Omnibus Rule provides that information regarding a person who has been deceased for more than 50 years is not PHI, and a covered entity is not required to comply with the Privacy Rule with respect to such information.

The Omnibus Rule modifies the Privacy Rule to provide that covered entities may disclose PHI regarding a deceased individual to family members and other relatives, close personal friends, and persons identified by the individual who were involved in the individual's care or payment for care, provided that the PHI is relevant to such persons' involvement.

Governmental entities making disclosures of limited data sets

Where a covered entity and a business associate are both governmental entities, the covered entity may disclose to the business associate a limited data set pursuant to a data use agreement in order for the business associate to carry out a health care

operations function.

Disclosures, without authorization, to schools about students or prospective students

A covered entity may disclose PHI, without a HIPAA-compliant authorization, to schools about students or prospective students if: (i) the PHI is limited to proof of immunization, (ii) the school is legally required to obtain proof of immunization prior to admitting the individual; and (iii) the covered entity obtains and documents the written or oral agreement from an individual, or a minor individual's parent or guardian if applicable.

Prohibition on health plan's use and disclosure of genetic information for underwriting purposes

The Omnibus Rule prohibits health plans (other than certain issuers of long-term care policies) from using "genetic information" for "underwriting purposes." For the purpose of this prohibition "underwriting purposes" with respect to a health plan are defined to include:

> 1. Rules for, or determination of, eligibility (including enrollment and continued eligibility) for, or determination of, benefits under the plan, coverage, or policy (including changes in deductibles or other cost-sharing mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program);
> 2. The computation of premium or contribution amounts under the plan, coverage, or policy (including discounts, rebates, payments in kind, or other premium differential mechanisms in return for activities such as completing a health risk assessment or participating in a wellness program);
> 3. The application of any pre-existing condition exclusion under the plan, coverage, or policy; and
> 4. Other activities related to the creation, renewal, or re-placement 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, coverage, or policy.[5]

The Omnibus Rule adds a definition of "genetic information" (as well as definitions of "genetic services" and "genetic test" which are applicable to the definition of "genetic information").[6]

Timing for compliance with the Omnibus Rule

The Omnibus Rule is effective March 26, 2013, and compliance is due within 180 days (i.e. by September 23, 2013). The Omnibus Rule provides that any future establishment of new or modified standards and implementation specifications will require compliance within 180 days of the applicable effective date. In addition, covered entities and business associates will need to modify their business associate agreements in order to comply with the Omnibus Rule, and the timing for such modifications is as follows:

- Generally, business associate agreements must comply with the Omnibus Rule requirements beginning September 23, 2013; yet
- Unless it is renewed or modified on or after March 26, 2013, any business associate agreement that a covered entity had entered into as of, and was operating pursuant to before, January 25, 2013 (and that complied with the applicable provisions of 45 C.F.R. §§ 164.314(a) or 164.504(e) that were in effect on January 25, 2013) shall be deemed compliant until the earlier of:
  - The date such contract or other arrangement is renewed or modified on or after September 23, 2013; or
  - September 22, 2014.

Similar transition provisions exist for data use agreements.

For questions about the implications of the Omnibus Rule for your organization, please contact one of the attorneys listed above.

Notes

1. "Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules," 78 F.R. 5566, available at **www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf**.
2. 45 C.F.R. § 164.402.
3. 45 C.F.R. § 164.520(c)(2)(v).
4. 45 C.F.R. § 164.522(a)(1)(vi).
5. 45 C.F.R. § 164.502(a)(5)(i)(A)-(B).
6. 45 C.F.R. § 160.103.

   Genetic information means:

   (1) Subject to paragraphs (2) and (3) of this definition, with respect to an individual, information about:

   a. The individual's genetic tests;
   b. The genetic tests of family members of the individual;
   c. The manifestation of a disease or disorder in family members of such individual; or
   d. Any request for, or receipt of, genetic services, or participation in clinical research which includes genetic services, by the individual or any family member of the individual.

   (2) Any reference in this subchapter to genetic information concerning an individual or family member of an individual shall include the genetic information of:

   a. A fetus carried by the individual or family member who is a pregnant woman; and
   b. Any embryo legally held by an individual or family member utilizing an assisted reproductive technology.
   c. Genetic information excludes information about the sex or age of any individual.

   Genetic services means:

   (1) A genetic test;
   (2) Genetic counseling (including obtaining, interpreting, or assessing genetic information); or
   (3) Genetic education.

   Genetic test means an analysis of human DNA, RNA, chromosomes, proteins, or metabolites, if the analysis detects genotypes, mutations, or chromosomal changes. Genetic test does not include an analysis of proteins or metabolites that is directly related to a manifested disease, disorder, or pathological condition.