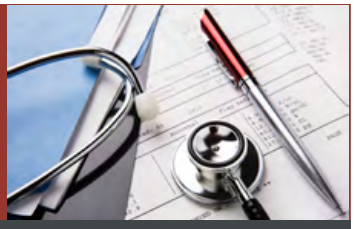
Health Care Alert



Published by Bradley Arant Boult Cummings LLP

HIPAA and HITECH Privacy and Security Rule Update: Final Omnibus Rule

January 25, 2013

The Office of Civil Rights ("OCR") of the Department of Health and Human Services ("HHS") published today the much anticipated final omnibus rule implementing the Health Information Technology for Economic and Clinical Health Act ("HITECH") under HIPAA. The final HITECH rule modifies the Privacy Rule, Security Rule, Breach Notification Rule, Genetic Information Nondiscrimination Act of 2008 ("GINA") Rule, and the Enforcement Rule (collectively referred to as the HIPAA Rules) for covered entities and the business associates handling protected health information ("PHI") on their behalf.

We are providing some action items, followed by a brief summary of a few of the major features of the final HITECH rules (the "Final Rule"). We are also providing links to the Final Rule as published in the Federal Register and a redline showing the changes to the existing regulations.

- ***Time is of the essence.*** Compliance with the Final Rule will require significant effort on the part of covered entities and business associates (including the subcontractors of traditional business associates). Covered entities and business associates must revise policies and procedures, train their workforce, and maintain documentation to demonstrate compliance with the Final Rule. Workforce training should include prompt reporting of breaches and changes in the Privacy Rule. Business associates should review their security systems and policies to ensure compliance with the security requirements before the compliance date.

- ***Reconsider and Designate Your Organizational Choices to Reflect New Realities.*** While the changes in organizational requirements are minimal, the health care industry has changed dramatically from the initial Privacy Rule in 2000 establishing organizational options and providing for affiliated covered entities, hybrid covered entities, and organized health care arrangements ("OHCA"s). Now is the time for covered entities to rethink their alignment of affiliated members and how to bring the non-health care component into the hybrid covered entity fold. Further, today providers participate in many arrangements designed to share protected health information for a common enterprise, namely integrated electronic health records and accountable care organizations ("ACOs"). Where covered entities once had concerns with the OHCA requirement that the participants "hold themselves out" as a joint arrangement, these types of joint activities are now quite common and need to be considered for integrated HIPAA compliance.

- ***Update Templates, Opt-Out Policies and Forms.*** Templates for business associates agreements, notices of privacy practices, marketing authorizations and other forms will need to be refined and updated to include certain specified information. Covered entities should review their current marketing and fundraising policies and procedures and ensure that marketing authorizations are obtained where warranted and that an appropriate and effective fundraising opt-out procedure is put in place.

- ***Inventory Business Associate and Update Business Associate Agreements.*** Since most business associate agreements likely will need to be amended, covered

Authors

Judd A. Harwood
205.521.8016
jharwood@babc.com

Amy S. Leopard
615.252.2309
aleopard@babc.com

Mark C. Lewis
615.252.2347
mlewis@babc.com

Dinetia Newman
601.592.9956
dnewman@babc.com

entities should inventory their existing business associates to (1) identify whether any business associates might be considered an agent subjecting the covered entity to the risk of expanded liability, (2) evaluate the relative risk of the protected health information being compromised, and (3)—if electronic protected health information is involved—to assess the security safeguards the business associate maintains. Business associates should continue their compliance efforts with respect to the Security Rule's administrative, physical and technical safeguards, and can begin to assemble lists of their direct subcontractors with whom they may be required to have a business associate agreement.

- ***Update Your Breach Response Plan.*** Covered entities and business associates will need to revise their breach response polices to conduct risk assessments and address the factors identified by OCR in determining whether protected health information has been "compromised." Covered entities and business associates should continue to have a process for mitigating the harmful effects of potential breaches despite the elimination of the harm threshold for reporting.

- ***Update Your Risk Assessment and Address Encryption.*** Covered entities (and now business associates) must conduct a risk analysis of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information. The failure to do so now has become an important enforcement focus on audit or when OCR receives a complaint or a breach report. In a recent interview, OCR Director Leon Rodriquez reported that his office is concerned about the failure to perform an analysis of possible alternatives when encryption of electronic protected health information is not considered reasonable and appropriate. "We love encryption," according to Rodriquez.

Compliance Dates

Proposed Rule: In the proposed HITECH rule (the "Proposed Rule"), OCR recognized that covered entities and business associates would need time to comply with most of the HITECH changes and allowed such entities 180 days to become compliant with the majority of HITECH's provisions. Planning for future revisions, OCR addressed compliance dates generally for new and modified HIPAA standards and implementation specifications, but left itself options to address and to otherwise provide in the regulations for different compliance dates when covered entities and business associates required additional time to become compliant.

Final Rule: The Final Rule is effective March 23, 2013 and, as proposed, covered entities and business associates must comply with most of the Final Rule within 180 days of the effective date (i.e., September 23, 2013). OCR adopted its proposal to require 180 days for compliance with future new or modified HIPAA standards and implementation specifications (unless specifically stated otherwise in the regulations). Note however that changes to the HIPAA Enforcement Rule (which are not changes to standards or implementation specifications) are effective on March 23, 2013 and require compliance on that date.

Covered entities and business associates must continue to comply with the HIPAA rules currently in effect and the breach notification requirements under the interim final Breach Notification Rule for breaches occurring on or after September 23, 2009 until September 23, 2013, at which time they must comply with the Final Rule's provisions.

Covered entities and business associates (as well as subcontractor business associates) that have in place a written agreement, negotiated in good faith and in compliance with prior HIPAA Rules and that are not modified or renewed (except for evergreen agreements) between March 23, 2013 and September 23, 2013 will be "deemed" compliant until September 23, 2014.

Co-Authors

Kevin Alonso
615.252.2330
kalonso@babc.com

Sarah K. Baker
615.252.2360
sbaker@babc.com

J.S. "Chris" Christie, Jr.
205.521.8387
jchristie@babc.com

Chelsey J. Hadfield
615.252.2392
chadfield@babc.com

Lauren B. Jacques
615.252.4637
ljacques@babc.com

Organizational Requirements

Current Rule: The Privacy and Security Rules outline the organizational requirements and implementation specifications for health care components of covered entities and for affiliated covered entities. Currently, covered entities have several choices with respect to how they handle affiliates and related entities. Legally separate covered entities with common ownership or control (e.g., a chain) may self-designate as a single covered entity for HIPAA compliance purposes. Within a covered entity, the component(s) of the entity performing functions that make the entity a health care provider, plan or clearinghouse may be segregated from those components that do not (covered entities that elect to segregate their components are referred to as hybrid entities). Hybrid entities may choose to include non-health care component activities that perform business associate activities within the health care component or keep them segregated. In the Proposed Rule, HHS proposed to require the business associate-like component within the health care component be directly subjected to HIPAA.

Finally, the Privacy Rule currently allows a covered entity to disclose protected health information "to another covered entity" that participates in an OHCA for any health care operations activities of the OHCA, such as utilization review, quality assessment and improvement and payment activities. In the Proposed Rule, HHS proposed to replace the words "to another covered entity" with the phrase "other participants" because not all participants in an OHCA may be covered entities.

Final Rule: OCR will retain the provisions in the Enforcement Rule establishing civil monetary penalty joint and several liability for affiliated covered entities and their members unless it is established that another member of the affiliated covered entity was responsible for the violation. The American Hospital Association had requested that OCR allow hybrid entities to decide whether to include business associate-like components in the health care component or keep them segregated since business associates will be directly subject to the HIPAA rules. Instead, OCR will require, rather than permit, covered entities that are hybrid entities to include a component that performs business associate-like activities within its health care component and be directly subject to the HIPAA Rules. The Final Rule modifies the provision allowing covered entities participating in an OHCA to disclose protected health information to other participants in the OHCA, regardless of whether the other participants are covered entities, to allow certain physicians and other OHCA participants in clinically integrated care to participate. OCR clarified that this permission does not extend to access by employers and pharmaceutical representatives whose access to protected health information is otherwise restricted.

Business Associates and Business Associate Agreements

Proposed Rule: HITECH expands the definition of individuals and entities that are considered business associates. Prior to HITECH, business associates were, for the most part, not directly governed by the Privacy or Security Rules. Rather, business associates' obligations arose out of their business associate agreements with their covered entity clients. OCR had proposed to make the subcontractors of a covered entity (third parties who perform functions or provide services to business associates) business associates. Under OCR's proposal, business associates would be required to enter into business associate agreements with their direct subcontractors, and the subcontractors would be required to comply with the Security Rule and HITECH's privacy and security provisions (e.g., the breach notification provisions).

Final Rule: Perhaps the most significant changes in the Final Rule are those affecting business associates. The Final Rule makes a business associate directly liable for:

- failures to comply with the Security Rule. As required by HITECH, the Final Rule requires business associates to comply with the Security Rule in much the same way that covered entities are required to comply (e.g., business associates must implement certain administrative, physical and technical safeguards along with policies and procedures as required by the Security Rule);

Co-Authors

Elliot J. Labovitz
205.521.8239
elabovitz@babc.com

Scott Lenz Jr.
615.252.2364
slenz@babc.com

Anna J. Long
615.252.2353
along@babc.com

Daniel F. Murphy
205.521.8017
dmurphy@babc.com

Jake Neu
615.252.4639
jneu@babc.com

- impermissible uses or disclosures of protected health information (e.g., uses or disclosures not permitted or required by the applicable business associate agreement or by law);
- failures to use, disclose or request the minimum amount of protected health information necessary to accomplish the intended purpose of the use, disclosure or request as required by the Privacy Rule's minimum necessary standard;
- failures to enter into business associate agreements with direct subcontractors that create, receive, transmit, and now *maintain*, protected health information on the business associate's behalf;
- failures to provide breach notifications to the applicable covered entities as required by the Breach Notification Rule;
- failures to provide access to a copy of protected health information to either the covered entity, the individual who is the subject of the protected health information or the individual's designee (whichever is specified in the applicable business associate agreement); and
- failures to disclose protected health information where required by the Secretary of HHS to investigate or determine the business associate's compliance with the rules.

The Final Rule expands the definition of "business associate" to cover certain organizations, some of which have only indirect relationships with the health care industry and may have little awareness of their compliance obligations. The Final Rule expands the definition of business associates to encompass health information organizations ("HIOs"), personal health record ("PHR") vendors offering a PHR to individuals on a covered entity's behalf, patient safety organizations ("PSOs"), and e-prescribing gateways (or others providing data transmission services with respect to protected health information to a covered entity that requires routine access to the protected health information).

In addition to PSOs, HIOs and PHR vendors, the Final Rule expands the definition of "business associate" to include subcontractors who create, receive, maintain or transmit protected health information on behalf of a business associate. A "subcontractor" means a person (excluding workforce members) to whom a business associate delegates a function, activity or service that the business associate has agreed to perform on behalf of the covered entity. For example, disclosures of protected health information by a business associate to a third party for the business associate's own management and administration do not make the third party a business associate. However, as previously required, the business associate would be required to obtain satisfactory assurances from the third party that the information will be held confidentially and will not be further used or disclosed except as required by law or for the purposes for which it was disclosed to the third party.

The "business associate" designation follows subcontractors "down the chain" of the information flow. For example, if a business associate delegates a function involving the disclosure of protected health information to a subcontractor, that subcontractor is a business associate as well. If the subcontractor delegates the function to a third party, that third party is a business associate to the subcontractor (and therefore both the subcontractor and the third party would be subject to the direct compliance obligations discussed above). As a result, the Final Rule may affect organizations that have only an indirect relationship with the health care industry and lack a full appreciation of their new compliance obligations.

The Final Rule also requires business associates to enter into business associate agreements with their direct subcontractors. Note, however, that covered entities are not required to marshal business associate agreements with every downstream entity now considered a business associate; rather, each business associate is required to enter into a business associate agreement with its direct subcontractors.

The Final Rule comments follow the Enforcement Rule commentary and recognize the federal common law of agency for determining whether a business associate that is an independent contractor will be considered the covered entity's agent for purposes of establishing vicarious liability for a HIPAA violation. As discussed below under the civil monetary penalties discussion, the comments emphasize control. In light of the potential vicarious liability for acts and omissions of business associates (and business associates' potential liability for their subcontractors), covered entities and business associates may need to re-think their approach to business associates agreements. Covered entities often do not place enough attention on ascertaining the agency status of their contractors. Before the Final Rule, covered entities often believed that more detailed instructions for business associates would lessen the likelihood of a covered entity's vicarious liability for business associate violations of HIPAA. Under the explanation of the Federal common law of agency in the Final Rule comments, those details may increase the likelihood of vicarious liability for HIPAA violations by business associates considered an agent of the covered entity.

Privacy Rule Changes Generally—

Proposed Rule: OCR proposed several changes to the Privacy Rule provisions regarding the uses and disclosures of protected health information. OCR proposed to require a covered entity to comply with the requirements of the Privacy Rule with regard to the protected health information of a deceased individual for a period of 50 years following the date of death. OCR also proposed to modify the definition of "protected health information" to make clear that the individually identifiable health information of a person who has been deceased for more than 50 years is not protected health information under the Privacy Rule.

Final Rule: The Final Rule adopts the approach of the Proposed Rule and clarifies that a covered entity's duty to safeguard the protected health information of a deceased individual no longer runs indefinitely. Instead, the covered entity's duty expires fifty (50) years after the death of the individual. The Final Rule modifies the public health disclosure provisions of the Privacy Rule to include a new category under which a covered entity may use or disclose protected health information for public health activities and purposes. The Final Rule now provides that a covered entity may use or disclose protected health information to a school, about an individual who is a student or prospective student of the school, if (1) the protected health information that is disclosed is limited to proof of immunization, (2) the school is required by state or other law to have such proof prior to admitting the individual, and (3) the covered entity obtains and documents the agreement to the disclosure from either a parent, guardian, or other person acting in loco parentis of the individual, if the individual is an unemancipated minor, or the individual, if the individual is an adult or emancipated minor.

Notice of Privacy Practices

Proposed Rule: OCR proposed several changes to covered entities' notices of privacy practices ("NPP") (e.g., the Proposed Rule would require a statement that certain disclosures require an authorization, would need to address potential marketing or fundraising activities, if any, along with the opt-out procedure etc.). OCR also proposed to revise provisions relating to the NPP for health plans that perform underwriting to require that those health plans include a statement that they are prohibited from using or disclosing protected health information that is genetic information about an individual for such purposes.

Final Rule: The Final Rule requires that NPPs include a statement that certain kinds of uses and disclosures (e.g., marketing) require an authorization. Also, with respect to health plans that post their NPPs on their websites, rather than requiring the health to provide the NPP to individuals within sixty days of a material change, the Final Rule allows such health plans to merely post the revised NPPs on their websites by the effective date of the change and then notify individuals in their next annual mailing. In addition, notice and a separate statement informing the individual will be necessary if the covered entity desires to disclose protected health information to the sponsor of a group health plan, health insurance issuer or HMO; or if an entity is a health plan, notice of intentions to disclose for underwriting purposes is required.

The Final Rule adopts the requirement for health plans that perform underwriting to include in the NPPs a statement that they are prohibited from using or disclosing protected health information that is genetic information about an individual for underwriting purposes, except with regard to long-term care policies, which are not subject to the underwriting prohibition. Health plans that have already modified and redistributed their NPPs to reflect the statutory prohibition are not required to do so again, provided the changes to the NPP are consistent with the Final Rule.

If there is a material change to the NPP, a health plan must prominently post the change on its website or provide the revised notice to the individuals covered by the plan within sixty (60) days of the change.

Restrictions on Health Plan Disclosures

Proposed Rule: HITECH requires covered entities to comply with an individual's request to restrict disclosures of protected health information to a health plan for payment or health care operations purposes if the information pertains solely to items or services paid out of pocket and in full. The Proposed Rule would implement that requirement, noticing operational difficulties inherent in the requirement (e.g., whether health care providers should be required to notify subsequent treatment providers, and how or if an individual should pay out of pocket for care that is reimbursed on a capitated basis).

Final Rule: The Final Rule adopts the approach of the Proposed Rule and clarifies that a covered entity must honor an individual's request to limit disclosure to his or her health plan if 1) the disclosure is for the purpose of carrying out payment or health care operations, 2) the disclosure is not otherwise required by law, and 3) the protected health information pertains solely to a health care item or service paid in full by the individual or someone other than the health plan on behalf of the individual.

Proposed Rule: The Privacy Rule generally sets out the uses and disclosures a covered entity is permitted to make to carry out treatment, payment, or health care operations. The Proposed Rule would prohibit the use of genetic information for health plans' underwriting purposes.

The Final Rule: The Final Rule prohibits health plans from using or disclosing an individual's protected health information that is genetic information for underwriting, even though such a use or disclosure is considered payment or health care operations.

Right to Agree or Object to Disclosure

Proposed Rule: The Privacy Rule includes standards applicable to covered entities' use or disclosure of protected health information about individuals to family members or others involved with an individual's care. Those standards are difficult to administer after an individual has died. OCR proposed that a covered entity be able to disclose the protected health information of a deceased individual to family members and certain others unless the covered entity was aware that the use or disclosure would be inconsistent with the individual's prior expressed preference.

Final Rule: The Final Rule adopts OCR's proposal enabling a covered entity to disclose to a family member, other relative, close personal friend, or any other person previously identified by a deceased individual the protected health information directly relevant to such person's involvement with the individual's health care or payment related to that health care unless doing so is inconsistent with any prior expressed preference of the individual that is known to the covered entity.

Right to Access Protected Health Information

Proposed Rule: HITECH provides individuals a right to request a copy of information maintained in their electronic health record in an electronic format. In the Proposed Rule, OCR broadened the type of information for which this right would apply to all designated record sets maintained electronically. OCR proposed that individuals have a right to request that the copy be in electronic form or the format requested by the individual, if the information is readily producible in such form or format, or, if not, in a readable electronic form and format agreed to by the covered entity and the individual.

Final Rule: The Final Rule conforms to the Proposed Rule explaining that if an individual requests to receive his or her own protected health information maintained electronically in one or more designated record sets, the covered entity must provide access in the particular electronic form or format requested if it is readily producible in the requested form or format. If the protected health information is not maintained in the requested form or format, the entity must provide the individual with the protected health information in a readable electronic form and format agreed to by both parties.

If the individual directs the covered entity to transmit a copy of the individual's protected health information to another person designated by the individual, the covered entity must transmit the protected health information to the person so designated. The designation must be in writing, signed by the individual, and clearly identify the designated person as well as where to send the copy.

Under the Final Rule, covered entities must act on an individual's request for access to his or her own protected health information, whether paper or electronic, within thirty (30) days following receipt of the request, regardless of whether the protected health information is maintained onsite. No longer will off-site storage or inaccessibility warrant a 30-day extension of the customary deadline under the Privacy Rule.

Fundraising

Proposed Rule: The Privacy Rule currently permits covered entities, without individual authorization, to use and disclose to business associates or institutionally related foundations certain protected health information about an individual for fundraising purposes. The Privacy Rule requires covered entities to include in their Notice of Privacy Practices ("NPPs") (1) notice that individuals' protected health information may be used for fundraising purposes, (2) a description in any fundraising materials of how individuals may opt out of future communications, and (3) make reasonable efforts to prevent future fundraising materials from being sent to individuals who have elected to opt out. The Proposed Rule would have strengthened individuals' fundraising opt-out rights, prohibited covered entities from conditioning treatment or payment on a patient's choice to receive or opt-out of fundraising communications, and prohibited (rather than required "reasonable efforts") sending fundraising communications to individuals who have opted out.

Final Rule: The Final Rule expands the information which may be disclosed by a covered entity without prior authorization for

the purpose of fundraising. Whereas the Privacy Rule previously permitted only the disclosure of demographic information and the dates of health care, the Final Rule now defines the demographic information that may be shared and also permits the disclosure of the department of service, treating physician, outcome of treatment, and health insurance status. For fundraising disclosures, the covered entity's NPP now must contain a statement notifying the individual that such information may be shared for this purpose. In addition, each fundraising communication must provide the individual with a clear and conspicuous opportunity to elect not to receive further fundraising communications that does not impose an undue burden on the individual (e.g., via email or a telephone number). Requiring patients to write a letter requesting to opt out would constitute an undue burden according to commentary in the Final Rule. The Final Rule also retains the Proposed Rule's prohibition on conditioning the treatment or payment on the individual's choice to opt-out of future fundraising communications.

Marketing

Proposed Rule: The Proposed Rule included additional restrictions on written communications sent to patients by covered entities when the covered entity receives financial remuneration in exchange for making the communication from the third party whose product is the subject of the marketing communication. The Proposed Rule differentiated between compensated written communications for treatment purposes, and those that are for health care operations purposes by excluding the former from the definition of "marketing." OCR explained that it considers compensated treatment communication to be directed towards an individual's specific care (e.g., a provider sending a pregnant patient a brochure recommending a specific birthing suite), whereas compensated health care operations communications are made in more of a population-based fashion (e.g., a mass mailing to all patients announcing a new affiliated physical therapy practice). Although compensated treatment communications were to be exempted from the marketing authorization requirements, a covered entity still would have been required to implement a process for individuals to opt-out of such communications and update its NPP to explicitly provide for this type of communication. The communication itself also would need to disclose the fact that the covered entity received compensation in return for sending the communication and contain a clear and conspicuous opt-out procedure.

Final Rule: In response to the comments, the Final Rule significantly modifies the Proposed Rule's approach to marketing by removing the distinction between treatment and health care operations communications. Instead, all communications whereby the covered entity receives financial remuneration from a third party whose product or service is being marketed, regardless of whether the communication is for a treatment or health care operations purpose, require an authorization from the patient. By treating all communications as marketing communications, implementation is simplified for covered entities because they will not need to develop two processes based on the purpose of the communication. Instead, all marketing communications which involve financial remuneration require the covered entity to obtain a valid authorization from the individual before using or disclosing protected health information, and the authorization must disclose the fact that the covered entity is receiving financial remuneration. The permitted disclosure is limited to the scope of authorization given, which may be revoked at any time. In addition, while a covered entity may choose to update its NPP, the Final Rule no longer requires that a covered entity include a statement that it may contact the individual to provide appointment reminders or information about treatment alternatives where the provider receives financial remuneration from a third party in exchange for making the communication. It should be noted that the Final Rule does not modify the exceptions to the authorization requirement for marketing communications. The rule still provides that no authorization is required where a covered entity receives financial remuneration from a third party to make a marketing communication if the communication is made face-to-face by a covered entity to an individual or consists of a promotional gift of nominal value provided by the covered entity.

The Final Rule also adopts additional exceptions to the authorization requirement. Most notably, refill reminders or other communications regarding drugs or biologics (including drug delivery systems such as insulin pumps) which are already prescribed for the individual do not require individual authorization. To fall within this exception, the financial remuneration received in exchange for communications about a drug currently prescribed to an individual must be "reasonable in amount," meaning that it must be reasonably related to the covered entity's cost of making the communication. The commentary clarified that permissible costs are those which cover the costs of labor, supplies, and postage to make the communication. Where the financial remuneration generates a profit or includes payment for other costs, it would not be considered "reasonable in amount." The other exceptions from the authorization requirement include communications promoting health but that do not promote a product or service from a particular provider and communications about government and government-sponsored programs.

Sale of PHI

Proposed Rule: Subject to certain exceptions, HITECH generally prohibits the sale of protected health information without an authorization from the subject of the information. The Proposed Rule included the general prohibition against the sale of protected health information and the exceptions contained in HITECH, and further required that covered entities (and

business associates, as applicable) obtain an authorization prior to disclosing protected health information in exchange for direct or indirect remuneration. The exceptions include (1) disclosures of protected health information for public health, research, treatment, and payment purposes; (2) disclosures in connection with the sale of all or part of the covered entity and related due diligence; (3) disclosures to or by a business associate in accordance with its duties to the covered entity; (4) disclosures to the subject of the information; (5) disclosures required by law; and (6) any other permissible purpose as long as the remuneration received by the covered entity is limited to the costs required to prepare and transmit the protected health information.

Final Rule: The Final Rule restates the general prohibition against the sale of protected health information without an individual authorization. It also retains, without significant modification, the exceptions set forth in the Proposed Rule (disclosures for public health purposes, research purposes, and treatment or payment purposes, etc.). The Final Rule defines the "sale of protected health information" to mean "a disclosure of protected health information by a covered entity or business associate, if applicable, where the covered entity or business associate directly or indirectly receives remuneration from or on behalf of the recipient of the protected health information in exchange for the protected health information." Thus, a "sale" is not limited to a transfer of ownership of protected health information, but also includes disclosures that are the result of access, license, or lease agreements. In addition, the term "remuneration" is interpreted in the commentary to mean both financial and nonfinancial benefits.

Research

Current Rule: OCR proposed no changes to the standards for de-identifying protected health information. On November 26, 2012, OCR published guidance regarding the de-identification of protected health information to identify methods and approaches for compliance with the Privacy Rule. The guidance explains and answers questions regarding two methods that can be used to satisfy the Privacy Rule's de-identification standards: Expert Determination and Safe Harbor. The purpose of this guidance was not to provide novel concepts or to change the current scheme for de-identification of protected health information, but instead to assist covered entities and business associates in understanding de-identification, the general process by which de-identified information is created, and the alternatives for achieving de-identification.

The Privacy Rule generally prohibits "compound authorizations." Compound authorizations arise where an authorization for the use and disclosure of protected health information is combined with any other legal permission. An exception to this general prohibition permits the combining of an authorization for a research study with any other written permission for the same study, including another authorization or informed consent to participate in the research. Notwithstanding that exception, the Privacy Rule prohibits combining an authorization that conditions treatment, payment, enrollment in a health plan, or eligibility for benefits (conditioned authorization) with an authorization for another purpose for which treatment, payment, enrollment, or eligibility may not be conditioned (unconditioned authorization). The intent of this limit on compound authorizations is to help ensure that individuals understand their right to decline the activity in the unconditioned authorization, but still receive treatment or other benefits or services by agreeing to the conditioned authorization. The practical effect of this limit on compound authorizations, however, results in a lack of integration and an inconsistency between the privacy requirements and current practice under the Common Rule (45 C.F.R. Part 46).

Final Rule: OCR makes no changes to the standards for de-identifying protected health information in the Final Rule. OCR adopts its proposed changes to the authorization provisions of the Privacy Rule, thus allowing a covered entity to combine conditioned and unconditioned authorizations for research, provided that the authorization clearly differentiates between the conditioned and unconditioned research components and clearly allows the individual the ability to opt in to the unconditioned research activities. The Final Rule explicitly provides for flexibility with respect to how covered entities meet the authorization requirements, provided that the core elements required for a valid authorization are included. Ultimately, this softening of the restriction on compound authorizations provides flexibility to clinical researchers, streamlines documents provided to research participants, and harmonizes the authorization provisions of the regulations with the Common Rule.

Covered entities desiring to employ a compound authorization have flexibility in how they choose to draft the authorization. For example, a covered entity could describe the unconditioned research activity on a separate page of a compound authorization and could also cross-reference relevant sections of a compound authorization to minimize the potential for redundancy. In addition, a covered entity could use a separate check box for the unconditioned research activity to signify whether an individual has opted-in to the unconditioned research activity, while maintaining one signature line for the authorization. Alternatively, a covered entity could provide a separate signature line for the unconditioned authorization to signal that the individual is opting in to the unconditioned research activities.

If a research subject revokes his or her authorization in the course of a clinical trial, be certain to document whether the

revocation applies to the conditioned authorization, the unconditioned authorization, or both the conditioned and unconditioned authorizations. If the revocation is not clear, commentary in the Final Rule suggests that the entire authorization must be treated as revoked.

Genetic Information under GINA

Proposed Rule: HHS proposed to modify the definition of "health information" to provide expressly that such term includes genetic information and a number of conforming changes to definitions and other provisions of the Privacy Rule. GINA prohibits discrimination based on an individual's genetic information in both the health coverage and employment contexts. With respect to health coverage, Title I of GINA generally prohibits discrimination in premiums or contributions for group coverage based on genetic information; proscribes the use of genetic information as a basis for determining eligibility or setting premiums in the individual and Medicare supplemental (Medigap) insurance markets; and limits the ability of self-funded group health plans, health insurance issuers, and Medigap issuers to collect genetic information or to request or require that individuals undergo genetic testing. Title II of GINA generally prohibits the use of genetic information in the employment context; restricts employers and other entities covered by Title II from requesting, requiring, or purchasing genetic information; and strictly limits such entities from disclosing genetic information.

In addition to the nondiscrimination provisions, section 105 of Title I of GINA contains new privacy protections for genetic information, which require the HHS Secretary to revise the Privacy Rule to clarify that genetic information is health information and to prohibit self-funded group health plans, health insurance issuers (including HMOs), and issuers of Medicare supplemental policies from using or disclosing genetic information for underwriting purposes.

On October 7, 2009, HHS published a proposed rule to strengthen the privacy protections for genetic information under the Privacy Rule by implementing the protections for genetic information required by GINA. HHS proposed to prohibit all health plans covered by the Privacy Rule from using or disclosing protected health information that is genetic information for underwriting purposes. HHS proposed to make a conforming change to § 164.502(a)(1)(iv) to clarify that an authorization could not be used to permit a use or disclosure of genetic information for underwriting purposes.

Final Rule: The Final Rule modifies the Privacy Rule to: (1) add definitions for the GINA-related terms of "family member," "genetic information," "genetic services, "genetic test," and "manifestation," or "manifested" and (2) make technical corrections to the definition of "health plan." With respect to the GINA-related terms, the Final Rule adopts definitions that are generally consistent with the definitions of such terms in the GINA Proposed Rule.

The Final Rule applies the prohibition on using or disclosing protected health information that is genetic information for underwriting purposes to all health plans that are covered entities under the Privacy Rule, except with regard to issuers of long-term care policies effective September 23, 2013, regardless of when or where the genetic information originated. Long-term care plans, while not subject to the underwriting prohibition, continue to be bound by the Privacy Rule to protect genetic information from improper uses and disclosures, and to use or disclose genetic information only as required or expressly permitted by the Privacy Rule, or as otherwise authorized by the individual who is the subject of the genetic information. The Final Rule also adopts the proposed conforming change to clarify that an authorization cannot be used to permit a use or disclosure of genetic information for underwriting purposes.

Security Standards

Current Rule: Under HIPAA, covered entities must follow the security standards and assess the potential security risks and vulnerabilities, then develop physical, administrative, and technical safeguards on the integrity, confidentiality and availability of electronic protected health information. Covered entities must implement all required safeguards enumerated under the rules and address reasonable and appropriate security policies and procedures considering the size of the entity, complexity, capabilities, technical infrastructure, hardware and software capabilities, associated costs, and the probability and criticality of potential risk to electronic protected health information.

The Final Rule does not substantively alter the Security Rule. As discussed elsewhere in this alert, however, the Final Rule does extend the requirements of the Security Rule to business associates. In connection with that extension, OCR made a few small changes to the content of Security Rule-compliant business associate agreements. For example:

- In lieu of requiring the business associate to implement administrative, physical and technical safeguards to protect the covered entity's protected health information, the business associate agreement must require the business associate to comply with the Security Rule; and

- In lieu of a requirement that the business associate ensure that its agents (including its subcontractors) reasonably and appropriately protect the covered entity's protected health information, the business associate agreement must require the business associate to enter into Security Rule-compliant business associate agreements with its subcontractors.

BREACH OF UNSECURED PHI

Breach Notification Rule

Current Rule: In 2009, OCR published an interim final rule implementing the breach notification provisions of HITECH requiring notice to affected individuals, HHS and possibly media outlets in the event of a breach of unsecured protected health information (the "Breach Notification Rule"). A reportable "breach" generally means any acquisition, access, use, or disclosure of protected health information in a manner not permitted by the Privacy Rule. Under the Breach Notification Rule, a breach occurs only if the acquisition, access, use, or disclosure of protected health information poses a significant risk of financial, reputational, or other harm to the individual (the "harm standard"), although a breach of secured protected health information is not reportable. Secured protected health information primarily means shredding or destroying paper, film, or other hard copy media or encrypting electronic protected health information or clearing, purging, or destroying electronic media in accordance with National Institute of Standards and Technology standards. In addition, the impermissible use or disclosure of a limited data set that does not contain birth dates or zip codes would not constitute a breach or require breach notification.

Covered entities must notify affected individuals of breaches without unreasonable delay, but no later than 60 days from the discovery of the breach. A covered entity is deemed to have discovered a breach as of the date the breach is known to any of its workforce or agents (which may include some business associates based on the federal common law of agency) or the date it would have been known had reasonable diligence been exercised. Business associates must notify only their affected covered entities of breaches within that same time frame. Covered entities also must notify HHS, either within 60 days of the end of the calendar year in which the breach occurred or, depending on the number of affected individuals, at the same time the individuals are notified. Covered entities also may be required to notify the media depending on the number of affected individuals. The compliance date for the breach notification rule was February 22, 2010.

Final Rule: In the Final Rule, OCR makes a number of significant changes to the Breach Notification Rule that will reshape how covered entities and business associates determine their breach notification obligations in the future.

Commenters expressed confusion over the role of the harm standard in determining whether a breach has occurred (i.e., is a breach presumed unless a significant risk of harm does not exist, or does a breach only exist where a significant risk of harm can be demonstrated?) To promote uniformity in response to breaches by covered entities and business associates, OCR abandoned the harm standard in favor of what it believes to be a more objective presumption of a breach requiring notification. This presumption of a breach requiring notification is rebuttable upon the demonstration by the covered entity or business associate that a low probability exists that the protected health information has been compromised.

OCR established four primary factors that covered entities and business associates must consider as part of this risk assessment. At a minimum, each factor must be assessed to constitute a risk assessment under the Final Rule. Each factor is discussed below.

1 The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification

OCR advises that covered entities and business associates need to consider this factor in light of the type of protected health information involved, including its level of sensitivity. Covered entities must pay special attention to types of information that could be used to harm the patient or further the unauthorized recipient's own interests. For example, the impermissible use or disclosure of information about sexually transmitted diseases could be used to harm the reputation of a patient. If the impermissibly used or disclosed information included financial information, such as credit card numbers or social security numbers, a greater likelihood of identity theft or fraud against the patient exists.

Furthermore, covered entities and business associates must consider any potentially identifying information and the likelihood of tying that information to a patient. Covered entities and business associates must consider the likelihood of re-identification of protected health information that may even on its surface appear anonymous in

nature. OCR provides the example of the unauthorized disclosure of patient discharge dates and diagnoses. Whether or not that information is re-identifiable could depend, for example, on the specificity of the diagnosis and the size of the area served by the covered entity or business associate.

2 The unauthorized person who used the protected health information or to whom the disclosure was made

Covered entities and business associates must consider who impermissibly received protected health information. To the extent this person or entity is not known, a covered entity or business associate should assume this factor weighs in favor of there being a greater than a low probability that the data has been compromised. When the person or entity is another covered entity or otherwise subject to the Privacy Rule, such as a physician, there is a lower probability that the protected health information has been or will be further compromised.

This factor must also be weighed in light of the likelihood of re-identification discussed above. If a limited data set were impermissibly obtained by a third party, the likelihood that the protected health information is compromised could depend on the person or entity's ability to re-identify the protected health information. OCR provides the example of the impermissible disclosure of service dates and accompanying diagnoses to an employer. The employer could review attendance logs and tie the data back to a particular employee, whereas it is less likely a person or entity without such a special relationship could do so. Disclosure to the employer in this example would increase the probability of the protected health information being compromised.

3 Whether the protected health information was actually acquired or viewed

If protected health information is not actually acquired or viewed, but rather only an opportunity to acquire or view the information existed, this factor weighs in favor of there being a low probability that the protected health information has been compromised. OCR provides the example of a stolen computer that was later recovered, and forensic analysis of the data stored on the computer reveals that the protected health information contained on the computer was never accessed or viewed. In this instance, there would have only been an opportunity to acquire or view the protected health information. Contrast this scenario with a batch of hardcopy medical records intended for the patient, but accidentally mailed to the wrong person by the covered entity. If the envelope is returned to the covered entity unopened, the likelihood the protected health information was acquired or viewed is low. If the envelope returned had been opened or not returned at all, the covered entity would need to assume that the protected health information was actually acquired or viewed.

4 The extent to which the risk to the protected health information has been mitigated

Mitigation upon the impermissible use or disclosure of protected health information might include obtaining satisfactory assurances that the information will not be further used or disclosed, such as through a confidentiality agreement, or that it will be destroyed. This factor must be closely considered in relation to the second factor discussed above. OCR discusses the fact that impermissible uses or disclosures to certain entities—such as a business associate, employee, or other covered entity—can more reasonably be considered mitigated upon receipt of satisfactory assurances that the information in question will not be further used or disclosed or will be destroyed, than impermissible uses or disclosures to an unrelated third party with no obligation to comply with the Privacy Rule.

Covered entities and business associates should implement policies and procedures for conducting and documenting the risk assessment for potential breaches of unsecured protected health information described above. The risk assessment cannot be taken lightly. OCR expects covered entities and business associates to conduct thorough risk assessments in good faith and the conclusions to be reasonable. The only instance in which a covered entity or business associate might not conduct a risk assessment for the breach of unsecured protected health information is upon the determination that breach notifications will be made upon the impermissible use or disclosure of protected health information, regardless of the probability of the information being compromised.

A final important change to the Breach Notification Rule is that OCR removed the breach exception for limited data sets that do not contain birth dates or zip codes. This limited data set exception was abandoned in favor of the more comprehensive risk analysis discussed above. Thus, the impermissible disclosure of a limited data set, even those with missing identifiers such as birth dates and zip codes, will activate a covered entity's or business associate's notification obligations under the breach notification rule, unless a thorough and documented risk assessment of at least the factors discussed above reveal a low probability that protected health information has been compromised.

ENFORCEMENT

Proposed Rule: In the Enforcement Rule and the Proposed Rule, OCR proposed amendments to implement the strengthened enforcement under HITECH, which established four categories of violations that reflect increasing levels of culpability and four corresponding penalty tiers that increased the possible civil monetary penalties ("CMPs"). OCR also proposed to implement the HITECH changes that removed the exception for a covered entity's liability for a business associate's HIPAA violations where certain conditions were met and instead proposed to make a covered entity's liability turn on whether the business associate was the covered entity's agent.

Final Rule: The Final Rule does not change the enforcement-related language from the Enforcement Rule's language. As set forth above in the discussion of business associates, the Final Rule comments recognize the rule under the federal common law of agency to determine whether an independent contractor business associate is a covered entity's agent for purposes of vicarious liability under HIPAA. Similarly, a business associate is liable for the HIPAA violations of its subcontractors that are the business associate's agents. OCR provided substantial commentary on the factors it will consider, emphasizing control.

The Final Rule in comments summarizes HITECH's four violation categories and their corresponding penalty tiers in a table. The table below is reproduced with additional comments added in parentheses and italics:

Categories of Violations and Respective CMP Range

Violation Category – Section 1176(a)(1)	Each Violation (range)	All Such Violations of Identical Provision In a Calendar Year
(A) Did Not Know (and could not have known)	$100 - $50,000	$1,500,000
(B) Reasonable Cause (new definition discussed below)	$1,000 - $50,000	$1,500,000
(C)(i) Willful Neglect-Corrected (within 30 days of discovery)	$10,000 - $50,000	$1,500,000
(C)(ii) Willful Neglect-Not Corrected (within 30 days of discovery)	$50,000	$1,500,000

The outcome of the four penalty tiers turns largely on the defined terms "willful neglect" and "reasonable cause" and whether the covered entity or business associate corrects the HIPAA violation within 30 days of discovering it. In the Enforcement Rule, "reasonable cause" was part of an affirmative defense. The Proposed Rule and the Final Rule make "reasonable cause" a definition that is the basis for the second tier CMP: "Reasonable cause means an act or omission in which a covered entity or business associate knew, or by exercising reasonable diligence would have known, that the act or omission violated an administrative simplification provision, but in which the covered entity or business associate did not act with willful neglect." Since this definition is so similar to the violations that fit within the first tier CMP, the first and second tiers will be difficult to distinguish. For a HIPAA violation to fall within the third tier instead of the fourth tier, the correction must be within 30 days of discovery of the violation.

In many circumstances, the stated maximum CMPs reflected above are illusory maximums. If the facts establish that multiple individuals were affected, that a continuing violation existed for multiple days, or that violations of different parts of the rules existed, the CMPs can include multiple maximums.

While the affirmative defense of reasonable cause is no longer available for violations not due to willful neglect, the affirmative defense of correcting the violation is still available. If the covered entity or business associate corrects the violation within 30 days of discovery, a civil penalty is prohibited. Accordingly, as soon as a covered entity or business associate learns of a possible HIPAA violation, the covered entity or business associate should correct the possible violation.

Let us know if we can help. For more information on HITECH and the Final Rule or if you need assistance preparing for the September 23, 2013 compliance date, please contact Kevin Alonso, Sarah Baker, Chris Christie, Chelsey Hadfield, Judd Harwood, Lauren Jacques, Elliot Labovitz, Scott Lenz, Amy Leopard, Mark Lewis, Anna Long, Dan Murphy, Dinetia Newman, Jake Neu, or one of the other attorneys in the Health Care Practice Group at Bradley Arant Boult Cummings.

BRADLEY ARANT BOULT CUMMINGS LLP OFFICE LOCATIONS:

ALABAMA
One Federal Place
1819 Fifth Avenue North
Birmingham, AL 35203-2119
205.521.8000

200 Clinton Avenue West, Suite 900
Huntsville, AL 35801-4900
256.517.5100

Alabama Center for Commerce
401 Adams Avenue, Suite 780
Montgomery, AL 36104
334.956.7700

MISSISSIPPI
188 E. Capitol Street, Suite 400
Jackson, MS 39201
601.948.8000

NORTH CAROLINA
100 North Tryon Street, Suite 2690
Charlotte, NC 28202
704.338.6000

TENNESSEE
1600 Division Street, Suite 700
Nashville, TN 37203
615.244.2582

WASHINGTON, DC
1615 L Street, N.W.
Suite 1350
Washington, DC 20036
202.393.7150

AMONG THE NATION'S BEST LAWYERS