JONES DAY

MARCH 2013

NEW ERA FOR PRIVACY COMPLIANCE: OVERVIEW OF THE HIPAA "FINAL RULE"

NEW ERA FOR PRIVACY COMPLIANCE: OVERVIEW OF THE HIPAA "FINAL RULE"

On January 25, 2013, the Office for Civil Rights ("OCR") of the U.S. Department of Health and Human Services ("HHS") published in the Federal Register a final omnibus rule ("Final Rule") that revises certain rules promulgated under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). These revised rules were issued pursuant to changes enacted by Congress in the Health Information Technology for Economic and Clinical Health ("HITECH") Act and the Genetic Information Nondiscrimination ("GINA") Act of 2008. Effective March 23, 2013, the Final Rule revises and finalizes an interim notice of proposed rulemaking ("Interim Rule") that OCR had published in 2009, although in many cases the date by which "covered entities" regulated by HIPAA ("Covered Entities") and their "business associates," as defined by the Final Rule ("Business Associates"), must comply with the new or modified rules will be September 23, 2013 or later. In some cases, the Final Rule grandfathers arrangements entered into under the Interim Rule.

Prior to the Interim Rule and the Final Rule, the HIPAA Privacy and Security Rules focused primarily on health care providers, health plans, and other entities that process health insurance claims. The Final Rule now expands many of the HIPAA Privacy and Security Rule requirements to directly regulate Business Associates that receive protected health information, including their subcontractors. Furthermore, penalties have been increased for noncompliance. The Final Rule also expands the duty to give notice to individuals when there has been a breach of unsecured protected health information. We address these changes below.

MODIFICATIONS TO THE BREACH NOTIFICATION RULE

- **Regulations:** 45 C.F.R. § 164.400 *et seq.*
- **Compliance Date:** Ongoing compliance required with Interim Rule and compliance with modifications implemented by Final Rule by September 23, 2013.
- **Executive Summary:** The Final Rule implements section 13402 of the HITECH Act by requiring various notifications following a breach of unsecured protected health information. The Final Rule eliminates the significant risk of harm standard from the Interim Rule for determining whether a breach has occurred. Covered Entities and Business Associates should examine current policies and procedures to ensure compliance with regulatory definitions relating to breach notifications and to ensure that any assessment tool or process evaluating risk to protected health information ("PHI") related to a disclosure includes, at a minimum, the regulatory factors discussed below to assess whether PHI was compromised.

NEW PRESUMPTION OF BREACH AND RISK ASSESSMENT FACTORS

In a highly significant change, OCR discards the Interim Rule's "significant risk of harm standard" approach to assessing whether there has been a breach of unsecured PHI that would trigger a duty to notify certain parties—namely, an approach that weighed the harm caused and an assessment of the risk to individuals. In place of this standard (which had been supported by much of the industry, including some members of Congress), the Final Rule now *presumes* that any unauthorized use, access, or disclosure is a "breach" unless a proper risk assessment finds a low probability that PHI has been compromised. Without such a risk assessment, notice of a "breach" will now be required.

The Final Rule generally maintains the HITECH Act's definition of "breach" to include the unauthorized acquisition, access, use, or disclosure of PHI that compromises the security or privacy of such information and the three HITECH Act statutory definitional exceptions.[1] As discussed in the Final Rule, a breach is presumed to have occurred if there has been any impermissible use or disclosure of a limited data set or a minimum necessary violation of the HIPAA Privacy Rule.[2] An acquisition, access, use, or disclosure of PHI not permitted under the HIPAA Privacy Rule is presumed to be a breach unless a Covered Entity or Business Associate demonstrates a low probability that PHI has been compromised by performing a risk assessment including *at least* the following four factors:

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

Following an unauthorized disclosure, a Covered Entity or Business Associate electing to assess the probability that PHI has been compromised must address each factor listed above in a comprehensive and thorough way so as to evidence a reasonable and good faith application of such factors.[3] OCR's position is that such an assessment or probability analysis should not be a new or novel concept for Covered Entities or Business Associates because similar risk assessments must be routinely performed following security breaches and for compliance with state breach notification laws. OCR provides the following example of a breach that may have a low probability of risk under such an assessment: a misdirected fax sent to the wrong physician group.

Here, OCR asserts that a Covered Entity or Business Associate may be able to demonstrate a low risk that PHI contained in a misdirected fax has been compromised if, upon receipt, the receiving physician calls the Covered Entity to report the delivery error and the destruction of the misdirected fax.[4]

OCR provides guidance and examples on how to analyze these four factors, as discussed below.

Factor One—Nature and Extent of PHI. In assessing the nature and extent of PHI, OCR recommends consideration of the type of PHI (e.g., clinical information, financial information) and the sensitivity of the information. Financial information including credit card numbers, Social Security numbers or other information that might increase an individual's risk of identity theft or financial fraud is considered highly sensitive information warranting careful analysis under any risk assessment. Regarding clinical information, OCR cautions that any risk assessment of such information should contemplate not only the amount of detailed information (e.g., test results, treatment plan, diagnoses, medication records), the size of the community served by a Covered Entity, and the context and ability to re-link available information, but also the probability the disclosed PHI might be used in a manner that is harmful to the individual or further the unauthorized recipient's own interests.

Factor Two—Identity of Unauthorized Recipient of PHI. In assessing risk under the second factor, Covered Entities and Business Associates should consider whether the unauthorized recipient has existing obligations to protect and maintain the privacy and security of information pursuant to HIPAA or to another federal agency by the Privacy Act of 1974 and the Federal Information Security Management Act of 2002. OCR states that an unauthorized disclosure to an entity also required to comply with HIPAA may support a demonstration of a low probability of risk that the PHI has been compromised.[5] However, an unauthorized disclosure to an entity that may have the capability or access to additional information in its own systems to re-identify information may suggest an increased probability PHI has been compromised. For instance, an inappropriate disclosure to an employer by a health plan may present greater risk because the employer may have access to information that permits the employer to re-identify PHI to specific employees.[6]

Factor Three—No Actual Viewing or Acquisition of PHI. The third factor requires consideration as to whether PHI was actually viewed or acquired by an unauthorized recipient or whether the disclosure only created the opportunity for such information to be viewed or acquired. For instance, an unencrypted laptop is stolen, but through the course of a forensic review of the device, it is confirmed PHI was not accessed, viewed, or otherwise compromised, which may demonstrate low probability of risk.[7] However, if PHI must be accessed to confirm the unauthorized disclosure of PHI, such as opening an envelope with materials containing PHI, then actual acquisition of PHI occurred because viewing of the information was necessary to identify the disclosure error.[8]

Factor Four—Mitigation of Risks to PHI. The final factor that must be assessed is whether certain risks related to an unauthorized disclosure may be appropriately mitigated to secure reasonable assurances that inappropriately disclosed PHI will not be further used or disclosed. In assessing mitigation assurances from third parties, OCR opines that the identity of an unauthorized recipient may affect not only the risk analysis, but reasonableness of reliance on recipients' assurances of destruction or lack of further disclosure. Similar to its analysis regarding a misdirected fax to the incorrect physician group, OCR asserts that a mitigation assurance from a Covered Entity or Business Associate may support a finding of low probability of risk to the PHI.[9] However, an identical mitigation assurance from a third party who is inexperienced with implementing and maintaining privacy and security protections for individuals may not warrant a finding of lower probability for risk to further disclosure of the PHI.

Discovery of Breach and Reasonable Diligence

A breach will be treated as discovered as of the first day that it is known or should reasonably have been known, exercising reasonable diligence—in essence, as soon as any person, other than the individual committing the breach, who is a workforce member or agent of a Covered Entity or Business Associate knows or should have reasonably known of the breach.[10] OCR notes the importance of training workforce members to promptly escalate reporting of privacy and security incidents. As to reasonable diligence, OCR asserts that any judgment as to whether diligence was "reasonable" would require considering what similarly situated persons or entities might investigate or audit.[11] Examples of reasonable diligence to discover a breach may include operational steps to learn of breaches, responses to indications of a potential breach, and industry practices related to monitoring and auditing.[12]

Timeliness of Breach Notice to Individuals

The Final Rule maintains the Interim Rule's notification requirement (i.e., without "unreasonable delay") but in no case later than 60 calendar days from the date that the breach is discovered, and restates OCR's concerns related to intentionally delayed notification within the 60-day window. OCR

acknowledges that any judgment as to whether an "unreasonable delay" has occurred is a fact-specific inquiry that takes into account many factors including, but not limited to, the nature of the breach, number of individuals affected, and available resources of a Covered Entity to provide such notice.[13]

Content and Method of Notice to Individuals

The Final Rule maintains the breach and notification content requirements without modification but notes that Covered Entities may tailor notices to adequately notify individuals without exposing Covered Entities to risks by disclosing potential weaknesses in security and safeguard measures.[14] OCR retains the Interim Rule's method of notification requirements. OCR expects that the Covered Entity—not the Business Associate—is ultimately responsible for ensuring notice to affected individuals, although, as discussed in the section "Business Associates and Business Associate Agreements" below, a Covered Entity may elect to delegate the delivery of such notice to a Business Associate.[15] OCR illustrates that this approach may be helpful in addressing breaches involving a health information organization because a health information organization, as a Business Associate for the participating Covered Entities, could provide notice on behalf of all participating Covered Entities. OCR also confirms that notice of a breach may be delivered to an individual by email provided such an individual has affirmatively agreed to receive breach notices by email and has not withdrawn such agreement.[16]

Notice to the Media

The Final Rule maintains the rule requiring a Covered Entity to provide notice to prominent media outlets following the discovery of a breach of unprotected PHI of more than 500 residents of a state or jurisdiction. Interestingly, although the Final Rule does not incorporate substantive revision to this provision, OCR provides insightful analysis as to certain hypothetical fact patterns. OCR advances its position that a Business Associate providing services to multiple Covered Entities experiencing a breach does not alter the analysis by each Covered Entity as to when notice to a media outlet is required. For instance, a breach by a Business Associate affecting 450 individuals related to one Covered Entity and 350 individuals related to another Covered Entity would not require a notice to a media outlet for either Covered Entity because no one Covered Entity incurred a breach of unsecured PHI for more than 500 individuals.[17] OCR also clarifies that a Covered Entity is not required to incur any cost to print or run media notices nor is a media outlet required to print or run media notices.[18]

Notification to Secretary of HHS

Recognizing that situations may exist where reasonable data breach detection mechanisms are in place and breaches may still be undetected for some time, the Final Rule incorporates an important modification to the language requiring a Covered Entity to provide notice to the Secretary of HHS. Now, the notice of a breach affecting fewer than 500 individuals must occur not later than 60 days after the end of the calendar year in which such breach is discovered, as opposed to when it occurs.[19] The Final Rule does not modify existing requirements for a Covered Entity to immediately notify the Secretary of HHS of all breaches affecting 500 or more individuals.[20]

Notification of a Covered Entity by a Business Associate

OCR recognizes that not all Business Associates are agents of their Covered Entities, and it is therefore unwilling to automatically impute a Business Associate's knowledge of a breach to its Covered Entity. Therefore, the Final Rule does not amend existing requirements for Business Associates to notify Covered Entities—not the affected individuals—when the Business Associate becomes aware of, or may reasonably know of, a breach. OCR encourages that parties describe in their Business Associate Agreements ("BAAs") their respective expectations as to who, how, and when notice will be provided to an individual related to a breach.[21]

BUSINESS ASSOCIATES AND BUSINESS ASSOCIATE AGREEMENTS

- **Regulations:** 45 C.F.R. §§ 160.103, 160.300 *et seq.*, 160.410, 164.502(a) and (e), 164.504(e) and 164.532
- **Compliance Dates:** BAAs entered into before January 25, 2013 must be amended by September 23, 2014. BAAs entered into after January 25, 2013 must be amended by September 23, 2013.
- **Executive Summary:** Business Associates are directly liable for uses and disclosures of PHI that violate the Privacy Rule or the terms of a BAA. Business Associates are directly liable for violations of applicable provisions of the Security Rule. Civil money penalty liability under the Privacy Rule will extend directly to Business Associates and their subcontractors who create or use PHI pursuant to a BAA ("Subcontractors"). Business Associates and Subcontractors will be required to report breaches of unsecured PHI to Covered Entities for the purpose of advancing further notification by Covered Entities to HHS. BAAs should be revised to comply with the Final Rule before the applicable compliance dates.

Business Associates should enter into compliant BAAs with their Subcontractors. Business Associates must also comply with the Security Rule for electronic PHI and may be subject to penalties for noncompliance.

- **Discussion:** One of the most significant changes under the Final Rule is that Business Associates and their Subcontractors are now directly liable for certain violations of the Security Rule and uses and disclosures of PHI in violation of the Privacy Rule. Business Associates and their Subcontractors are also made subject to the Privacy Rule's anti-retaliation provisions. Previously, Business Associates and Subcontractors were liable only under agreements with Covered Entities. Business Associates will be subject to compliance reviews by HHS and to investigations by HHS upon a filing of a complaint against a Business Associate. Other obligations of Business Associates and their Subcontractors will include the following:

  - To keep records and submit compliance reports to HHS when HHS requires such disclosure in order to investigate the Business Associate's compliance and to cooperate with complaint investigations and compliance reviews;
  - To disclose PHI as needed by a Covered Entity to respond to an individual's request for an electronic copy of PHI;
  - To notify a Covered Entity of any breach of unsecured PHI; and
  - To make reasonable efforts to limit use and disclosure of PHI and requests for PHI to the minimum necessary.

The rules governing Business Associates will extend down the entire line of their Subcontractors to the extent that PHI is involved. Moreover, Business Associates will be required to obtain assurances (typically, but not necessarily, through BAAs[22]) that Subcontractors will appropriately safeguard PHI. A Business Associate that becomes aware of noncompliance by its Subcontractors will be subject to the same requirements under the Privacy Rule that currently apply to Covered Entities who become aware that their Business Associates are noncompliant,[23] which can include delivering notice to the Covered Entity, fixing the breach, terminating the subcontractor BAA, and/or reporting the noncompliance to HHS.

From and after the applicable compliance dates, BAAs will need to require Business Associates to: (i) comply, where applicable, with the Security Rule with regard to electronic PHI, (ii) report breaches of unsecured PHI to Covered Entities, and (iii) ensure that any subcontractors that create or receive PHI on behalf of the Business Associate agree to the same restrictions and conditions that apply to the Business Associate. BAAs must also establish contractual liability for Business Associates if a Covered Entity delegates to the Business Associate certain Privacy Rule obligations that are not subject to direct civil monetary penalty liability (e.g., distributing notices of privacy practices or amending PHI pursuant to an individual's request). Business Associates and their Subcontractors should perform risk assessments and revise and/or enter into BAAs in order to comply with this change, particularly in light of the greater penalties and enforcement.

NOTICES OF PRIVACY PRACTICES

- **Regulations:** 45 C.F.R. § 164.520
- **Compliance Dates:** Changes must be displayed at offices and facilities and on web sites by September 23, 2013. New notices by health plans must be delivered in the next annual mailings to enrollees or during the next open enrollment period.
- **Executive Summary:** The Final Rule introduced several significant changes to the requirements related to a Covered Entity's notices of privacy practices ("NPP"). Many of these changes are related to substantive changes to other provisions in the Privacy Rule and the substance of those changes is discussed in other sections of this Commentary (e.g., marketing, fundraising, changes related to restrictions on disclosures of PHI to health plans, breach notification). In order to have a HIPAA-compliant NPP, Covered Entities will need to revise and redistribute their current NPPs to align with the new requirements of the Final Rule by the applicable compliance date.

Authorizations. OCR clarified that the Privacy Rule does not require the NPP to include a list of all situations requiring authorization, which would have led to cumbersome NPPs. OCR explained that an NPP must contain a statement indicating that an individual's authorization must be obtained for (i) most uses and disclosures of psychotherapy notes (if the Covered Entity records or maintains psychotherapy notes), (ii) uses and disclosures of PHI for marketing purposes, and (iii) disclosures that constitute a sale of PHI. Further, the NPP must state that other uses and disclosures not described in the NPP will be made only with authorization from the individual.

Breach Notification. Covered Entities are now required to include a statement in their NPPs regarding the right of affected individuals to be notified following a breach of unsecured PHI. OCR clarified that this requirement may be satisfied with a simple statement that an individual has a right to or will receive notifications of breaches of his or her unsecured PHI. In response to comments that this requirement would add undue complexity and length to NPPs, OCR noted that the statement did not need to address the specifics of how the Covered Entity would address the breach notification process. For example, the NPP does not need to describe how the Covered Entity will conduct a risk assessment, include the legal analysis or detail regarding the

definitions of terms such as "breach" or "unsecured PHI," or describe the types of information that will be provided to the individual if there is a breach of unsecured PHI. OCR noted that Covered Entities may include such information, but due to concerns over the NPP's length and issues related with revising an NPP, Covered Entities need to carefully consider whether including such additional information is beneficial.

Fundraising. A Covered Entity that will use or disclose PHI for fundraising must continue to describe such intended use and disclosure in its NPP. There is a new requirement, however, that the NPP include a statement that the individual may opt-out of fundraising communications. The NPP does not need to describe the opt out mechanism because the fundraising communication itself will need to include a description of the opt-out process.

Restriction on Health Plan Disclosure. NPPs must be revised to describe the right of individuals to restrict certain disclosures of PHI to a health plan if the individual pays out of pocket in full for the health care item or service this new right. This requirement applies only to Covered Entities that are health care providers. OCR clarified that other Covered Entities may retain the existing language indicating that a Covered Entity is not required to agree to a requested restriction on the use and disclosure of PHI. In most instances, health care providers will be able to address this new right as an exception to existing language related to requested restrictions.

GINA. If a Covered Entity is a health plan (other than certain issuers of a long-term care policies) and it intends to use or disclose PHI for underwriting purposes, that Covered Entity's NPP must include a statement that the Covered Entity is prohibited from using or disclosing PHI that is genetic information of an individual for underwriting purposes.

Appointment Reminders. Previously, NPPs needed to contain a statement that the Covered Entity may contact an individual to provide appointment reminders or information about treatment alternatives or other health-related benefits and services that may be of interest to the individual. Because of changes to the definition of "marketing" under the Final Rule, this language is no longer necessary.

Distribution of Revised NPPs. OCR indicated that the changes to the NPPs required under the Final Rule are material changes, which therefore require distribution of revised NPPs. OCR believes the modifications to the Privacy Rule NPP standards "are significant and are important to ensure that individuals are aware of the HITECH Act changes that affect privacy protections and individual rights regarding protected health information."[24]

Distribution of NPPs—Health Plans. If a health plan currently posts its NPP on its web site, it must (i) prominently post the material change or its revised NPP on its web site by the effective date of the material change (which, to be in compliance with the Privacy Rule, must be no later than September 23, 2013) and (ii) provide the revised NPP (or information about the material change and how to obtain the revised NPP) in its next annual mailing to individuals then covered by the plan. The next annual mailing would likely be at the beginning of the plan year or during the open enrollment period. If a health plan does not have a customer service web site, it must provide the revised NPP (or information about the material change and how to obtain the revised NPP) to individuals covered by the plan within 60 days of the material revision to the NPP.

Distribution of NPPs—Health Care Providers. The Final Rule does not modify the Privacy Rule's requirements to distribute revised versions of an NPP. When a health care provider with a direct treatment relationship with an individual revises its NPP, the health care provider must make the NPP available upon request on or after the effective date of the revision as well as making the NPP available at the delivery site and posting the NPP in a clear and prominent location at the covered entity's facility. To counter arguments that requiring the distribution of revised NPPs would create a burden (through printing costs and personnel time), OCR clarified that health care providers are not required to print and hand out a revised NPP to all individuals seeking treatment. Instead, health care providers must post the revised NPP in a clear and prominent location and make copies of the NPP available to individuals at the care delivery site. The requirement to provide a copy of the NPP to, and obtain a good faith acknowledgment of receipt from, an individual applies only to new patients. In sum, OCR believes placing these requirements on health care providers is neither overly burdensome nor costly. Revised NPPs that meet the requirements described above must be displayed and available for pick up at offices and facilities by September 23, 2013.

Notices to Those with Disabilities. If a covered entity is required to comply with Section 504 of the Rehabilitation Act of 1973 or the Americans with Disabilities Act of 1990, the covered entity must ensure effective communication with individuals with disabilities, including communication of its NPP. Depending on the individuals who receive services, a covered entity could meet this obligation by making the revised NPP or notice of material changes to the NPP available in alternate formats (e.g., Braille, large print, or audio).

GENETIC INFORMATION NONDISCRIMINATION ACT

- **Regulations:** 45 C.F.R. §§ 160.103 164.506 164.514
- **Compliance Date:** September 23, 2013
- **Executive Summary:** Most Covered Entity health plans will be prohibited from using or disclosing genetic information for underwriting purposes.

GINA[25] prohibits discrimination based on an individual's genetic information in both the health coverage and employment contexts. GINA also contains provisions protecting the privacy of genetic information, which require the Secretary of HHS to prohibit group health plans, health insurance issuers (including HMOs), and issuers of Medicare supplemental policies from using or disclosing genetic information for underwriting purposes.

The new regulations promulgated under GINA as part of the Final Rule incorporate "genetic information" into the definition of "health information" under the Privacy Rule. "Genetic information" includes information about: (i) an individual's genetic tests, (ii) the genetic tests of family members of such individual, and (iii) the manifestation of a disease or disorder in family members of such individual (i.e., family medical history). GINA also provides that the term "genetic information" includes any request for, or receipt of, genetic services or participation in clinical research that includes genetic services by an individual or family member of such individual.

The Final Rule also extends the prohibition against using or disclosing genetic information for underwriting purposes to all "health plans" that are Covered Entities. This will capture more entities under this prohibition than set forth in the GINA statute, including dental and vision benefit plans, and all employee welfare benefits plans that provide health benefits, but will exclude issuers of long-term care policies.[26] Health plans must also include provisions relating to genetic information in their NPPs as described above.

MARKETING PRACTICES

- **Regulations:** 45 C.F.R. §§ 164.501, 164.508(a)(3)
- **Compliance Date:** September 23, 2013
- **Executive Summary:** The Final Rule requires patient authorizations in additional contexts by expanding the definition of "marketing" to include communications for treatment and health care operations purposes where the Covered Entity receives "financial remuneration" for making those communications.

The Final Rule requires individual authorization for a broader scope of marketing practices than HIPAA has historically. Existing regulations provide that communications relating to certain treatment and health care operations purposes are categorically carved out of the definition of "marketing" and therefore do not require patient authorization. Thus, a Covered Entity using PHI in connection with such communications need not have authorization from affected individuals—even if the Covered Entity is paid to make such communications by a third party. The Final Rule narrows that carveout: "Marketing" is now defined to include any communications for such treatment and health care operations purposes if the Covered Entity "receives financial remuneration in exchange for making the communication." "Financial remuneration" is defined for this purpose as "direct or indirect payment from or on behalf of a third party whose product or service is being described." OCR also clarifies that 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.[27]

The issue of whether a Covered Entity receives financial remuneration is central to an analysis of whether authorization is required for a given communication under the Final Rule. Beginning on the compliance date, the Final Rule will, for example, require authorization for a Covered Entity to send a mailing to its patients regarding its acquisition of new state-of-the-art medical equipment if the communication is paid for by the manufacturer of that equipment.[28] However, the Final Rule would not require authorization if the mailing about that equipment were paid for by a local charitable organization (or other unrelated third party) whose products or services were not described in the communication.[29] Notably, in order to fit the "marketing" definition, the financial remuneration that 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. OCR noted that if the financial remuneration received by the Covered Entity is for any purpose other than for making the communication, then the marketing provision does not apply.[30] For example, in OCR's analysis, if a third party funded a Covered Entity's implementation of a disease management program, the Covered Entity could nevertheless provide individuals with communications about that program without obtaining individual authorization because those communications would not encourage the individuals to use or purchase the third party's product or service.[31] Additionally, OCR opines that it would not be considered marketing, and no authorization would be required, if a hospital sent flyers to its patients about a new

hospital wing, where funds for that wing were donated by a third party.[32] Under OCR's analysis, the hospital would have received financial remuneration, but not in exchange for the mailing of the flyers.[33]

The Final Rule also provides that a Covered Entity making marketing communications that involve financial remuneration 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.[34] This authorization must contain the elements and statements of a valid authorization under 45 C.P.R. § 164.508(c), including adequate descriptions of the intended purposes of the requested uses and disclosures (i.e., the scope of the authorization) and a clear statement in the authorization that the individual may revoke the authorization at any time he or she wishes to stop receiving the marketing material.

Notably, the Final Rule includes a new categorical exception from the definition of "marketing" applicable to refill reminders or other communications about a drug or biologic currently being prescribed to an individual. The Final Rule permits Covered Entities to receive financial remuneration for these communications as long as the amounts received are reasonably related to the cost of making the communications. OCR clarifies that 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.[35] If the remuneration generates a profit or includes payment for other costs, it would run afoul of the "reasonably related" language. OCR acknowledges that it received many comments inquiring about the scope and breadth of this exception, and while OCR indicates its intent to provide further guidance with respect to the wide variety of situations it was presented by commenters, it does specify that the scope of the exception included (i) communications about the generic equivalent of a drug being prescribed to an individual, (ii) adherence communications encouraging individuals to take their prescribed medication as directed, and (iii) where an individual is prescribed a self-administered drug or biologic, communications regarding all aspects of a drug delivery system, such as an insulin pump.[36]

SALES OF PHI

- **Regulations:** 45 C.F.R. §§ 164.508(a)(4), 164.502(a)(5)(ii)
- **Compliance Date:** September 23, 2013
- **Executive Summary:** The Final Rule provides restrictions on payments for disclosures of PHI by Covered Entities or Business Associates that are authorized by the Privacy Rule.

The Final Rule generally prohibits the sale of PHI by a Covered Entity or Business Associate unless (i) the Covered Entity or Business Associate receives an authorization that states that the authorized use of PHI will result in direct or indirect remuneration to it or (ii) one of several exceptions applies. Exceptions to the PHI sale prohibition under the Final Rule include a general exception for remuneration for disclosures authorized by the Privacy Rule and a specific exception for research purposes; however, each of these exceptions applies only if that remuneration is limited to a reasonable, cost-based fee for the preparation and transmittal of the PHI. The Final Rule provides other exceptions with no cost-based cap on permissible payment amounts, including exceptions for (i) disclosures made for purposes of certain public health activities, (ii) disclosures for treatment and payment, (iii) disclosures made in connection with the sale, transfer, merger, or consolidation of a Covered Entity (and related due diligence where the recipient is, or will become, a Covered Entity), and (iv) disclosures required by law.

While outright sales of PHI without authorization have never been permitted under HIPAA, existing regulations do not impose restrictions on payments for disclosures of PHI that are authorized by the Privacy Rule.

FUNDRAISING

- **Regulations:** 45 C.F.R. § 164.514(f)
- **Compliance Date:** September 23, 2013
- **Executive Summary:** The Final Rule permits a Covered Entity to use additional types of PHI in connection with its fundraising efforts (e.g., department of service or treating physician), but such uses are held to more stringent standards.

The Final Rule expands the scope of PHI that may be used for fundraising purposes without receiving an authorization. In addition to an individual's demographic information and dates of service authorized under existing regulations, the Final Rule permits a Covered Entity to use or disclose to a Business Associate or institutionally related foundation the individual's department of service, treating physician, outcome information, and health insurance status. This expansion permits Covered Entities to employ more targeted fundraising efforts and to avoid sending communications to patients or families who have suffered negative outcomes.

The Final Rule also subjects fundraising uses and disclosures to the following additional requirements:

- While prior fundraising communications were required to be accompanied by a description of a means by which the recipient could opt out of further fundraising

communications, as of the compliance date of the Final Rule, that opt-out mechanism must (i) be "clear and conspicuous" and (ii) not require the individual to incur an undue burden or more than a nominal cost. OCR clarifies that Covered Entities are free to decide which methods individuals can use to opt out of receiving further fundraising communications, as long as the chosen methods meet this undue burden or nominal cost requirement.[37] In OCR's view, requiring an individual to write an opt-out letter would be an undue burden for this purpose and recommends that Covered Entities consider the use of a toll-free phone number, email address, or similar opt-out mechanism.[38] Notably, the Final Rule provides that a Covered Entity may provide an individual who has opted out of further fundraising communications with a method to opt back in.

- A Covered Entity may not condition treatment or payment on an individual's choice with respect to receipt of fundraising communications.
- A Covered Entity may not make fundraising communications to an individual who has elected not to receive communications. This is a higher standard than that required by existing regulations, which merely require a Covered Entity to make "reasonable efforts" to ensure that communications are not sent to an individual who has opted out. OCR acknowledged that this higher standard will require Covered Entities to promptly reconcile their mailing lists and their opt-out lists, noting that "[Covered Entities] voluntarily choosing to send fundraising communications to individuals must have data management systems and processes in place to timely track and flag those individuals who have opted out of receiving fundraising communications to ensure that they are not sent additional fundraising communications."[39]

PATIENT RIGHTS

- **Regulations:** 45 C.F.R. §§ 164.502(f), 164.512(b)(1)(vi), 164.522(a)(1)(vi), 164.524(c)
- **Compliance Date:** September 23, 2013
- **Executive Summary:** The Final Rule makes a number of minor changes with respect to patient rights, most notably that the right of patients to access electronic copies of their PHI will now extend to any kind of PHI stored electronically in a designated record set.

The Final Rule provides the following changes with respect to patient rights:

Electronic PHI. The Final Rule expands individuals' rights to access their electronic PHI. HIPAA originally provided that an individual has the right to PHI in the form or format requested, or such other form or format as the individual and Covered Entity may agree. The HITECH Act provided further that, if a Covered Entity maintained PHI in an electronic health record ("EHR"), a requesting individual has a right to that EHR. The Final Rule broadens this requirement: If a Covered Entity maintains PHI electronically in one or more designated record sets (i.e., whether or not an EHR), it must provide an individual requesting an electronic copy of that information with access in the form and format requested, or such other form or format as the individual and Covered Entity may agree.[40]

The Final Rule also provides a shorter window for Covered Entities to respond to individuals' access requests, requiring responses within 30 days with a single 30-day extension permitted where the Covered Entity provides the individual with a written statement of the reasons for the delay and a date by which the request will be completed.[41] This effectively reduces the response time for PHI that is not maintained or accessible on-site by 30 days as compared with the regulations in effect prior to the compliance date.

Deceased Individuals. Under the Final Rule, a Covered Entity's obligations to an individual cease 50 years following his or her death.[42] Prior regulations provided no such limitation.

School Immunizations. The Final Rule permits Covered Entities to release a student's proof of immunization to a school without a written authorization, provided that the school is required by the state to have such proof prior to admitting the student and the Covered Entity obtains and documents the agreement (which may be verbal) to the disclosure from a parent, guardian, or other person acting *in loco parentis* for the student, or from the student, if he or she is an adult or emancipated minor.[43] This policy is intended to obviate the need for a formal, written authorization, but the Covered Entity must, nevertheless, document the agreement to disclose, such as by saving an email communication to that effect or by noting a phone call in the student's medical record.[44]

Restrictions on Disclosure of PHI to Health Plans. The Final Rule requires a Covered Entity to agree to an individual's request to restrict disclosures of PHI to a health plan if the disclosure pertains solely to a health care item or service for which the individual (or a person other than the health plan on the individual's behalf) has paid in full out of pocket, provided that the disclosure is not required by law.[45]

CLINICAL RESEARCH

- **Regulations:** 45 C.F.R. § 164.508(b)(3)(iii)
- **Compliance Date:** September 23, 2013

- **Executive Summary:** The Final Rule permits (i) compound authorizations involving unconditioned authorizations and certain research-related conditioned authorizations and (ii) general authorizations for future research under certain circumstances.

The Final Rule makes two key changes regarding clinical research authorizations:

Compound Authorizations for Research Uses and Disclosures. HIPAA generally prohibits a Covered Entity from conditioning treatment, payment, enrollment in a health plan, or eligibility for benefits on the signing of use or disclosure authorizations except in certain circumstances, including the conditioning of research-related treatment on the provision of an authorization relating to that research. Prior to the Final Rule, a Covered Entity was prohibited from combining an individual's properly conditioned authorization with an authorization for a purpose that could not be conditioned.

The Final Rule permits a Covered Entity to combine conditioned and unconditioned authorizations for most kinds of research,[46] provided that the combined authorization clearly differentiates between the conditioned and unconditioned research components and clearly allows the individual the option to opt in to the unconditioned research activities.[47] OCR intends this softening of the restriction on compound authorizations to reduce costs for the research community by eliminating the need for multiple forms for research studies (such as those featuring a clinical trial and a related biospecimen banking activity) and making patient authorization requirements under the Privacy Rule consistent with existing informed consent requirements.[48]

As a practical matter, this change permits researchers with some flexibility in meeting the authorization requirements for their research. For example, Covered Entities may minimize redundant language by describing an unconditioned research activity on a separate page of a compound authorization or cross-reference relevant sections of a compound authorization. OCR also leaves to the discretion of the Covered Entity whether to have separate signatures for each activity in a compound authorization or a single signature with check boxes indicating the individual's opt-in to each authorization.[49]

Authorizations for Future Research Uses or Disclosures. OCR has previously interpreted the Privacy Rule to require that authorizations for research be study-specific for purposes of complying with the requirement that an authorization include a description of each purpose of the requested use or disclosure.[50] In the Final Rule, research authorizations need not be study-specific, provided that they describe future uses or disclosures sufficiently to enable individuals to reasonably expect that their PHI could be used or disclosed for future research.

PENALTIES AND ENFORCEMENT

- **Regulations:** 45 C.F.R. §§ 160.306(c), 160.308, 160.401, 160.408, 160.410
- **Effective Date:** March 26, 2013
- **Executive Summary:** The Final Rule adopts all changes to the enforcement rules required by the HITECH Act and not previously implemented in the Interim Rule. These changes generally bolster OCR's enforcement powers.

Changes to the penalty and enforcement provisions under the Privacy and Security Rules include the following:

Additional Actions Relating to Willful Neglect. When a preliminary review of facts relating to a complaint indicates a possible violation due to willful neglect, (i) OCR is required to investigate, and (ii) OCR will conduct a compliance review.

Amount of Civil Monetary Penalties. The Final Rule adopts the range and scope of civil monetary penalties set forth in the Interim Rule:[51]

- **Did Not Know:** $100–$50,000 per violation ($1.5 million calendar year cap)
- **Reasonable Cause:** $1,000–$50,000 per violation ($1.5 million calendar year cap)
- **Willful Neglect, Corrected:** $10,000–$50,000 per violation ($1.5 million calendar year cap)
- **Willful Neglect, Not Corrected:** $50,000 per violation ($1.5 million calendar year cap)

While the amounts and categories are unchanged, the Final Rule revises the definition of "reasonable cause" to mean "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."

Factors Considered in Determining the Amount of a Civil Monetary Penalty. The Final Rule clarifies that OCR will consider the following factors in determining an offending party's liability, each of which may be mitigating or aggravating:[52]

- The nature and extent of the violation;
- The nature and extent of the harm resulting from the violation;
- The history of prior noncompliance;
- The financial condition of the offending party; and
- Such other matters as justice may require.

Notably, OCR clarifies in commentary to the Final Rule that the financial condition of the offending party could affect the amount of civil monetary penalties in either direction. For example, an entity in poor financial condition may face a lesser penalty if that condition affected its ability to comply, while an entity with greater financial resources may be subject to higher penalties in part because it had the resources to maintain compliance.[53]

Business Associates. As discussed under the heading "Business Associates and Business Associate Agreements" above, a Business Associate is subject to civil monetary penalties under the Final Rule if OCR determines that it has violated applicable HIPAA provisions.

Liability for Agents. The Final Rule provides that a Covered Entity is liable under federal common law of agency for violations resulting from the acts or omissions of its agents, including Business Associates. This change removes a previously effective carve-out to vicarious liability for a Covered Entity where the Covered Entity was complying with the terms of a valid Business Associate Agreement. Business Associates, in turn, are similarly liable for violations resulting from the acts or omissions of their own agents, including Subcontractors.[54]

NOT THE FINAL WORD

Despite the breadth of this final rulemaking effort by OCR, future rulemaking and guidance will be provided requiring industry stakeholders to continue to review and assess internal practices and procedures for privacy compliance. For instance, the Final Rule does not address previously published proposed rulemaking regarding the accounting for disclosures requirement in section 13405 of HITECH. Additionally, rulemaking regarding the distribution of a percentage of certain civil monetary penalties or monetary settlement to an individual affected by a violation of the Privacy Rule or Security Rule as a requirement of section 13410(c) of HITECH remains outstanding. Throughout the Final Rule, OCR includes comments and references to future guidance that will be available to Covered Entities and Business Associates. The significance of the Final Rule may be less than the finality on outstanding rulemaking and guidance, but signaling a new era of future and ongoing privacy rulemaking and guidance outside of formal rulemaking processes. As such, stakeholders are best served by engaging in a careful and meaningful review of the Final Rule. They should also coordinate with internal and external resources to implement responsive measures to establish and maintain ongoing privacy compliance procedures that will be effective in mitigating risks related to audits and investigations and substantial penalties for alleged noncompliance.

LAWYER CONTACTS

For further information, please contact your principal Firm representative or one of the lawyers listed below. General email messages may be sent using our "Contact Us" form, which can be found at www.jonesday.com.

Jeffrey L. Kapp
Cleveland
+1.216.586.7230
jlkapp@jonesday.com

Kevin D. Lyles
Columbus
+1.614.281.3821
kdlyles@jonesday.com

Claire E. Castles
Los Angeles
+1.213.243.2629
ccastles@jonesday.com

Colin S. Leary
San Francisco
+1.415.875.5795
cleary@jonesday.com

Soleil E. Teubner
San Francisco
+1.415.875.5709
steubner@jonesday.com

ENDNOTES

1 The Final Rule modifies the statutory exception applicable to unintentional acquisition, access, or use of PHI by an employee to a substituted term of "workforce members" given its definition within and for the purposes of the HIPAA Rules to include employees, volunteers, trainees, and other persons whose conduct is under the direct control of a Covered Entity or Business Associate.

2 *See* 78 Fed. Reg. 5566, 5644 (January 25, 2013).

3 *See* 78 Fed. Reg. 5566, 5643 (January 25, 2013).

4 *See* 78 Fed. Reg. 5566, 5642 (January 25, 2013).

5 *See* 78 Fed. Reg. 5566, 5643 (January 25, 2013).

6 *See id.*

7 *See id.*

8 *See id.*

9 *See id.*

10 *See* 78 Fed. Reg. 5566, 5647 (January 25, 2013).

11 *See id.*

12 *See id.*

13 *See* 78 Fed. Reg. 5566, 5648 (January 25, 2013).

14 *See* 78 Fed. Reg. 5566, 5649 and 5649 (January 25, 2013).

15 *See* 78 Fed. Reg. 5566, 5651 (January 25, 2013).

16 *See* 78 Fed. Reg. 5566, 5651 (January 25, 2013).

17 *See* 78 Fed. Reg. 5566, 5653 (January 25, 2013).

18 *See id.*

19 *See* 78 Fed. Reg. 5566, 5654 (January 25, 2013).

20 *See id.*

21 *See id.*

22 OCR declined to create a new classification of agreements for Subcontractors (e.g., Subcontractor Agreements) and suggested that Business Associates need to enter into Business Associate Agreements with Subcontractors, as appropriate. 78 Fed. Reg. 5566, 5573, 5677 (January 25, 2013).

23 78 Fed. Reg. 5566, 5600 (January 25, 2013).

24 78 Fed. Reg. 5566, 5625 (January 25, 2013).

25 Public Law 110–233, 122 Stat. 881 (2008).

26 *See* 78 Fed. Reg. 5566, 5659, and 5660 (January 25, 2013).

27 *See* 78 Fed. Reg. 5566, 5595 (January 25, 2013).

28 *See* 78 Fed. Reg. 5566, 5593 (January 25, 2013).

29 *Id.*

30 *Id.*

31 *Id.*

32 *Id.*

33 *See id.* We note that OCR explicitly states that, in its example of a hospital that publishes a flyer about a new wing donated by a third party, the hospital would have received "financial remuneration" for purposes of the marketing rule. We believe that this analysis is flawed because a communication describing a donated hospital wing is not describing a product or service of the donor, as is required to fall within the definition of "financial remuneration." However, we agree with OCR's ultimate conclusion that the distribution of such a flyer by a hospital would not be "marketing" under the Final Rule.

34 *See* 45 C.F.R. § 164.508(a)(3).

35 *See* 78 Fed. Reg. 5566, 5593 (January 25, 2013).

36 *Id.*

37 *See* 78 Fed. Reg. 5566, 5619 (January 25, 2013).

38 *See id.*

39 *See* 78 Fed. Reg. 5566, 5621 (January 25, 2013).

40 *See* 45 C.F.R. § 164.524(c).

41 *See* 45 C.F.R. § 164.524(b)(2)(ii).

42 *See* 45 C.F.R. § 164.502(f).

43 *See* 45 C.F.R. § 164.512(b)(1)(vi).

44 *See* 78 Fed. Reg. 5566, 5684 (January 25, 2013).

45 *See* 45 C.F.R. § 164.522(a)(1)(vi).

46 Notably, the Final Rule does not relax standards for authorizations relating the use or disclosure of psychotherapy notes. Whether research-related or not, such authorizations may only be combined with another authorization for a use or disclosure of psychotherapy notes. *See* 78 Fed. Reg. 5566, 5610 (January 25, 2013).

47 OCR clarifies that combined authorizations cannot require individuals to opt-out of unconditioned research activities (e.g., "check here if you do NOT want your data provided to the biospecimen bank"). *See* 78 Fed. Reg. 5566, 5610 (January 25, 2013).

48 *See* 78 Fed. Reg. 5566, 5610, 5683 (January 25, 2013).

49 *See* 78 Fed. Reg. 5566, 5610, 5611 (January 25, 2013).

50 *See* 78 Fed. Reg. 5566, 5611-5613 (January 25, 2013).

51 *See* 78 Fed. Reg. 5566, 5583 (January 25, 2013).

52 *See* 45 C.F.R. § 160.408.

53 *See* 78 Fed. Reg. 5566, 5585 (January 25, 2013).

54 *See* 45 C.F.R. § 164.402(c).