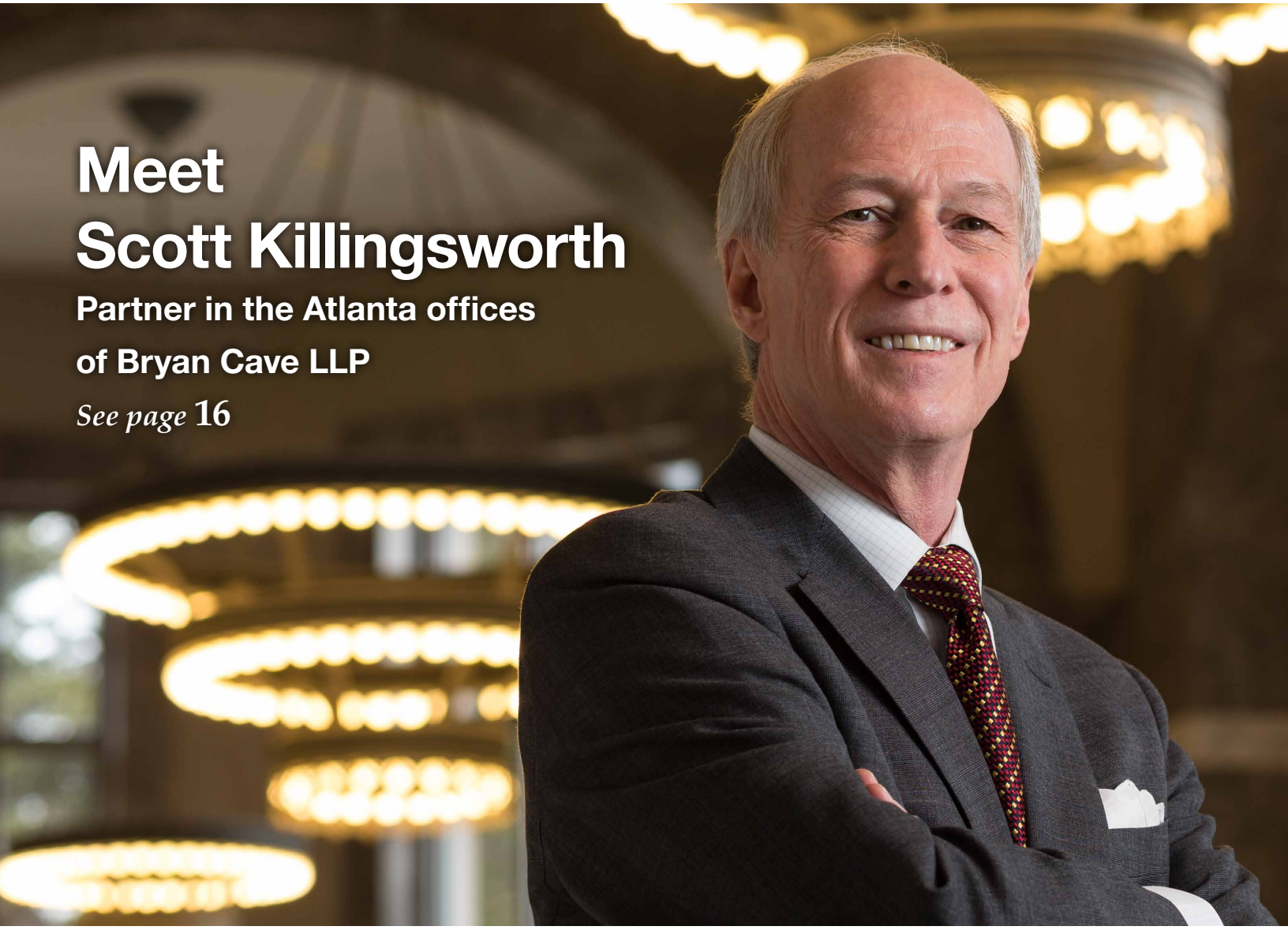
HCCA HEALTH CARE COMPLIANCE ASSOCIATION

Compliance TODAY

May 2013

A PUBLICATION OF THE HEALTH CARE COMPLIANCE ASSOCIATION

WWW.HCCA-INFO.ORG



Meet Scott Killingsworth

Partner in the Atlanta offices of Bryan Cave LLP

See page 16

25
Medicare Coverage Analysis: Protecting your institution
Alexandra Burleigh

31
How does your RAC stack up?
Jason T. Lundy

36
Complying with the new HIPAA Omnibus Rule: Part 1
Adam H. Greene, Rebecca L. Williams, Louisa Barash, and John Hodges-Howell

43
The Lilly FCPA enforcement action: Key lessons learned
Thomas Fox

by Adam H. Greene, JD, MPH; Rebecca L. Williams, JD, RN; Louisa Barash, JD; and John Hodges-Howell, JD

Complying with the new HIPAA Omnibus Rule: Part 1

» Entities must comply with HIPAA Omnibus Rule by September 23, 2013.
» Breach notification has gone from a "harm" to a "compromise" standard.
» Breach risk assessments must meet minimum content requirements.
» The new rule puts limits on marketing, sale of PHI, and fundraising opt-outs.
» The new rule has more flexibility for fundraising, research, immunization records, and decedent information.

Adam H. Greene *(adamgreene@dwt.com) is a Partner in the Washington DC office of Davis Wright Tremaine LLP and Co-Chair of its Health Information Practice Group.* ***Rebecca L. Williams*** *(beckywilliams@dwt.com) is a Partner in the Seattle office of Davis Wright Tremaine LLP and Co-Chair of its Health Information Practice Group.* ***Louisa Barash*** *(louisabarash@dwt.com) is a Partner in the Seattle office of Davis Wright Tremaine LLP.* ***John Hodges-Howell*** *(johnhodgeshowell@dwt.com) is an Associate in the Seattle office of Davis Wright Tremaine LLP.*


Greene


Williams


Barash


Hodges-Howell

This is the first part in a two-part series designed to assist you in understanding the new rule and updating your organization's compliance program. Part 1 focuses on changes to the breach notification standard and new limits and flexibility on uses and disclosures of PHI. Part 2 will explain new requirements for business associates and subcontractors, enhancements for patient rights, and enforcement clarifications.

On Jan. 17, 2013, the Department of Health and Human Services (HHS) released the long-awaited "Omnibus Rule,"[1] which amends a wide range of privacy, security, and breach notification requirements under the Health Insurance Portability and Accountability Act (HIPAA)[2] and the Health Information Technology for Economic and Clinical Health (HITECH) Act.[3] The Omnibus Rule represents the most comprehensive set of changes to the HIPAA regulations since their inception, and it is important to understand how the changes apply to your organization.

For starters, the Rule modifies the breach notification standard; imposes new rules governing uses and disclosures of protected health information (PHI) in areas such as marketing, sale of PHI, and disclosure of decedent information; enhances patient rights to access and to restrict disclosure of PHI; expands certain HIPAA obligations to business associates and their subcontractors; clarifies enforcement approaches; and addresses privacy obligations for health plans under the Genetic Information and Nondiscrimination Act of 2008 (GINA).[4] Covered entities and business associates generally must comply with these changes by September 23, 2013, although they have up to an additional year to amend existing business associate agreements.

Regulatory history

The Omnibus Rule earned this nickname because it finalizes four separate interim final or proposed rules: an interim final HIPAA breach notification rule (Aug. 2009); interim final changes to HIPAA's enforcement provisions (Oct. 2009); a proposed rule

to implement the HIPAA provision of GINA (Oct. 2009); and a proposed set of amendments to HIPAA's privacy, security, and enforcement provisions (July 2010) to implement the HITECH Act and to improve the workability of the regulations in response to longstanding concerns. Although the Omnibus Rule addresses much of the HITECH Act, HHS has yet to issue final regulations addressing the accounting of disclosures requirements and the distribution of a portion of HIPAA settlements and penalties to harmed individuals.

New breach standard

Changes to the breach notification standard create new uncertainty. The Omnibus Rule materially revises the definition of a breach, which seems to make breach notification more likely. The HITECH Act requires covered entities and business associates to notify affected individuals, HHS, and in some cases, the media following discovery of a breach of unsecured PHI. Breach means the acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule[5] that "compromises the security or privacy" of the PHI. Under the interim final Breach Notification Rule, the privacy or security of PHI was deemed to be compromised if there was a significant risk of financial, reputational, or other harm to the individual as a result of the impermissible use or disclosure of PHI (commonly referred to as the "harm standard").

The harm standard arguably was the most controversial aspect of the interim Breach Rule. Commenters who opposed the harm standard (including certain members of Congress) argued that it set too high a bar for triggering breach notification and that it was too subjective, resulting in inconsistent interpretations. The Omnibus Rule replaces this "harm standard" with (according to HHS) a more objective process for assessing whether PHI has been compromised. The new standard, however, still appears to leave covered entities and business associates with a lot of questions.

The Omnibus Rule amends the definition of breach to clarify that the impermissible acquisition, access, use, or disclosure of PHI is presumed to be a breach, and breach notification is necessary unless a covered entity or business associate can demonstrate, through a documented risk assessment, that there is a low probability that the PHI has been compromised. To do so, the Omnibus Rule identifies four factors that must be considered in a risk assessment:

- The nature and extent of the PHI involved
- The unauthorized person who used the PHI or to whom the disclosure was made
- Whether the PHI actually was acquired or viewed
- The extent to which the risk to the PHI has been mitigated

The Preamble to the Omnibus Rule provides significant discussion of how to apply these factors, and notes that other factors may be considered where necessary. The big question is what exactly is meant by the "compromise" of PHI. Other than the four factors listed above and a number of examples, HHS does not define the term. Many interpret that the modified standard does not significantly alter the prior analysis under the harm standard. Officials from the HHS Office for Civil Rights have stated that the new standard focuses more on the unauthorized use of the PHI, rather than the potential impact on individuals. HHS states that it will issue additional guidance in the future to aid covered entities and business associates in performing risk assessments with respect to frequently occurring scenarios, and recent statements by HHS suggest that a breach notification assessment tool is in the works.

Additionally, the Omnibus Rule deletes an exception for certain limited data sets. The

interim final Breach Notification Rule included an exception to the definition of "breach" for limited data sets that also did not include birthdates or ZIP codes. The Omnibus Rule, however, removes this exception, subjecting any acquisition, access, use, or disclosure of such a data set to breach notification or to a risk assessment to demonstrate a low probability of compromise.

Also, the Omnibus Rule clarifies the deadline for reporting small breaches (those involving less than 500 individuals) to HHS. For breaches affecting fewer than 500 individuals, the Omnibus Rule clarifies that covered entities must notify HHS within 60 days after the end of the calendar year in which the breaches were "discovered," not in which the breaches occurred.

New restrictions and flexibility on using and disclosing PHI

Fundraising

HHS offered some welcome news to health care providers by expanding the use and disclosure of PHI for fundraising purposes. Previously, a covered entity could use or disclose only demographic information and dates of service for fundraising. A longstanding complaint among health care providers has been that these limits do not allow appropriate targeting of fundraising efforts. In response, HHS expanded the categories of PHI that may be used and disclosed for fundraising to also include department of service, treating physician, outcome information, and health insurance. Accordingly, a health care provider seeking to raise funds for a new cancer center, for example, can target its efforts to oncology patients who had positive outcomes and are not on Medicaid or uninsured.

Further, the HITECH Act requires covered entities to provide individuals with greater opportunity to opt out of receiving fundraising communications. The Privacy Rule already

required an opportunity to opt out with each fundraising communication, but the Omnibus Rule requires that the opportunity to opt out be "clear and conspicuous," that the method for doing so not require an undue burden, and that the covered entity not make fundraising communications to the individual after the individual has opted out. Covered entities may, however, provide an individual who has opted out with a method to opt back in to future fundraising communications. In addition, the Omnibus Rule requires the covered entity's Notice of Privacy Practices to indicate that an individual may opt out of fundraising communications.

Marketing

In accordance with the HITECH Act, the Omnibus Rule expands what uses and disclosures of PHI are considered marketing and, therefore, require an individual's authorization. The Omnibus Rule requires authorization for all treatment and health care operations communications that encourage the use of a product or service when a covered entity receives "financial remuneration" for making the communication from the third party whose product or service is being marketed. For example, prior to September 23, 2013 (the compliance date of the Omnibus Rule), an authorization would not be required for a hospital to send a flyer to all of its patients about the availability of a new imaging device at the hospital, even if the communication was paid for by the manufacturer of the imaging device. Under the Omnibus Rule, the hospital no longer would be permitted to send communications about its new imaging device if the manufacturer of the device pays the hospital for the communications, unless the hospital first obtains authorizations from its patients.

The Omnibus Rule includes an exception, as provided in the HITECH Act, for communications about a drug or biologic that currently is prescribed to the individual, as long as any remuneration is reasonably related to the covered entity's cost of making the communications. Accordingly, a drug manufacturer may subsidize a physician's cost for sending out refill reminders.

In accordance with the HITECH Act, the Omnibus Rule expands what uses and disclosures of PHI are considered marketing and, therefore, require an individual's authorization.

Sale of PHI

The Omnibus Rule limits a covered entity or business associate in receiving remuneration in exchange for PHI. HIPAA never has allowed a covered entity to simply sell PHI without an authorization. Previously, however, there was no restriction on a covered entity receiving payment for a disclosure of PHI that the Privacy Rule permitted. In contrast, the Omnibus Rule generally prohibits the sale of PHI by a covered entity or business associate unless an authorization is obtained or an exception applies.

Exceptions include disclosures made: (1) for treatment and payment; (2) for public health; (3) as part of the sale, transfer, merger, or acquisition of a covered entity (or related due diligence) where the recipient is or will become a covered entity; and (4) as required by law. In such cases, there is no cap on the amount of payment the disclosing covered entity may receive.

The Omnibus Rule includes a general exception for any permissible disclosure if remuneration is limited to the cost of

preparation and transmittal. The other exceptions, which were specified in the HITECH Act, have limited impact. There is an exception for business associates or subcontractors where the only remuneration is for the business associate's or subcontractor's activity, but this has limited impact, because the Preamble clarifies that remuneration for services, rather than PHI, is not a violation. The Omnibus Rule also excludes disclosures to provide an individual with access to the individual's own PHI or to provide an accounting of disclosures, but in both cases HIPAA otherwise limits any permissible payments to a reasonable, cost-based fee. The Omnibus Rule also includes an exception for research, but payment is limited to a reasonable, cost-based fee to cover the cost of preparation and transmittal, which is the same limit the Omnibus Rule generally applies to other types of disclosures.

Although not addressed in the HITECH Act, the Omnibus Rule finalizes HHS's proposal to allow a blending of "conditioned" and "unconditioned" authorizations into a single document.

Research

Although not addressed in the HITECH Act, the Omnibus Rule finalizes HHS's proposal to allow a blending of "conditioned" and "unconditioned" authorizations into a single document. Generally, HIPAA does not allow a covered entity to condition treatment on the individual's executing an authorization. One of the exceptions is for clinical research, where the covered entity may condition the research-related treatment on execution of an authorization to use and disclose the individual's PHI in the research. Previously, however, HIPAA prohibited combining such a conditioned authorization with an authorization that could not be conditioned, such as an authorization to use and disclose the individual's PHI for a tissue bank.

The Omnibus Rule will permit the combining of conditioned and unconditioned authorizations, allowing the individual to opt in to the unconditioned authorization. This is welcome news for the research community, as it simplifies authorization paperwork. For example, a researcher will be able to rely on a single authorization for a clinical trial that requires execution of the authorization to participate in the trial and that also includes an opt in (such as a check box or a second signature line) authorizing the covered entity to use and disclose the individual's PHI for a tissue bank. The authorization must make clear that the individual may choose not to opt in to the tissue bank and that the choice will not impact treatment, payment, or benefits.

The Preamble of the Omnibus Rule also includes a change of interpretation of HIPAA that will be a boon for the research community. Previously, HHS interpreted that an authorization for research must be study-specific. A valid authorization could not authorize use and disclosure of PHI for future research. The research community long has stated that this interpretation stands as a significant impediment to beneficial secondary research efforts. HHS clarifies that it has changed its interpretation and now permits an authorization to encompass future research studies. The language of the authorization must adequately inform the individual that the individual's PHI may be used in future research studies. HHS did not amend the regulation itself with respect to this issue.

Decedent information

The Omnibus Rule provides covered entities greater flexibility with respect to the PHI of deceased individuals. A covered entity was previously required to apply HIPAA protections to decedent information without regard to how long ago the individual died, but the Omnibus Rule now limits HIPAA protections to 50 years after an individual's death.

Additionally, the Omnibus Rule provides covered entities with greater flexibility to disclose a decedent's PHI to persons who were involved in the decedent's care or payment. Previously, a common conservative view of HIPAA was that a covered entity could not disclose PHI to a family, friend, or other person involved in an individual's care or payment after the individual's death unless the person was the decedent's personal representative. Now, the Omnibus Rule clarifies that covered entities may continue to communicate with involved family and friends after an individual's death, unless the individual's previously expressed preferences are to the contrary.

Student immunization records

Although not required by the HITECH Act, the Omnibus Rule provides covered entities with greater flexibility to disclose student immunization records. Specifically, a covered entity will be permitted to disclose the immunization record of a student or prospective student to a school if: (1) state law requires the school to have proof of immunization; and (2) the covered entity obtains and documents the agreement of the parent or guardian. The parent or guardian's agreement may be in writing, either in hard copy or electronically, but need not satisfy the requirements for a HIPAA authorization. Alternatively, a covered entity may rely on a parent or adult student's verbal agreement, in which case the covered entity must document the agreement. Covered entities should note that the relevant state law is that which governs the school, and this may differ if the covered entity is located in a different state.

Genetic information

The Omnibus Rule, in accordance with GINA, clarifies that genetic information is a type of health information and prohibits health plans (other than long-term care plans) from using or disclosing genetic information for underwriting purposes. As with other regulations under GINA, "genetic information" is broadly defined to include manifestation of a disease or disorder in a family member of an individual, in addition to genetic tests of individuals and family members, and requests for and receipt of genetic services. The Preamble clarifies that the actual manifestation of a disease or disorder in the individual would not be considered genetic information. A health plan that intends to use or disclose PHI for underwriting purposes must add a statement to its Notice of Privacy Practices providing that it will not use or disclose genetic information for such purposes. Other than clarifying that genetic information is health information, the provision does not impact health care providers (although it may impact their group health plans).

Steps for responding to breach notification and limits on uses and disclosures

Based on the Omnibus Rule, organizations subject to HIPAA should implement or revise a breach response process. Some key features of such a process include:

- Educating the workforce on how to spot and quickly report a breach;
- Revising policies to reflect the new low-probability-of-compromise standard;
- Ensuring that risk assessments addresses the four criteria specified above and are conducted in a reasonably objective and consistent manner; and
- Integrating state breach notification requirements.

To address changes to permissible uses and disclosures under HIPAA, organizations should consider the following steps:

- Revising policies and procedures to address new limits on fundraising, receipt of remuneration for marketing or disclosures of PHI, decedent information, student immunization records, research, and (for health plans) the use of genetic information in underwriting;
- Revising other policies and procedures based on 10 years of experience with complying with the Privacy Rule (e.g., what have been recurring problems) and new issues (e.g., social media, use of personal mobile devices); and
- Targeting relevant training (e.g., training the Marketing department on new restrictions, training persons involved in research on new flexibility, training clinical staff on permissible disclosures to friends and family of deceased individuals).

Organizations have until September 23, 2013 to comply with the new requirements.

Part 2 of this article will appear in our June 2013 issue.

1. Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, 78 Fed. Reg. 5,566-5,702 (Jan. 25, 2013) (to be codified at 45 C.F.R Parts 160 and 164).
2. Health Insurance Portability and Accountability Act of 1996, as amended, 42 U.S.C. §§ 1320d to 1320d-9.
3. Health Information Technology for Economic and Clinical Health, 42 U.S.C. §§ 17901 to 17954.
4. Genetic Information Nondiscrimination Act of 2009 § 105, 42 U.S.C. § 1320d-9.
5. Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. Part 160 and Part 164, Subparts A and E.