Health Care Law Monthly

March 2013
Volume 2013 * Issue No. 3

 HEALTH CARE LAW MONTHLY (USPS 005-212; ISSN 15260704, EBOOK ISBN 978-1-5791-1659-0) is published monthly for $620 per year by Matthew Bender & Co., Inc., 1275 Broadway, Albany, N.Y. 12204-2694. Periodical Postage is paid at Albany, N.Y. and at additional mailing offices. Postmaster: Send address changes to Health Care Law Monthly, 136 Carlin Road, Conklin, N.Y. 13748-1531.

Contents:

HEALTH CARE LAW MONTHLY welcomes your comments and opinions. Please direct all correspondence and editorial questions to: Adriana Sciortino, LexisNexis Matthew Bender, 121 Chanlon Road, New Providence, NJ 07974 (1-908-771-8662); e-mail: adriana.sciortino@lexisnexis.com. For all other questions, call 1-800-833-9844. NOTE: The information herein should not be construed as legal advice, nor utilized to resolve legal problems.

HEALTH CARE LAW MONTHLY welcomes your comments and opinions. Please direct all correspondence and editorial questions to: Adriana Sciortino, LexisNexis Matthew Bender, 121 Chanlon Road, New Providence, NJ 07974 (1-908-771-8662); e-mail: adriana.sciortino@lexisnexis.com. For all other questions, call 1-800-833-9844. NOTE: The information herein should not be construed as legal advice, nor utilized to resolve legal problems.

(Pub. 349)

THE HITECH FINAL RULE HAS ARRIVED: COVERED ENTITIES AND BUSINESS ASSOCIATES MUST ADJUST TO SIGNIFICANT CHANGES

By
Brad M. Rostolsky and Nancy E. Bonifant[1]

On Friday, January 25, 2013, the Office for Civil Rights (OCR) of the U.S. Department of Health and Human Services (HHS) published the long-awaited HITECH final rule – 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 (the ''Final Rule'').[2] After more than a three-year wait from the passage of the 2009 Health Information Technology for Economic and Clinical Health Act (the ''Act'' or ''HITECH Act''), the Final Rule aims to implement the changes to federal privacy and security obligations triggered by the Act, which changes were first addressed in the July 14, 2010, proposed regulations (the ''Proposed Rule'').[3] This article presents some of the Final Rule's key changes and clarifications to the existing Privacy, Security, and Breach Notifications rules set forth in the Final Rule, and reflects the significant impact the Final Rule will have on overall compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

The Final Rule serves as an omnibus rule, and in effect provides final regulations with regard to four distinct aspects of previously proposed rulemakings. The Final Rule implements final rulemaking with regard to the Proposed Rule, the 2009 (interim final) Breach Notification Rule, the 2009 (interim final) Enforcement Rule, and the 2009 Genetic Information Nondiscrimination Act (GINA) proposed rule. As was expected, the Final Rule does not address the May 2011 proposed accounting and access report rule.

The Final Rule, which is effective on March 26, 2013, generally allows covered entities and business associates 180 days after the effective date (September 23, 2013) to become compliant with its changes to the Privacy, Security, and Breach Notification Rules.[4] The changes to the Enforcement Rule, however, are effective upon the effective date of the Final Rule.[5] Lastly, the Final Rule generally extends a significant grandfather period to business associate agreements that were in effect as of January 25, 2013, if: (1) such agreements are in compliance with the existing Privacy and Security Rules, and (2) are not renewed or modified from March 26, 2013, until September 23, 2013.[6] HHS has deemed such unmodified/non-renewed pre-Final Rule publication date business associate agreements to be compliant until the earlier of the date of renewal/modification or September 22, 2014 (i.e., one year subsequent to the general compliance date).

---

[1] Brad M. Rostolsky is a partner in the Life Sciences Health Industry Group in the Philadelphia office of Reed Smith practicing in the area of health care regulatory and transactional law. Brad is the co-leader of the firm's HIPAA and Health Law Privacy Practice Area, and regularly advises clients (including hospitals, medical practices, pharmacies, long term care facilities, and medical device companies) on all aspects of health information privacy and security compliance (HIPAA and state law). His experience also includes assisting hospitals on arrangements with physicians, such as joint ventures, physician recruitment, practice acquisitions, employment arrangements, as well as compliance with federal and state laws fraud and abuse requirements. Nancy E. Bonifant is an associate in the Life Sciences Health Industry Group in the Washington D.C. office of Reed Smith practicing in the area of health care regulatory law. She works with all types of health industry clients, including various types of health care providers and suppliers, including acute and post-acute institutional providers, pharmacies, independent diagnostic testing facilities, DMEPOS suppliers, and hospice programs. Nancy's work on behalf of these clients includes fraud and abuse compliance (for example, compliance with the Federal Anti-Kickback Statute and beneficiary inducement prohibition), government investigations, Medicare reimbursement, health care licensing issues, health information privacy and security compliance (HIPAA and state law), and False Claims Act defense.

[2] 78 Fed. Reg. 5566 (Jan. 25, 2013).

[3] 75 Fed. Reg. 40868 (July 14, 2010).

[4] 78 Fed. Reg. at 5566.

[5] *Id.* at 5669.

[6] *Id.* at 5603 (to be codified at 45 C.F.R. § 164.532(e)(1)).

A. Impact on Business Associates

Arguably the most significant aspect of the Final Rule's change to the overall scope and application of HIPAA's implementing regulations, the Final Rule dramatically (though certainly expected in light of the Act's directives) extends to business associates the need to comply directly with the Security Rule and significant aspects of the Privacy Rule. Additionally, HHS made certain definitional changes and clarifications with regard to which individuals and entities qualify as a business associate.

1. Expanded Definition

The Final Rule significantly expands the definition of business associate to include health information organizations, e-prescribing gateways, and other entities that facilitate data transmission services to a covered entity and require access to PHI on a routine basis.[7] Significantly, the preamble to this aspect of the Final Rule includes a potentially far-reaching discussion of the ''conduit'' exception (often referred to as the ''common carrier'' exception) and the government's view of when certain types of vendors qualify as a business associate. In declaring that the conduit exception should be narrowly construed, HHS clarifies (both in the preamble and definition of business associate itself) that ''an entity that maintains protected health information on behalf of a covered entity is a business associate and not a conduit, even if the entity does not actually view the protected health information.''[8] Additionally, the Final Rule includes in the expanded definition of business associate entities that offer a personal health record on behalf of a covered entity.

2. Subcontractors

The Final Rule's expansion of the definition of business associate is most dramatically reflected in its inclusion of business associate subcontractors as actual business associates. As a result of this change, a business associate's subcontractors (and subcontractors of a subcontractor, all the way down the chain) will be regulated in the same manner as any other business associate under the Final Rule, provided that the subcontractor has been delegated a function, activity, or service that involves the creation, receipt, maintenance, or transmission of PHI.[9]

3. Direct Liability

Under the HITECH Act and the Final Rule, business associates and subcontractors are directly liable for civil monetary penalties under the HIPAA Privacy Rule for ''impermissible uses and disclosures of PHI,'' which include violations of the minimum necessary rule, as well as the following HITECH requirements: (a) For a failure to provide breach notification to the covered entity; (b) For a failure to provide access to a copy of electronic PHI to either the covered entity, the individual, or the individual's designee (whichever is specified in the BAA); (c) For a failure to disclose PHI where required by the Secretary to investigate or determine the business associate's compliance with the HIPAA Rules; (d) For a failure to provide an accounting of disclosures; and (e) For a failure to comply with the requirements of the Security Rule.[10]

While ''impermissible uses and disclosures of PHI'' include any use or disclosure that would violate the Privacy Rule if done by a covered entity, it is the Business Associate Agreement and Business Associate Subcontractor Agreement that ''clarify and limit, as appropriate, the permissible uses and disclosures'' of PHI by business associates and subcontractors. Therefore, the HITECH Act and the Final Rule tie much of ''business associate [direct] liability to making uses and disclosures in accordance with the uses and disclosures laid out in such agreements, rather than liability for compliance with the Privacy Rule generally.''[11]

a. The Privacy Rule and Direct Liability under Business Associate Agreements (BAAs) and Business Associate Subcontractor Agreements (BASAs)

Under Section 13404(a) of the HITECH Act and the Final Rule, business associates become directly liable

[7] *Id.* at 5571.

[8] *Id.* at 5572; *see* 45 C.F.R. § 160.103 (defining "Business Associate").

[9] 78 Fed. Reg. at 5572.

[10] 78 Fed. Reg. at 5598–99, 5601.

[11] *Id.* at 5601.

for uses and disclosures of PHI that do not comply with the business associate's or subcontractor's BAA or BASA, respectively. Stated differently, effective September 23, 2013, a business associate that breaches its BAA is contractually liable to the applicable covered entity and may be directly liable to HHS. Interestingly, however, direct liability to HHS is not dependent upon the actual existence of a BAA or BASA—"liability for impermissible uses and disclosures attaches immediately when a person creates, receives, maintains, or transmits protected health information on behalf of a covered entity or business associate and otherwise meets the definition of a business associate."[12] Therefore, while the BAA may clarify and limit permissible uses and disclosures of PHI, business associates are still prohibited from using and disclosing PHI in a manner that would violate the Privacy Rule if done by a covered entity regardless of the existence of a BAA.

HHS received many comments questioning whether covered entities are required to obtain satisfactory assurances in the form of a BASA from a business associate's subcontractor. The Final Rule makes clear that a covered entity is not required to enter into a contract or other arrangement with a business associate that is a subcontractor. Rather it is the obligation of the business associate that has engaged the subcontractor to enter into a BASA.[13]

Interestingly, as stated above, whether a person is a business associate depends upon whether that person creates, receives, maintains or transmits PHI on behalf of a covered entity and not on whether the person has entered into a BAA with the covered entity. Therefore, a business associate's obligation to enter into a BASA is triggered when the business associate engages a subcontractor to create, receive, maintain, or transmit PHI on behalf of the business associate. That obligation exists regardless of whether the covered entity has met its obligation of requiring the business associate to enter into a BAA.[14]

b. The Security Rule and Direct Liability

The Final Rule adopts the HITECH Act's provisions extending direct liability for compliance with the Security Rule to business associates. While BAAs executed prior to January 25, 2013, do not need to become HITECH-compliant until the earlier of September 23, 2014 or when the BAA is renewed or modified,[15] beginning September 23, 2013, business associates (which includes subcontractors) must comply with, and are directly liable for violations of, the Security Rule's administrative, physical, and technical safeguards requirements in Sections 164.308, 164.310, and 164.312, as well as the Rule's policies and procedures and documentation requirements in Section 164.316. Such requirements include performing a Security Rule risk assessment (which has been the trigger for multiple recent HHS enforcement actions), establishing a risk management program, and designating a security official.[16]

In response to comments regarding the cost of compliance for both traditional/prime business associates and subcontractors, HHS reminds business associates of their current obligations under BAAs that comply with the existing Privacy and Security Rules: business associates must (1) implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic PHI that the business associate creates, maintains or receives, and (2) require their agents (and subcontractors) to implement reasonable and appropriate safeguards as well. Therefore, HHS expects only "modest improvements" are likely necessary for business associates and subcontractors to come into compliance. The requirements of the Security Rule also remain flexible and scalable, and business associates may choose security measures that are appropriate for their size, resources, and the nature of the security risks they face.[17]

B. Breach Notification Rule

With regard to the existing regulatory exceptions to what constitutes a breach, as well as the mechanics

[12] *Id*. at 5598.

[13] *Id.* at 5573, 5590, 5601.

[14] *See id.* at 5697 (outlining the new requirements at 45 C.F.R. § 164.502(e)(1) and (2)).

[15] *Id.* at 5603.

[16] *Id.* at 5569, 5589.

[17] *Id.* at 5589.

of notifications and associated obligations under the 2009 interim final Breach Notification Rule, the Final Rule serves merely as a clarifying document. The Final Rule does, however, make one far reaching and extremely significant change to the interim final rule – the removal of the risk of harm assessment.[18]

1. Presumption of Breach/Risk of Harm Assessment Replaced

The Final Rule explicitly provides that impermissible uses or disclosures of PHI will be presumed to be a breach unless the associated covered entity or business associate demonstrates that there is a ''low probability that the protected health information has been compromised.''[19] Because the determination of risk of harm to an individual under the interim final rule's standard often proved challenging – particularly with regard to determination of reputational harm – HHS replaced the risk of harm assessment with a four-pronged, ''more objective'' test. Though refusing to implement a bright line standard as to what qualifies as a breach, the Final Rule requires covered entities and business associates to consider the following factors (along with any other relevant considerations) designed to ''focus more objectively on the risk that the protected health information has been compromised'' as compared to the significant risk to an individual caused by the impermissible use or disclosure:

- The nature and extent of the PHI involved, including types of identifiers and the likelihood of re-identification.
- The unauthorized person who used the PHI or to whom it was disclosed (if the person to whom the PHI was improperly disclosed is another covered entity or someone obligated to protect PHI, this would favor a determination that there is a low probability that the PHI was compromised).
- Whether the PHI was actually acquired or viewed (if, for example, a laptop containing unencrypted PHI is lost, but later found and forensic analysis reveals that the PHI was never accessed, this would favor a determination that no notification is required).
- The extent to which the risk to the PHI has been mitigated (if PHI is improperly used or disclosed, the covered entity or business associate should immediately take steps to mitigate any potential risk to the PHI, which would favor a determination that there is a low probability that the PHI was compromised).[20]

Although the Final Rule's preamble discussion highlights the above factors' replacement of the risk of harm assessment as an attempt to ensure a more objective and uniform application of the rule, discussion associated with the first of the four new factors does specifically address the need for covered entities and business associates to consider ''whether the [impermissible] disclosure involved information ... is of a more sensitive nature.''[21] Furthermore, HHS clarifies that such sensitive information includes more than PHI addressing sexually transmitted diseases, mental health conditions, or substance abuse treatment. This appears to suggest that whether PHI has been ''compromised'' will still require some consideration of the risk of harm to the individual albeit within the confines of the Final Rule's new overall approach to analyzing a breach of unsecured PHI.

2. Significant Clarifications

The Final Rule removes the interim final Breach Notification Rule's exception relating to an impermissible disclosure of PHI involving only a limited data set that also excludes dates of birth and zip codes.[22] Instead, such potential breaches should be analyzed under the Final Rule's new standard.

In terms of the annual notifications that covered entities must make to HHS regarding each calendar year's breaches involving fewer than 500 individuals (which may be made within 60 days after the end of applicable calendar year), HHS clarifies that the trigger for such notification is the date of a breach's discovery as opposed to the date on which the incident occurred.[23]

[18] *Id.* at 5641.
[19] *Id.*
[20] *Id.* at 5642.
[21] *Id.*
[22] *Id.* at 5644.
[23] *Id.* at 5654.

Clarifying an ambiguous aspect of the interim final rule's media notice requirement, HHS makes it clear that a covered entity is not required to incur any cost to print or run the media notice. Instead, it is permissible to fulfill this obligation through the issuance of a press release.[24]

Lastly, emphasizing that the timing requirement for notification is truly "without unreasonable delay," HHS warns that, depending on the facts and circumstances associated with a particular breach, notification may be viewed as late even if it comes within 60 calendar days of the discovery of the breach.[25]

C. Individual Rights

Unfortunately (although not unexpected), the Final Rule does not address the new statutory requirements for accounting of disclosures of PHI for treatment, payment, and health care operations purposes, which were the subject of a May 2011 proposed rule and will be subject to future rulemaking.[26] The Final Rule does revise an individual's right to restrict certain uses and disclosures of PHI, as well as to access their PHI to the extent such information is maintained in a designated record set.

1. Right to Request a Required Restriction

The Final Rule revises an individual's right to request certain restrictions on the uses and disclosures of the individual's PHI in light of new statutory requirements under HITECH.[27] Now, covered entities are *required to comply* with an individual's request to restrict disclosure of the individual's PHI to a health plan where (1) the disclosure is for payment or health care operations purposes and is not otherwise required by law, and (2) the PHI pertains solely to health care services or items for which the individual, or another person on the individual's behalf (other than a health plan), has paid the covered entity in full.[28]

[24] *Id.* at 5653.

[25] *Id.* at 5648.

[26] *Id.* at 5568.

[27] *See* Section 13405(a) of the HITECH Act.

[28] 78 Fed. Reg. at 5628–30 (to be codified at 45 C.F.R. § 164.522(a)(1)(iv)).

a. "Required by Law" Exception

The "required by law" exception allows covered entities to disclose PHI to health plans for payment and health care operations purposes despite a requested restriction where another law compels the covered entity to make the disclosure and that obligation is enforceable in a court of law. This includes, for example, Medicare conditions of participation with respect to health care providers participating in the program, as well as State and other laws that require providers to submit a claim to a health plan for a covered service and provide no exception for individuals wishing to pay out-of-pocket for the service.[29]

Notably, a contractual requirement to submit a claim or otherwise disclose PHI to an HMO, (as opposed to a requirement under State or other law), does not meet the "required by law" exception. Such provider contracts with HMOs must be renegotiated and updated prior to September 23, 2013 to be consistent with these new requirements under the Privacy Rule.[30]

b. Operational Concerns

To address many concerns regarding how to practically operationalize a restriction, HHS is relying on covered entities complying with existing minimum necessary policies and procedures, as well as on covered health care providers counseling their patients on the patient's obligations to ensure enjoyment of the right. Importantly, covered entities are not required to create separate medical records or otherwise segregate PHI subject to a restriction. Instead, HHS reminds covered entities that they should already have in place, and be familiar with applying, minimum necessary policies and procedures that limit the PHI disclosed to a health plan to the amount reasonably necessary to achieve the purpose of the disclosure. Therefore, these procedures and mechanisms should be employed in this context as well to limit the disclosure of PHI subject to a restriction when, for example, a health plan performs an audit of a covered entity's medical records or otherwise requests disclosures of PHI for

[29] *Id.* at 5628.

[30] *Id.* at 5629.

the health plan's payment or health care operations purposes.[31]

With respect to downstream providers, such as pharmacies and other providers, HHS encourages health care providers to counsel their patients on the patients' obligations to request restrictions from other providers and pay out-of-pocket for follow-up care. For prescribed medication, the prescribing provider will likely need to provide the patient with a paper prescription to allow the patient an opportunity to request a restriction and pay for the prescription before the pharmacy has submitted a bill to the health plan, which generally occurs automatically when an e-prescribing tool is used. Providers should also counsel patients where unbundling of services is not possible or state law prohibits in-network providers from accepting out-of-pocket payments and, therefore, the patient must pay for the entire bundled service or use an out-of-network provider to ensure the PHI is not disclosed to the patient's health plan.[32]

c. Payment in Full

While covered entities are not required to abide by a required restriction if an individual's payment is dishonored, HHS expects that providers will make a "reasonable effort" to contact the individual and obtain payment prior to billing a health plan. HHS does not prescribe what efforts are "reasonable," but instead defers to the provider's policies and the individual circumstances. Providers may choose, however, to require payment in full at the time of the request for a required restriction to avoid payment issues altogether. Therefore, it will be important for covered health care providers to outline clearly in their policies and procedures the "reasonable efforts" the provider will take in such circumstances or if the provider requires payment in full at the time of the request.[33]

2. Right to Access PHI

Expanding on HITECH's requirement to provide individuals with an *electronic* copy of PHI maintained in an *electronic health record* (EHR) system, the Final Rule provides that an individual has a right to obtain an electronic copy of PHI that is maintained in *any electronic system*.[34] Additionally, with regard to PHI maintained in hard copy or electronic designated record sets, HHS limits the time in which covered entities must act on a request, clarifies the reasonable, cost-based fee that a covered entity may charge for providing access to PHI, and sets forth new requirements for an individual's request to provide access and copies directly to third parties.

a. Right to Access PHI in an Electronic Form and Format

Under the Final Rule, with respect to PHI maintained in electronic designated record sets, covered entities are now required to provide individuals with access to such PHI in the *electronic* form and format requested by the individual, if it is readily producible, or, if not, in a readable *electronic* form and format as agreed to by the covered entity and the individual.

Importantly, HHS acknowledges that the "readable electronic form" will vary by system and does not require covered entities to purchase new software or systems to accommodate a request for a specific electronic form that is not readily producible by the covered entity. However, covered entities must still provide individuals with some kind of readable electronic form and HHS anticipates that some covered entities may need to update legacy or other systems to meet this basic requirement. HHS interprets "readable electronic form" to mean a "digital information stored in a standard format enabling the information to be processed and analyzed by computer," such as MS Word or Excel, text, HTML or text-based PDF.[35]

If an individual requests an electronic form that the covered entity cannot produce, the covered entity must offer other electronic formats that are available of its systems. Only in the event that an agreement cannot be reached between the individual and the covered with regard to an electronic format, the covered entity may provide the individual with a readable hard copy form (as is currently permissible under the existing Privacy Rule with respect to PHI

[31] *Id.* at 5628.

[32] *Id.* at 5629–30.

[33] *Id.*

[34] *See* Section 13405(e) of the HITECH Act; 78 Fed. Reg. at 5631 (to be codified at 45 C.F.R. § 164.524(c)(2)(ii)).

[35] 78 Fed. Reg. at 5631.

maintained in either hard copy or electronic designated record sets).[36]

b. Covered Entity's Time to Provide Access to PHI

Although not required by the HITECH Act, HHS removes the additional 30 days provided to covered entities to either (1) deny a request or (2) grant and provide access to individuals with regard to PHI that is not maintained or accessible to the covered entity on-site. Under the existing Privacy Rule, covered entities had up to 90 days to respond to an individual's request for PHI maintained off-site.[37] Now, covered entities must take the required action within 60 days regardless of whether the PHI is maintained on- or off-site.[38]

c. Fees

Under the existing Privacy Rule, covered entities may charge a reasonable, cost-based fee for providing individuals with access to their PHI. The Final Rule clarifies that such a fee may include labor costs for copying PHI, but may not include labor costs for actually retrieving (or locating) the PHI. In particular, labor costs for copying may include technical staff time spent to create and copy the electronic file, such as compiling, extracting, scanning and burning PHI to media, and distributing the media. Additionally, if, for example, an individual requests that the covered entity save PHI to a compact disc (CD) and then mail the CD to the individual, the covered entity may charge for the cost of supplies for creating, and the postage for transmitting, the CD.[39]

d. Requests to Provide Access to Third Parties

The Final Rule provides that if requested by the individual, covered entities must transmit a copy of PHI directly to a third party designated by the individual. In such circumstances, the individual's request *must* be in writing, signed by the individual, and clearly identify the designated third party and where to send the copy of the PHI. While covered entities may rely on the information provided by the individual in the written request, covered entities must also implement reasonable policies and procedures under Section 164.514(h) to verify the identity of the individual making the request, as well as implement reasonable safeguards under Section 164.530(c) to protect the PHI that is used or disclosed. Such safeguards include, for example, ensuring that the covered entity correctly enters in the email address of the third party into its system.[40]

D. Notice of Privacy Practices

The Final Rule mandates the inclusion of several additional statements in a covered entity's Notice of Privacy Practices (NPP), which triggers a covered entity's obligation under the existing Privacy Rule to redistribute its revised NPP. The Final Rule requires that a covered entity's NPP include a statement indicating that the following uses and disclosures require authorization from the individual: (1) Most uses and disclosures of psychotherapy notes (where appropriate); (2) Uses and disclosures of protected health information for marketing purposes; and (3) Uses and disclosures that constitute a sale of protected health information.[41] Perhaps more importantly, in addition to the uses and disclosures described above, an NPP must now contain a statement that other uses and disclosures *not described in the NPP* will be made only with an authorization from the individual.[42]

Covered entities must include in their NPP a statement that covered entities are required to notify affected individuals following a breach of unsecured PHI.[43] If a covered entity intends to contact an individual in support of its fundraising activities, the covered entity must include in the NPP a statement informing the individual of this intention and that the

[36] *Id.* at 5633.
[37] *See* 45 C.F.R. § 164.524(b)(2)(ii).
[38] 78 Fed. Reg. at 5637.
[39] *Id.* at 5635–36 (to be codified at 45 C.F.R. § 164.524(c)(4)).
[40] *Id.* at 5634–35 (to be codified at 45 C.F.R. § 164.524(c)(3)(ii)).
[41] *Id.* at 5624 (to be codified at 45 C.F.R. § 164.520(b)(1)(ii)(E)).
[42] *Id.* at 5624 (to be codified at 45 C.F.R. § 164.520(b)(1)(ii)(E)).
[43] *Id*. at 5624 (to be codified at 45 C.F.R. § 164.520(b)(1)(v)(A)).

individual has the right to opt out of receiving such communications.[44] If a covered entity is a health plan that underwrites (except certain long-term care plans) and intends to use or disclose PHI for underwriting purposes, the covered entity must include a statement in its NPP informing the individual that the plan cannot use genetic information for such purposes.[45] Lastly, the Final Rule also requires that covered entities include a statement in their NPP regarding individual's limited right to request required restrictions.[46]

E. Authorizations

The Final Rule significantly alters the regulations that govern the use or disclosure of PHI for which a covered entity must obtain an authorization, and imposes additional burdens on covered entities and business associates that market or sell PHI. At the same time, certain requirements governing authorizations for the use or disclosure of PHI for research purposes have been relaxed. Nevertheless, the Final Rule does not alter the content of the Privacy Rule's core elements and required statements that are outlined in 45 C.F.R. § 164.508(c). Thus, the substance of a HIPAA-compliant authorization for the use or disclosure of PHI largely remains intact.

F. Marketing

1. Financial Remuneration and Treatment and Health Care Operations Communications

In a marked departure from the proposed rule's approach to marketing, the Final Rule requires authorizations for all health care operations *and treatment* communications where the covered entity receives financial remuneration for making the communication from a third party whose products or services are being described.[47] Under the existing Privacy Rule, treatment and certain health care operations communications were specifically excluded from the definition of "marketing."[48] Those same exceptions are no longer applicable if in exchange for making the communication, the covered entity receives financial remuneration from a third party.

"Financial remuneration" is defined as "direct or indirect payment from or on behalf of a third party whose product or service is being described," but does not include payments for the actual treatment of the individual. Indirect payments refer to payments that flow from an entity on behalf of the third party whose product or service is being described to the covered entity. Notably, financial remuneration does not include non-financial, *in-kind* benefits; instead, it is limited to actual *monetary* payments.[49] For example, a third party may provide a covered entity with *in-kind* goods, such as written materials, that describe the third party's products or services. The covered entity may then distribute those materials to its patients for the purpose of recommending the third party's product or service as an alternative treatment without obtaining an authorization. By contrast, if the covered entity also receives a *monetary* payment from the third party for the purpose of making the communication, then an authorization is required.

Importantly, for financially remunerated treatment and health care operations communications that will require an authorization under the Final Rule, the scope of the authorization need not be limited to communications describing a single product or service or the products or services of a single third party. Instead, authorizations may apply to subsidized communications generally, provided that the authorization adequately describes the intended purposes of the requested uses and disclosures. Such authorizations must also disclose the fact that the covered entity is receiving financial remuneration from a third party.[50]

Going forward, covered entities will need to answer two important questions prior to using or disclosing PHI for treatment or health care operations communications that involve the receipt of financial remuneration from a third party: (1) whether the

[44] *Id.* at 5624 (to be codified at 45 C.F.R. § 164.520(b)(1)(iii)(A)).
[45] *Id.* at 5625 (to be codified at 45 C.F.R. § 164.520(b)(1)(iii)(C)).
[46] *Id*. at 5624 (to be codified at 45 C.F.R. § 164.520(b)(1)(iv)(A)).
[47] 78 Fed. Reg. at 5595.
[48] 45 C.F.R. § 164.501 (defining "marketing").
[49] 78 Fed. Reg. at 5595–96 (to be codified at 45 C.F.R. § 164.501(defining "marketing")).
[50] *Id.* at 5596.

covered entity is receiving "financial remuneration" as defined by the Privacy Rule, and (2) whether the covered entity is receiving the financial remuneration for the purpose of making the communication.

2. Prescription Refill Reminders

As expected, HHS includes the statutory exception to the definition of "marketing" for communications about a "drug or biologic that is currently being prescribed" to the individual in the Final Rule, as well as regulatory text that expressly includes prescription refill reminders within that exception.[51] While HHS intends to provide further guidance on the scope of the exception, it clarifies in the Final Rule that the following communications are included within the exception: (a) Communications regarding generic equivalents of a currently prescribed drug; (b) Communications that encourage individuals to take their prescribed medication as directed; and (c) For individuals who are prescribed a self-administered drug or biologic, communications regarding all aspects of a drug delivery system.[52]

While a covered entity may receive financial remuneration in exchange for making these communications and still remain within the marketing exception, such remuneration must be limited to the covered entity's costs for making the communication. Permissible costs include only the costs of labor, supplies, and postage. Where a covered entity generates a profit or receives payment for other costs in exchange for making a prescription refill reminder, the exception would not apply and the covered entity must obtain individual authorization prior to using or disclosing PHI in furtherance of the communication.[53]

G. Sale of Protected Health Information

The HITECH Act and Final Rule generally prohibit the sale of PHI by a covered entity or business associate unless the covered entity or business associate obtains an authorization from the individual in compliance with the new Section 164.508(a)(4).[54] There are important exceptions to this prohibition and, therefore, the authorization requirement. However, some of these exceptions are limited to those disclosures where the remuneration received by the covered entity or business associate includes *only* a reasonable cost-based fee to cover the costs to prepare and transmit the PHI.

1. Sale of PHI Defined

HHS defines the "sale of PHI" to a mean a disclosure of PHI by a covered entity (or business associate, if applicable) where the covered entity directly or indirectly receives "remuneration"[55] from or on behalf of the recipient of the PHI in exchange for the PHI.[56] In addition to financial payments, the term "remuneration" includes nonfinancial benefits, such as in-kind benefits. Importantly, HHS does not limit a "sale" to those transactions where there is a transfer of ownership of PHI; the sale of PHI provisions apply equally to disclosures in exchange for remuneration including those that are the result of access, license, or lease agreements.[57]

Notably, HHS does not consider the sale of PHI to encompass payments a covered entity may receive in the form of grants or contracts to perform programs or activities, including research activities, even if the covered entity is required to report PHI-containing results as a condition of receiving the funding. In such circumstances, the covered entity is not receiving remuneration in exchange for disclosing PHI, but is instead receiving remuneration to perform the program or research activity. By contrast, a sale of PHI occurs when the covered entity primarily is being compensated to supply PHI it maintains in its role as a covered entity (or a business associate).[58]

---

[51] *Id.* at 5596–97 (to be codified at 45 C.F.R. § 164.501(defining "marketing")).

[52] *Id.* at 5596.

[53] *Id.* at 5596–97.

[54] *See* Section 13405(d) of the HITECH Act; 78 Fed. Reg. at 5606 (to be codified at 45 C.F.R. § 164.502(a)(5)(ii)(A)).

[55] Unlike the marketing provisions discussed above, which are limited to the receipt of financial payments, "remuneration" as applied in the sale of PHI provisions is not limited to financial payments and therefore is applicable to the receipt of nonfinancial as well as financial benefits. *See* 78 Fed. Reg. at 5607.

[56] 78 Fed. Reg. at 5606 (to be codified at 45 C.F.R. § 164.502(a)(5)(ii)(B)).

[57] *Id.* at 5606.

[58] *Id.*

2. Exceptions

The sale of PHI prohibition and authorization requirement is not applicable to the following situations where the covered entity or business associate receives remuneration in exchange for disclosing PHI:

- For public health purposes;
- For treatment and payment purposes;
- For the sale, transfer, merger or consolidation of all or part of the covered entity and for related due diligence; and
- As required by law.

The remuneration received for the above exceptions *is not limited* to a covered entity's or business associate's reasonable costs to prepare and transmit the PHI. By contrast, the exceptions outlined below do include various limitations on the type of remuneration a covered entity or business associate may receive:

- For research purposes.

To be within the exception, a covered entity or business associate may only receive a reasonable cost-based fee to cover the cost to prepare and transmit the PHI. HHS also clarifies that a reasonable cost-based fee may include both direct and indirect costs, including labor, materials, and supplies for generating, storing, retrieving, and transmitting the PHI; labor and supplies to ensure the PHI is disclosed in a permissible manner; as well as related capital and overhead costs. However, if a covered entity or business associate incurs a profit from the PHI disclosure for research purposes, then the exception is not applicable and an authorization is required.

Importantly, and as discussed further below, if a covered entity or business associate incurs a profit for disclosing PHI for research purposes, an IRB or Privacy Board waiver to the authorization requirement in compliance with Section 164.512(i) is no longer sufficient.

- To the individual to provide the individual with access to PHI or an accounting of disclosures.

Limitations on the fees a covered entity or business associate may charge as set out in Sections 164.524 and 164.528 still apply for a disclosure of PHI to come within the exception.

- To or by a business associate for activities that the business associate undertakes on behalf of a covered entity, or on behalf of a business associate in the case of a subcontractor.

Such remuneration provided by a covered entity to a business associate (or by a business associate to a subcontractor), must be for the actual performance of the activities that the business associate (or subcontractor) undertakes on behalf of a covered entity (or business associate).

- For any other purpose permitted by or in accordance with the Privacy Rule.

Similar to the research exception discussed above, to be within this exception, a covered entity or business associate may only receive a reasonable cost-based fee to cover the cost to prepare and transmit the PHI.[59]

H. Fundraising

Section 164.514(f) of the Privacy Rule permits a covered entity to use or disclose certain elements of an individual's PHI to make fundraising communications without obtaining the individual's authorization provided that certain requirements are met. Fundraising communications include communications made by the covered entity, an institutionally-related foundation, or a business associate on behalf of the covered entity for the purpose of raising funds for the covered entity.[60] Under Section 13406(b) of the HITECH Act, HHS must issue rules requiring that covered entities provide clear and conspicuous opportunities to recipients of fundraising communications to opt out of receiving future fundraising communications. Importantly, the revised rules do not require covered entities to send pre-solicitation opt out opportunities prior to the first fundraising communication.[61]

1. Additional Elements of PHI May Be Used or Disclosed for Fundraising Purposes

Under the existing Privacy Rule, covered entities may use or disclose only demographic information

[59] *Id.* at 5607–09 (to be codified at 45 C.F.R. § 164.502(a)(5)(ii)(B)(2)).
[60] *Id.* at 5620–21.
[61] *Id.* at 5622.

relating to the individual and dates of health care services provided to the individual for fundraising communications.[62] The Final Rule clarifies the scope of such demographic information to include name, address, other contact information, age, gender, and date of birth.[63] Additionally, the Final Rule expands the scope of the PHI that a covered entity may use or disclose to a business associate or institutionally-related foundation to include department of service, treating physician, and outcome information.[64]

2. New Requirements Governing Fundraising Communications

Under the existing Privacy Rule, a covered entity may not use or disclose PHI for fundraising purposes unless a statement is included in the covered entity's notice of privacy practice notifying the individual of the potential for such communications. Now, as discussed above, that statement must also inform individuals of their right to opt-out of fundraising communications.[65] Additionally, the Final Rule enhances the requirements governing fundraising communications in four key aspects. More specifically, HHS replaces the standard that covered entities must make "reasonable efforts" not to send fundraising communications to individuals who opt out of such communications with the following new specifications:

- First, with each fundraising communication "made"—not just "sent"—to an individual, a covered entity must provide the individual with a "clear and conspicuous opportunity to elect not to receive any further fundraising communications." The revised standard is meant to apply to both written and oral communications. Importantly, although HHS gives a covered entity wide latitude to determine the method by which an individual may opt out of such communications, the method "may not cause the individual to incur any undue burden or more than a nominal cost."[66]
- Second, the regulation makes clear that a covered entity "may not condition treatment or payment on the individual's choice with respect to the receipt of fundraising communications."[67]
- Third, a covered entity is prohibited from making fundraising communications to an individual where the individual has elected not to receive these communications "under paragraph (f)(1)(ii)(B) of this section."[68] Curiously, Section 164.514(f) does not contain a section (f)(1)(ii)(B), so we assume that HHS is referring to the opt out provision in Section 164.514(f)(2)(ii).
- Fourth, a covered entity is permitted—but not required—to provide a method for an individual who has previously opted out of receiving fundraising communications to opt back in.[69]

Importantly, the Final Rule on fundraising balances HHS' attempts to provide strong protections for individuals who opt out of receiving fundraising communications while still granting flexibility to covered entities to determine the scope of the opt out. Stated differently, a covered entity may limit an individual's opt-out to a specific fundraising campaign or apply the opt-out to all fundraising communications made by the covered entity.[70]

* * *

Although this article does not attempt to detail every aspect of the Final Rule's impact on HIPAA's implementing regulations, it is worth noting that the Final Rule adopts, without modification, the changes to HIPAA enforcement reflected in the October 30, 2009, Interim Final Enforcement Rule[71] and as set forth in the Proposed Rule. Although the most significant changes to the Enforcement Rule have been a reality since 2009, it is clear–especially in consideration of transformation to HIPAA compliance reflected by the Final Rule–that both covered entities and business associates will be revisiting.

---

[62] 45 C.F.R. § 164.514(f)(1).

[63] 78 Fed. Reg. at 5621.

[64] *Id.* at 5622 (to be codified at 45 C.F.R. § 164.514(f)(1)).

[65] *Id.* at 5622 (to be codified at 45 C.F.R. §§ 164.514(f)(2)(i), 164.520(b)(1)(iii)(A)).

[66] *Id.* at 5622 (to be codified at 45 C.F.R. § 164.514(f)(2)(ii)).

[67] *Id.* at 5622 (to be codified at 45 C.F.R. § 164.514(f)(2)(iii)).

[68] *Id.* at 5621 (to be codified at 45 C.F.R. § 164.514(f)(2)(iii)).

[69] *Id.* at 5621 (to be codified at 45 C.F.R. § 164.514(f)(2)(v)).

[70] *Id.* at 5621.

[71] 74 Fed. Reg. 56123 (October 30, 2009).