BNA, INC.

HEALTH IT LAW & INDUSTRY

BNA Employee-Owned Since 1947

REPORT

Major Changes to HIPAA Privacy, Security, and Enforcement Rules Proposed by HITECH Privacy NPRM



By Gerry Hinkley,
Allen Briskin, and
Douglas Grimm

A much anticipated Notice of Proposed Rulemaking (''NPRM''), addressing the changes to HIPAA mandated by the Health Information Technology for Economic and Clinical Health Act (''the HITECH Act'' or ''the Act''), was published by HHS in the Federal Register on July 14.[1] Public comment will be accepted by HHS on or before September 13.

While the NPRM covers a wide variety of subjects, it contains noteworthy major changes to the Privacy, Security and Enforcement Rules with respect to business associates and business associate agreements, use and disclosure of protected health information (''PHI'') for marketing and fundraising, sale of PHI, rights of individuals to request access to their health records, and expansion of HIPAA's enforcement provisions. HIPAA-covered entities, their business associates and their business associates' subcontractors are advised to pay close attention to this NPRM and to respond to HHS's request for comments as noted in the NPRM.

Hinkley is co-chair of the health care industry team at Pillsbury Winthrop Shaw Pittman LLP in San Franciso, and Briskin is of counsel, also in Pillsbury's San Francisco office. Grimm is a senior associate in Pillsbury's health care group in Washington. Hinkley may be contacted at gerry.hinkley@pillsburylaw.com. Briskin may be contacted at allen.briskin@pillsburylaw.com. Grimm may be contacted at douglas.grimm@pillsburylaw.com.

[1] 75 Fed. Reg. 40868 (Jul. 14).

 ISSN 2151-2876

Business Associates

The Proposed Rule addresses the HITECH Act's impact upon the functions and responsibilities of business associates on a number of fronts. Most of the Proposed Rule's changes focus on conforming the Privacy and Security Rules to the HITECH Act's extension of those Rules' requirements to business associates,[2] and do not make unanticipated substantive changes to the obligations of covered entities and business associates. However, the Proposed Rule does extend the requirements for business associates to subcontractors of business associates, and thereby adds complexity to, and potential inconsistent interpretation of, the legal obligations of business associates and their subcontractors.

Expanded and Clarified Definition of "Business Associate"

The Proposed Rule would expand and clarify the definition of the term ''Business Associate.''[3] These changes are largely ministerial.

First, the Proposed Rule would clarify that performing the functions of a ''Patient Safety Organization,'' described in the Patient Safety and Quality Improvement Act of 2005 (''PSQIA''),[4] would constitute a ''function or activity involving the use or disclosure of protected health information'' and would therefore cause an entity performing those functions for a covered entity to be a business associate of that covered entity.[5] In doing so, the Proposed Rule refers specifically to the functions of such a ''Patient Safety Organization'' in the PSQIA regulations.[6]

The Proposed Rule conforms the definition of ''Business Associate'' to the HITECH Act's requirement that health information exchange organizations, e-prescribing gateways, and vendors that contract with covered entities to offer personal health records to patients, enter into business associate agreements with covered entities.[7] The Proposed Rule accomplishes this change by adding a reference to these types of organizations to the definition's list of illustrative examples of business associates.[8] It is noteworthy that the Proposed Rule's inclusion of personal health record vendors as business associates remains within the limits set by the HITECH Act. Not all personal health record vendors who receive protected health information from covered entities are business associates of those covered entities. Instead, only those personal health record vendors that offer the record *on behalf of the covered entity* are business associates.[9] Personal health record vendors that act on behalf of their individual customers, and not on behalf of covered entities, remain outside the scope of the business associate rules.

Also added to the illustrative examples of business associates is an ''other person that provides data transmission services with respect to protected health information and that requires access on a routine basis to such protected health information.''[10] By this example, the Proposed Rule suggests that a data transmission provider that does not access protected health information on a routine basis is not a business associate.

The Proposed Rule similarly provides a small number of illustrative examples of parties that are excluded from the definition of ''Business Associate.'' These include a health care provider, with respect to disclosures received from another covered entity for treatment purposes;[11] a plan sponsor, with respect to disclosures from a group health plan, insurer or HMO that are made to the plan sponsor for limited purposes;[12] government agencies receiving protected health information for purposes of determining eligibility for or enrollment in certain government health plans,[13] and covered entities participating in an organized health care arrangement and performing specified functions for that arrangement.[14]

Expanded Application of Business Associate Rules to Subcontractors of Business Associates

The Proposed Rule would expand the obligations of business associates and their subcontractors. Under the current rule, business associates may subcontract some of their functions as business associates to others, and disclose protected health information to those subcontractors to permit them to perform those functions, if they simply ''ensure that [the subcontractor] agrees to the same restrictions and conditions that apply to the business associate with respect to such information.''[15] Under the Proposed Rule, such a subcontractor is itself a business associate if it ''creates, maintains, or trans-

---

[2] HITECH Act, Sections 13401(a) and 13404(a), codified at 42 U.S.C. §§ 17931 & 17934.

[3] Proposed Rule 45 C.F.R. § 160.103 ''Business Associate''.

[4] 42 U.S.C. §§ 299b-21 *et. seq*.

[5] Proposed Rule 45 C.F.R. § 160.103 ''Business Associate'' (1)(i)(A).

[6] Current Rule 42 C.F.R. § 3.20. These functions include (1) efforts to improve patient safety and the quality of health care delivery; (2) collection and analysis of patient safety work product; (3) development and dissemination of information with respect to improving patient safety, such as recommendations, protocols, or information regarding best practices; (4) utilization of patient safety work product for the purposes of encouraging a culture of safety and of providing feedback and assistance to effectively minimize patient risk; (5) maintenance of procedures to preserve confidentiality with respect to patient safety work product; (6) provision of appropriate security measures with respect to patient safety work product; (7) utilization of qualified staff; and (8) activities related to the operation of a patient safety evaluation system and to the provision of feedback to participants in a patient safety evaluation system.

[7] HITECH Act, Section 13408, codified at 42 U.S.C. § 17938.

[8] Proposed Rule 45 C.F.R. § 160.103 ''Business Associate'' (3)(i) & (ii).

[9] *Id*. § 160.103 ''Business Associate'' (3)(ii).

[10] *Id*. § 160.103 ''Business Associate'' (3)(i).

[11] *Id*. § 160.103 ''Business Associate'' (4)(i).

[12] *Id*. § 160.103 ''Business Associate'' (4)(ii). The limited purposes for which such disclosure can be made are described in 45 C.F.R. 164.504(f), and include the furnishing of summary information to plan sponsors in connection with obtaining premium bids, modifying, amending or terminating a group health plan, or confirming an individual's participation in a plan.

[13] *Id.* § 160.103 ''Business Associate'' (4)(iii).

[14] *Id*. § 160.103 ''Business Associate'' (4)(iv).

[15] Current Rule 45 C.F.R. § 164.504(e)(2)(i)(D).

  HITR ISSN 2151-2876

mits protected health information on behalf of the business associate.''[16]

As a result of this change, the Proposed Rule would require business associates' agreements with their subcontractors to comply with the requirements for covered entities' agreements with business associates,[17] and would subject those subcontractors to all the other requirements of the Privacy and Security Rules that apply to business associates as a result of the HITECH Act and the other provisions of the Privacy and Security Rules themselves.[18] Under the Proposed Rule the business associate agreement between a business associate and a subcontractor would have to comply with all the requirements that apply to business associate agreements between covered entities and their business associates.[19]

Clarification of Business Associates' Obligations

The Proposed Rule would amend a number of the Privacy and Security Rules' sections that have been revised to specifically describe the obligations, formerly owing of covered entities only, with which business associates will be required to comply by virtue of the direct application of the Rules to them. A brief review of these changes illustrates the impact of the HITECH Act upon business associates—and upon their subcontractors, as described above. Under the Proposed Rule, the Secretary of Health and Human Services will be authorized to receive and investigate complaints against business associates (and thus their subcontractors) for failures to comply with the Privacy and Security Rules,[20] business associates (and thus their subcontractors), like covered entities, will be required to maintain records and submit compliance reports to the Secretary, cooperate in complaint investigations and compliance reviews, permit the Secretary access to information for such purposes,[21]; the Secretary will be empowered to act against business associates (and thus their subcontractors) in connection with complaints and noncompliance,[22] business associates (and thus their subcontractors) will be forbidden to threaten, intimidate, coerce, harass or discriminate against persons for filing complaints, cooperating with regulatory reviews or actions, or opposing unlawful actions,[23] and business associates (and thus their subcontractors) will be subject to civil money penalties for violations under the rules that apply to covered entities.[24]

Moreover, the Proposed Rule would provide that, to the extent that the business associate's arrangement with a covered entity calls for the business associate to carry out the covered entity's obligations under the Privacy or Security Rule, the business associate agreement must call for the business associate to comply with the applicable requirements as they would apply to the covered entity in the performance of that obligation.[25]

Clarification Regarding Uses and Disclosures by Business Associates

The Proposed Rule would modify the Privacy Rule's provisions regarding uses and disclosures of protected health information by business associates. The Proposed Rule would provide that the business associate (and thus its subcontractors) may use or disclose protected health information only as permitted by the applicable business associate agreement or as required by law.[26] In addition, under the Proposed Rule, the business associate (and thus its subcontractor) would not be permitted to use or disclose protected health information in a manner that would violate the rule, if done by the covered entity, except in limited circumstances.[27]

The Proposed Rule would clarify that a business associate may disclose protected health information to a subcontractor, and permit the subcontractor to create or receive protected health information on the covered entity's behalf, if the business associate obtains satisfactory assurance that the subcontractor will safeguard that information. The covered entity, however, is not required to obtain those assurances from a subcontractor of the business associate.[28] Instead, if the business associate discloses protected health information to a subcontractor, or allows the subcontractor to create or receive protected health information on the business associate's behalf, it is the business associate's responsibility to obtain those satisfactory assurances from the subcontractor.[29] These satisfactory assurances must be obtained by an agreement that meets the Proposed Rule's requirements for business associate agreements.[30]

Business Associate's Responsibility Regarding Conduct of Subcontractor

Under the current rule, covered entities are deemed not to be in compliance with the Privacy Rule if they know of patterns of activity or practice of a business associate that constitutes a material breach of the applicable business associate agreement, unless the covered entity takes reasonable steps to cure the breach or end the violation and, if such steps are unsuccessful, to terminate the business associate arrangement.[31] The Proposed Rule would require the business associate to perform the same responsibility with respect to its subcontractors.[32]

---

[16] Proposed Rule 45 C.F.R. § 160.103 ''Business Associate'' (3)(iii).
[17] *Id*. § 160.502(a)(4).
[18] HITECH Act, Sections 13401(a) and 13404(a), codified at 42 U.S.C. §§ 17931 & 17934.
[19] Current Rule 45 C.F.R § 164.504(e)(5).
[20] Proposed Rule 45 C.F.R. § 160.306(a) & (c).
[21] *Id.* § 160.310.
[22] *Id.* § 160.312.
[23] *Id*. § 160.316.
[24] *Id*. §§ 160.402 & 160.404(b), 160.406, 160.408(c) & (d), 160.410(a) and (c).
[25] *Id*. § 160.504(e)(2)(H).
[26] *Id*. §§ 160.502(a)(4) & (5).
[27] *Id*. §§ 164.504(e)(i)(2)(A) & (B).
[28] *Id*. § 164.502(e)(1)(i).
[29] *Id.* § 164.502(e)(1)(ii).
[30] *Id.* § 164.502(e)(2).
[31] Current Rule 45 C.F.R. § 164.504(e)(1)(ii).
[32] *Id*. § 164.504(e)(1)(iii).

Transition Provisions; Additional Time to Conform Business Associate Agreements

Generally speaking, the Proposed Rule would require compliance with its terms within 180 days following its publication in the Federal Register.[33] However, the Proposed Rule would provide affected parties additional time to conform their business associate agreements to the new requirements.[34] Generally speaking, if at the time the Proposed Rule takes effect, parties have business associate arrangements that comply with the current rule, they will have an additional year to bring their arrangements into compliance with the Proposed Rule.[35] In application, if a covered entity, or a business associate with respect to a subcontractor, had in place an agreement or arrangement that complied with the current rule, and did not modify or renew that arrangement during the 180 day period following the effective date of the proposed rule (60 days following its publication, or for a total of 240 days following publication), it would not be required to enter into a new conforming business associate agreement for another year.[36]

If the parties do renew or modify their arrangement during this initial 240 day period, they must incorporate the new terms required by the Proposed Rule. If they do not renew or modify their agreement during this period, however, their arrangement will be deemed to be in compliance until they do renew or modify, or for an additional period of one year (*i.e.*, 240 days plus one year), whichever occurs first.[37]

It is noteworthy that the additional time for compliance offered for business associate agreements does not apply to the Proposed Rule's other requirements. Thus, the substantive changes of the Proposed Rule, notably its requirements that subcontractors of business associates act as business associates themselves, applies 180 days following publication of the final rule.[38]

Marketing

The HITECH Act made substantive changes to the Privacy Rule with respect to requirements for a HIPAA compliant authorization to be obtained by covered entities and business associates for marketing communications, unless an exception applies.[39] The Preamble to the NPRM explained that the provisions of HITECH relating to marketing reflected concerns as to the efficacy of the current Privacy Rule to regulate subsidized health care marketing communications to individuals utilizing their PHI and a desire of Congress to close potential loopholes in the current Privacy Rule that might permit unauthorized communications motivated by commercial purposes.[40]

The NPRM implemented the HITECH Act changes by making changes to the definition of ''marketing'' by adding a definition of ''financial remuneration,''[41] providing that treatment communications for which financial remuneration is received are not included as ''marketing'' requiring an authorization if an appropriate notice is given to the recipient together with an ability to opt out of future communications,[42] providing a limited exception from the definition of ''marketing'' for refill notifications where financial remuneration is received,[43] and providing that health care operations communications for which financial remuneration is received requires an authorization.[44]

Definition of Financial Remuneration

The term ''financial remuneration'' is key to understanding the limitation on permissible health care operations disclosures. While the HITECH Act used the term ''direct or indirect payment,'' the NPRM adopted the term ''financial remuneration'' to distinguish the concept from ''payment for health care.'' As defined, ''financial remuneration'' means ''direct or indirect payment from or on behalf of a third party whose product or service is being described'' in a communication.[45] Thus payments by others to a covered entity or business associate to promote the products or services of a third party, so long as they are not made on behalf of the third party, would not trigger the definition of ''marketing'' for purposes of the Privacy Rule. In addition, remuneration that is not financial is disregarded.[46]

Definition of Marketing

The principal changes to the definition of ''marketing'' are an attempt to make a clear distinction between communications for treatment and communications for health care operations.[47] Thus, the NPRM rearranges the current definition of ''marketing'' to delineate three major categories of communications that would not constitute ''marketing:'' certain treatment communications, certain refill reminders and certain health care operations communications.[48]

Communications for treatment that are not subsidized do not fall within the meaning of ''marketing.'' Moreover, communications for treatment for which financial remuneration is received do not require an authorization so long as the provider's notice of privacy practices states that such communications may be made and the communication provides notice of the financial remuneration and an unburdensome process for opting out of receipt of future communications is allowed.[49] Unlike the exception applicable to refill reminders, there is no required correlation between the amount of the subsidy and the cost of the communication with respect to treatment communications.

By contrast, communications for health care operations for which financial remuneration is received re-

[33] *Id.* § 164.104(c)(1).
[34] *Id.* § 164.532.
[35] *Id.* § 164.532(e)(2).
[36] *Id.* § 164.532(e)(1).
[37] *Id.* § 164.532(e)(2).
[38] Proposed Rule 45 C.F.R. § 164.532(e)(1).
[39] HITECH Act, Section 13406(a), codified at 42 U.S.C. § 17936.
[40] 75 Fed. Reg. 40884 (Jul. 14, 2010)
[41] Proposed Rule 45 C.F.R. § 164.501 ''Marketing'' (3).
[42] *Id.* §§ 164.501 ''Marketing'' (2)(i); 164.514(f)(2); 164.520(b)(1)(iii)(A).
[43] *Id.* § 165.501 ''Marketing'' (2)(ii).
[44] *Id.* § 164.501 ''Marketing'' (2)(iii).
[45] *Id.* § 164.501 ''Marketing'' (3).
[46] 75 Fed. Reg. 40886 (Jul. 14, 2010).
[47] *Id.* at 40885-86.
[48] Proposed Rule 45 C.F.R. § 164.501 ''Marketing'' (2).
[49] *Id.* § 165.501 ''Marketing'' (2)(i); 164.514(f)(2); 164.520(b)(1)(iii)(A).

  HITR ISSN 2151-2876

quire an authorization without exception.[50] Communications for health care operations for which no subsidy is received do not require an authorization and communications promoting health and wellness generally are not ''marketing.''[51]

The NPRM identified HHS's concern that it may be difficult in some instances to distinguish between treatment communications and health care operations communications. Subsidized communications intended for a broad audience will generally be health care operations communications, while individually targeted communications based on individual factors to further treatment will more likely be considered for treatment. The NPRM requested comments on this subject.[52]

The Preamble to the NPRM stressed HHS's concern that the intent of Congress is unclear whether communications for treatment for which financial remuneration is received should be treated the same as for health care operations communications for which financial remuneration is received, that is, that in both cases an authorization would be required. In spite of this ambiguity, HHS has provided in the NPRM that communications for treatment for which financial remuneration is received are nevertheless not ''marketing'' so long as notice and opt out requirements are met.[53] This underscores HHS's predisposition to enable treatment communications. However, the NPRM requests comments on the appropriateness of applying any or no restrictions upon subsidized treatment communications.[54]

The NPRM requested comments regarding the scope of the required opt-out for subsidized treatment communications, that is whether the recipient should be able to opt out of future communications related to the same products and services covered by the first communication rather than being able to opt out of all future subsidized treatment communications. The NPRM also requested comments regarding the ''workability'' of providing intended recipients with an opportunity to opt out of receiving subsidized treatment communications prior to the first such communication.[55]

Refill Reminders

The HITECH Act included a statutory exception to the restrictions on marketing for refill reminders[56] The NPRM essentially restates the statute, which permits subsidized refill reminders for a drug or biologic that is currently prescribed, so long as the subsidy is reasonably related to the cost of making the communication.[57] The NPRM requested comments on whether the exception for refill reminders should be expanded to permit communications related to currently prescribed drugs and biologics that extend beyond mere refill reminders, such as to describe treatment alternatives and new drugs and biologics. The NPRM also requested comments on the types of costs that could be subsidized in the context of refill reminders.[58]

Disclosure of PHI for Fundraising

The Privacy Rule permits a covered entity to provide to a business associate or a related fundraising organization PHI consisting of certain demographic information about individuals and the dates that health care services were provided to such individuals so long as the covered entity's notice of privacy practices includes a statement that the covered entity may use this information to contact patients for fundraising purposes.[59] The HITECH Act directed the Secretary of HHS to establish regulations requiring covered entities to provide an opt out mechanism in every fundraising communication.[60] The NPRM proposed such regulations mandating a clear and conspicuous opt out from further communications to be contained in each fundraising communication and further mandating that the means to opt out not be burdensome on the individual.[61] The covered entity's notice of privacy practices must specify that individuals have a right to opt out of receiving such communications.[62] A covered entity may not require a patient to receive fundraising communications as a condition of treatment or services and a covered entity may not send fundraising communications to an individual who has opted out.[63] The Secretary has requested comments about the workability of a pre-solicitation opt out.[64]

Sale of PHI

The HITECH Act addressed the controversial topic of the potential sale of protected health information (''PHI'') by generally requiring an authorization be obtained by a covered entity or a business associate before a sale of PHI for remuneration can be made.[65] The Act enumerates a number of exceptions to this blanket prohibition. In addition, the Act conferred upon the Secretary of HHS the power to recognize additional exceptions,[66] which the Secretary has exercised to a certain extent in the NPRM.

The NPRM restated the general prohibition against receipt of payment, directly or indirectly, in exchange for the disclosure of PHI, without a HIPAA compliant authorization.[67] The authorization must include an express statement that the disclosure is in exchange for payment in order that the affected individual can be informed of that fact in deciding whether to give the authorization.[68] There is no requirement that the authori-

[50] *Id.* § 164.501 ''Marketing'' 2(iii).
[51] 75 Fed. Reg. 40886 (Jul. 14, 2010).
[52] *Id.*
[53] 75 Fed. Reg. 40885-86 (Jul. 14, 2010).
[54] *Id.* at 40886.
[55] *Id.*
[56] HITECH Act, Section 13406(a)(2)(A), codified at 42 U.S.C. § 17936.
[57] Proposed Rule 45 C.F.R. § 164.501 ''Marketing'' (2)(ii).
[58] 75 Fed. Reg. 40885 (Jul. 14, 2010).
[59] 45 C.F.R. § 165.514(f)(1), (2).
[60] HITECH ACT, Section 13406(b), codified at 42 U.S.C. § 17936(b).
[61] Proposed Rule 45 C.F.R. § 164.514(f)(1).
[62] *Id.* § 164.520.
[63] Proposed Rule 45 C.F.R. § 164.514(f)(1)(ii).
[64] 75 Fed. Reg. 40897 (Jul. 14, 2010).
[65] HITECH Act, Section 13405(d), codified at 42 U.S.C. § 17935(d).
[66] *Id.*; section 13405(d)(2)(G), codified at 42 U.S.C. § 17935(d)(2)(G).
[67] Proposed Rule 45 C.F.R. § 164.508(a)(4)(i).
[68] *Id.*

zation state that the recipient of the PHI may further disclose the PHI for remuneration.[69]

Exceptions

Public Health. Disclosures in connection with receipt of remuneration for public health purposes do not require an authorization, provided the disclosures are in accord with the provisions of the Privacy Rule permitting such disclosures.[70]

While the HITECH Act conferred authority on the Secretary to evaluate the impact of and potentially impose limits on the amounts that could be paid, the Secretary declined to impose such limits, but is soliciting comments on the topic.[71]

Research Purposes. Disclosures in connection with receipt of remuneration for research purposes permitted under the Privacy Rule do not require an authorization, so long as the remuneration is reasonably related to the cost of preparing and transmitting the information.[72]

Treatment and Payment. Disclosures in connection with receipt of remuneration for treatment and payment in accord with the Privacy Rule do not require an authorization.[73] Although the HITECH Act did not expressly include a reference to ''payment,'' the Secretary determined that disclosure of PHI to obtain payment is not a sale of PHI.[74]

Disclosures in Connection with Sale, Transfer, Merger, Consolidation. Transactions involving the sale, transfer or corporate transaction of a covered entity or business associate are included within the definition of ''health care operations.'' Disclosures in connection with such transactions do not require an authorization.[75]

To or By Business Associates. Disclosures to or by a business associate in furtherance of its activities on behalf of a covered entity do not require an authorization, provided the remuneration paid to the business associate by the covered entity is only for the performance of such activities.[76]

To an Individual. Disclosures to an individual pursuant to a HIPAA permitted request for disclosure does not require an authorization.[77]

Disclosures Required by Law. Disclosures to law enforcement permitted under the Privacy Rule or otherwise required by law do not require an authorization.[78]

This exception was added by the Secretary under authority to recognize additional exceptions conferred by the HITECH Act.[79]

Disclosures Permitted by the Privacy Rule. The Secretary also used the authority to recognize additional exceptions to except disclosures otherwise permitted by the Privacy Rule so long as the remuneration is reasonably related to the cost of making the disclosure or otherwise is authorized by law.[80] In the Preamble to the NPR, HHS notes that there are a wide variety of State authorized fees for providing information and asks for public comment on this proposed exception.[81]

Right to Request Restrictions on Use and Disclosure

What may have seemed like a good idea at the time, the HITECH Act included a provision requiring the Secretary of HHS to promulgate regulations enabling individuals who pay out of pocket in full for a particular health care service to require the provider not to furnish information to a health care plan about the service unless such disclosure is otherwise required by law.[82] The resulting proposed regulation raises many more questions than it answers.[83]

The proposed regulation provides that a covered entity must agree to a requested restriction on disclosure to a health plan if the disclosure is for the purpose of payment or health care operations and is not required by law and the information to be restricted relates solely to treatment for which payment has been made in full on behalf of the individual.[84]

HHS stated in its commentary that implicit in the rule is a requirement that an individual be permitted by a covered entity to pay for discrete services, rather than all services covered by a health plan. HHS also stated that amounts paid under this rule should not be expected to be applied to annual deductible requirements under health plan coverage.[85]

In the Preamble, HHS noted the issues that should be addressed with respect to this proposed regulation and about which it is requesting comments. These issues include:

- The types of interactions among individuals and covered entities that may frustrate compliance with the rule;
- How communications ancillary to the subject restricted treatment may be affected, such as electronic prescriptions that may be automatically communicated to a health plan;
- The potential obligation of covered entities who know of the restriction to notify downstream providers;
- The types of disclosures that may be required by law, notwithstanding a restriction;

[69] 75 Fed. Reg. 40890 (Jul. 14, 2010).
[70] Proposed Rule 45 C.F.R. § 164.508(a)(4)(ii)(A). *See* 45 C.F.R. §§ 164.512(b), 164.514(e).
[71] Proposed Rule 45 C.F.R. § 164.508(a)(4)(ii)(A); HITECH Act, Section 13405(d), codified at 42 U.S.C. § 17935(d); 75 Fed. Reg. 40891 (Jul. 14, 2010).
[72] Proposed Rule 45 C.F.R. § 164.508(a)(4)(ii)(B).
[73] *Id.* § 164.508(a)(4)(ii)(C).
[74] 75 Fed. Reg. 40891 (Jul. 14, 2010).
[75] *Id.*; Proposed rule 45 C.F.R. § 164.608.(a)(4)(ii)(D).
[76] *Id.* § 164.608(a)(4)(ii)(E).
[77] *Id.* § 164.508(a)(4)(ii)(F).
[78] *Id.* § 164.508(a)(4)(ii)(G).
[79] 75 Fed. Reg. 40892 (Jul. 14, 2010.)
[80] Proposed rule 45 C.F.R. § 164.508(a)(4)(ii)(H). The Privacy Rule is comprised of Subpart E of Part 160 of 45 C.F.R.
[81] 75 Fed. Reg. 40892 (Jul. 14, 2010).
[82] HITECH Act, Section 13405(a), codified at 42 U.S.C. § 17935(a).
[83] Proposed Rule 45 C.F.R. § 164.522(a)(ii), (vi).
[84] *Id.*
[85] 75 Fed. Reg. 40900 (Jul. 14, 2010).

  HITR ISSN 2151-2876

- How compliance with the regulation would be accomplished in an HMO setting where payment for services is on a prepaid or periodic basis;

- The extent to which covered entities may be required to attempt to secure payment from an individual seeking to invoke this right; and

- The implications of payment by a health plan for follow up care after prior related services are paid for separately on behalf of the individual.

Clearly, numerous comments will be forthcoming regarding this controversial provision of the HITECH Act and these regulations.

Access to Information Contained in an Electronic Health Record

The HITECH Act provides that an individual shall be entitled to obtain a copy in electronic format of the individual's PHI that a covered entity maintains in an electronic health record. In addition, the Act requires that the covered entity provide information in that format to another person specified by the individual. The covered entity may only charge its labor costs and supply and media costs for providing such data.[86] The NPRM proposes regulations to implement this part of the HITECH Act.[87]

While the Act limited its application to information maintained in an electronic health record, the NPRM has expanded the scope of the Act's requirements in proposing regulations that apply to information maintained in a designated record set, regardless of its being contained in an electronic health record.[88] If the information is maintained in an electronic format, the covered entity must provide access to the PHI in the electronic format requested, if it can be so produced, and if not, then in a readable electronic format or any other format agreeable to the covered entity and the individual.[89]

The requested information must be provided in a timely and convenient manner to the individual. HHS noted that the current regulations would permit up to 90 days to respond to a request for access to information and that this part of the regulations is not being affected by the NPRM. However, HHS requested comments on this provision as it relates to access to electronic records.[90] If the information is to be provided to a third party, the request must be in writing and signed by the individual.[91]

In the Preamble to the NPRM, HHS commented that covered entities must take appropriate measures to ensure the security of information that is being provided on request, particularly if the information is made available through web-based applications or portals. HHS also noted that it is assumed covered entities will be able to respond to requests through electronic modalities, but requests comments on that assumption.[92]

Changes to the Enforcement Rule

The proposed rule contains substantial changes to HIPAA's Enforcement Rule that address overall compliance with the statute, investigations, and the imposition of civil monetary penalties.[93] As discussed above, civil monetary penalties may now be assessed directly against business associates.[94] The rule proposes a tiered structure for the penalties, with more serious violations meriting higher penalties. In determining the amount of a civil money penalty, OCR will consider the following factors:

1. The nature and extent of the violation, taking into account the number of individuals affected and the time period during which the violation occurred;
2. The nature and extent of any physical, financial, or reputational harm, or whether an individual's ability to obtain health care was hindered by the violative action;
3. The covered entity's or business associate's history of prior compliance with the statute, including whether similar violations have occurred in the past, the extent of any past attempts to rectify past noncompliance, the receptiveness of a business associate or covered entity to technical assistance provided by OCR, the manner of response to prior complaints;
4. The financial condition of the covered entity or business associate, including analysis of whether financial difficulties affected the entity's compliance efforts, whether imposition of monetary penalties would jeopardize the entity's provision or payment for health care, and the size of the entity;
5. Other factors as required for justice.[95]

Affirmative Defenses

OCR proposes that no civil monetary penalties be assessed for violations occurring prior to February 18, 2011, if the violations are offenses punishable under HIPAA's criminal penalties provisions. For violations occurring after February 18, 2011, civil monetary penalties may not be assessed if a penalty has been imposed under HIPAA's criminal penalties provisions.[96]

For violations occurring prior to February 18, 2009, civil monetary penalties may not be imposed on a covered entity if a) the covered entity establishes that it did not have knowledge of the violation and would not have known that the violation occurred even by the exercise of reasonable diligence, or b) the violation is due to circumstances that make it unreasonable to comply, the violation is not due to willful neglect, and is corrected within thirty days of when it actually learned of the violation or should have learned, by the use of reasonable diligence, of the violation, whichever is sooner. OCR retains the discretion to extend the 30-day period as it deems necessary.[97] OCR proposes similar standards for violations occurring on or after February 18, 2009, while broadening its application to include business associates in addition to covered entities. Notably, OCR may waive imposition of penalties in whole or in part,

[86] HITECH Act, Section 13405(e), codified at 42 U.S.C. § 17935(e).
[87] Proposed Rule 45 C.F.R. § 164.524.
[88] 75 Fed. Reg. 40901 (Jul. 14, 2010).
[89] Proposed Rule 45 C.F.R. § 164.524(c)(2)(ii).
[90] 75 Fed. Reg. 40903 (Jul. 14, 2010).
[91] Proposed Rule 45 C.F.R § 164.524(c)(3).
[92] 75 Fed. Red. 40901 (Jul. 14, 2010).
[93] Proposed Rule 45 C.F.R. 160.300–.418.
[94] *Id.* §§ 160.300; 160.304; 160.306(a), (c); 160.308; 160.310; 160.312; 160.316; 160.401; 160.402(c)(2); 160.404(b); 160.406; 160.408(c), (d); 160.410(a), (c).
[95] *Id.* § 160.408.
[96] *Id.* § 160.410(a).
[97] *Id.* § 160.410(b).

to the extent that the payment of the penalty would be excessive relative to the violation.[98]

Implementation Timeframes

The majority of HITECH's provisions took effect on February 18, 2010. However, OCR states that ''[w]e recognize that it will be difficult for covered entities and business associates to comply with the statutory provisions until after we have finalized our changes to the HIPAA rules.''[99] Therefore, OCR proposes to provide covered entities and business associates with 180 days beyond the effective date of the final rule to come into compliance with ''most of the rule's provisions.''[100] Further, OCR proposes and seeks comment on a general 180-day compliance period for all future HIPAA-related rulemakings.[101]

[98] *Id.* § 160.412.

[99] 75 Fed. Reg. 40868, 40871 (Jul. 14, 2010).
[100] *Id.*
[101] Proposed Rule 45 C.F.R. § 160.105.

  HITR ISSN 2151-2876