HIPAA Omnibus Final Rule Modifies Notice of Privacy Practices Requirements for Covered Entities

By Kimberly J. Kannensohn, Nathan Kottkamp and Allison Harms, McGuireWoods, LLP, Richmond, VA

On Jan. 17, 2013, the Department of Health and Human Services (“HHS”) released the Omnibus Final Rule pursuant to the Health Information Technology for Economic and Clinical Health Act of 2009 (“HITECH Act”) and the Genetic Information Nondiscrimination Act of 2008 (“GINA”). The Final Rule modifies and expands the requirements for the statements that covered entities must include in their Notice of Privacy Practices (“NPP”). An NPP is the HIPAA-mandated notice that apprises patients of their rights with regard to protected health information (“PHI”) and the limits imposed upon a covered entity’s uses and disclosures of PHI.

**Notice of Privacy Practices**

The Privacy Rule requires covered entities to maintain and distribute an NPP, which must provide that any uses or disclosures other than those expressly permitted by the Privacy Rule will be made only with the written authorization of an individual.1 The Final Rule expands the requirements to include provisions designed to afford individuals with a better understanding of (i) a patient’s right to restrict disclosures; (ii) the types of uses and disclosures that require individual authorization; (iii) a patient’s right to opt out of certain disclosures;2 (iv) rights to notice in the event of a breach; and (v) rights with respect to the use of their genetic information for health plan underwriting purposes.

**Uses and Disclosures**

*Disclosures for which Patient Authorization is not Required*

The Privacy Rule requires that an NPP be (i) written in plain English, (ii) include a capitalized header explaining that the NPP describes how medical information about an individual may be used and disclosed and how the individual can obtain access to such medical information, and (iii) must contain a description, and for treatment, payment and health care operations, at least one example, of the types of uses and disclosures that the covered entity is permitted to make without patient authorization, including:

* Treatment – for example, if a treatment is provided by a specialist who asks a primary care physician to share a patient’s PHI.
* Payment – for example, to complete a claim form to obtain payment from an insurer.
* Healthcare Operations – for example, to engage in quality review activities or for the implementation of compliance programs.
* Public Health, Abuse or Neglect, and Health Oversight – for example, to alert a person who may have been exposed to a disease or may be at risk for contracting or spreading a disease.
* Other Authorizations Required by Law, including: legal proceedings and law enforcement; Workers’ Compensation; PHI related to Inmates; Military, National Security and Intelligence Activities; for the Protection of the President; certain approved research purposes; organ donation; for use by coroners, medical examiners and funeral directors; or any other reason such a disclosure would be required by law.3

The NPP description of uses and disclosures must be sufficiently detailed to place the individual on notice of the uses and disclosures that are permitted or required by the Privacy Rule and other applicable law. Further, the covered entity must include a separate statement regarding its intentions in the NPP if the covered entity intends to (i) contact the individual to provide appointment reminders; (ii) provide information regarding treatment alternatives or other health-related benefits and services; or (iii) disclose PHI to the plan sponsor (assuming the covered entity is a group health plan, health insurance issuer, or HMO).4

*Disclosures for which Patient Authorization is Required*

The Final Rule modifies § 164.520(b)(1)(ii)(E) to expand the statements in the NPP regarding uses and disclosures that require authorization. The Privacy Rule requires that the NPP include a statement regarding uses and disclosures that will be made only with the individual’s written authorization and that the individual may revoke such authorization in accordance with § 164.508(b)(5).5 Although the Final Rule does not require the NPP to include a list of all situations requiring authorization, the NPP must contain a statement indicating that the following uses and disclosures will be made only with authorization from the individual: (i) most uses and disclosures of psychotherapy notes (if recorded by a covered entity); (ii) uses and disclosures of PHI for marketing purposes, including subsidized treatment communications; (iii) disclosures that constitute a sale of PHI; and (iv) other uses and disclosures not described in the NPP. The Final Rule adopts, as proposed, the requirement that if a covered entity intends to send fundraising communications to an individual, the NPP must also inform the individual of this intent and that the individual has the right to opt out of such fundraising communications with each solicitation.6 Finally, the Final Rule requires that the NPP contain a statement indicating that the covered entity is required to notify the patient of any breach of his or her unsecured PHI.

Additionally, consistent with GINA, health plans are required to include a statement in their NPPs that they are prohibited from using or disclosing genetic information of an individual for underwriting purposes.7 The Final Rule included a limited exception to this requirement for certain issuers of long-term care policies.

**Individual Rights to Authorize or Restrict Disclosure of PHI**

The Privacy Rule requires that the NPP contain a statement of the individual’s rights with respect to PHI and a brief description of how the individual may exercise these rights, including: (i) the right to request restrictions or limitations on certain uses and disclosures of PHI, (ii) the right to receive confidential communications of PHI, (iii) the right to inspect and copy PHI, (D) the right to amend PHI in certain circumstances, (E) the right to receive an accounting of disclosures of PHI, and (F) the right of an individual, including an individual who has agreed to receive the NPP electronically, to obtain a paper copy of the NPP from the covered entity upon request.8

The Final Rule modifies § 164.520(b)(1)(iv) to provide that an NPP must state that a healthcare provider may choose not to comply with a restriction request, unless an individual has paid for services out-of-pocket, in full, and the individual requests that the healthcare provider not disclose PHI related solely to those services to a health plan. The NPP may specify that a patient’s request to restrict be made in writing, and that the request should identify: (i) the information to be restricted, (ii) the type of restriction being requested (i.e. on the use of information, the disclosure of information, or both), and (iii) to whom the limits should apply. If such a request is made, the healthcare provider must accommodate the individual’s request, except where the healthcare provider is required by law to make a disclosure.9

The Final Rule does not require covered entities to inform other downstream covered entities of an individual’s request not to disclose PHI to a health plan; however, the commentary to the Final Rule suggests that covered entities should consider providing notification where feasible.10

**Covered Entity Duties**

The Privacy Rule requires a covered entity to state in its NPP that: (i) the covered entity is required by law to maintain the privacy of PHI and to provide individuals with notice of its legal duties and privacy practices with respect to PHI; (ii) the covered entity is required to abide by the terms of the NPP currently in effect; (iii) the covered entity reserves the right to change the terms of its NPP and to make the new NPP provisions effective for all PHI that it maintains, and (iv) the covered entity will provide individuals with a revised NPP in accordance with the Privacy Rule requirement.

Additionally, the NPP must contain (i) a statement that individuals may complain to the covered entity and to the Secretary if they believe their privacy rights have been violated; (ii) a brief description of how an individual may file a complaint with a covered entity; and (iii) a statement that the individual will not be retaliated against for filing a complaint. The NPP must also contain the name or title, and telephone number of a person or office to contact for further information as well as the date the NPP, as revised, became effective.11 The Final Rule does not modify these requirements. Finally, to comply with GINA, health plans are required to include a statement in their NPPs that they are prohibited from using or disclosing genetic information of an individual for underwriting purposes.12

**Notification to Individuals of Modifications to the NPP**

The Final Rule does not modify the current requirement, applicable to all covered entities, to distribute revisions to the NPP.13 Therefore, when a healthcare provider revises an NPP, the healthcare provider must make the NPP readily available upon request on or after the effective date of the revisions at the delivery site to existing patients who request a copy, must post the revised NPP on its website, if applicable, and must post the NPP in a prominent location on its premises. Providers may even post a summary of the NPP, provided that the full NPP is immediately available. New patients who receive services for the first time after modification of an NPP should be provided with a copy of the revised NPP. Consistent with the existing rules, providers should retain copies of previous versions of their NPPs and of any written acknowledgements by patients of receipt of NPPs.

The Final Rule requires a health plan that currently posts its NPP on its website in accordance with § 164.520(c)(3)(i) to: (i) prominently post the material change or its revised notice on its website by the effective date of the material change to the notice (i.e., the compliance date); and (ii) provide the revised notice, or information about the material change and how to obtain the revised notice, in its next annual mailing to individuals then covered by the plan, such as at the beginning of the plan year or during open enrollment. If a health plan does not have a customer service website, then the health plan must provide the revised NPP, or information about the material change and how to obtain the revised notice, to individuals covered by the plan within 60 days of the material revision to the notice.

**Conclusion**

The Final Rule, which became effective on March 26, 2013, modifies and expands the statements that covered entities must include in their NPP. Noncompliance with the Final Rule exposes covered entities to patient complaints, governmental investigations, and civil and criminal penalties. Covered entities should re-evaluate the content of their NPPs and their policies and procedures regarding revision and distribution to determine whether they are compliant with the Final Rule. As the deadline to comply with the new NPP requirements is September 23, 2013, covered entities should begin to work toward compliance as soon as possible.

|  |  |
| --- | --- |
| 1 | 45 C.F.R. § 164.520. |
| 2 | 45 C.F.R. § 164.520(b)(1) |
| 3 | 45 C.F.R. § 164.520(b)(1) |
| 4 | 45 C.F.R. § 164.520(b)(1)(iii)(A)-(C) |
| 5 | 45 C.F.R. § 164.520(b)(1)(ii)(E) |
| 6 | 45 C.F.R. § 164.520(b)(1)(iii)(B) |
| 7 | 45 C.F.R. § 164.520(b)(1)(iii)(C) |
| 8 | 45 C.F.R. § 164.520(b)(1)(iv)(A)-(F) |
| 9 | 45 C.F.R. § 164.520(b)(1)(iv)(A) |
| 10 | 78 Fed. Reg. 5567, 5,629 (Jan. 25, 2013) |
| 11 | 45 C.F.R. § 164.520(b)(v) |
| 12 | 45 C.F.R. §164.520(b)(1)(iii)(C) |
| 13 | 45 C.F.R. § 164.520(c)(2)(iv) |

*The ABA Health eSource* is distributed automatically to members of the [ABA Health Law Section](http://www.americanbar.org/content/aba/groups/health_law.html) .