HHS Issues New HITECH/HIPAA Rule: Implications for Hospice Providers

Hospice Provider Compliance “To Do” List

Providers need to complete the following updates by September 23, 2013:

- Update their patient privacy notices
- Update their policy on reviewing and reporting a breach of protected health information (PHI) or electronic protected health information (ePHI)
- Update their business associate agreements unless they qualify for an extended transition period
- Update fundraising communication to include an “opt-out” option for patients

On January 17, 2013, the Department of Health and Human Services (HHS) Office for Civil Rights (OCR) released an omnibus Final Rule that implements modifications to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) as required by the Health Information Technology for Economic and Clinical Health (“HITECH”) Act. The Final Rule marks the most significant re-write of the HIPAA rules since the law was enacted.

For hospice providers, a number of the Final Rule provisions likely require substantial operational changes and the development of new compliance documents, including amended policies and procedures, revised notices of privacy practices and new and revised business associate agreements. This summary provides an overview of the key changes introduced in the Final Rule relevant to hospice providers.

When is Compliance Required?

Compliance with most of the new requirements introduced in the Final Rule is required by September 23, 2013. An extended compliance period is provided for the modification of certain existing business associate agreements, as described in more detail below.

New Breach Standard

The Final Rule made a substantial change to the definition of a “breach” of protected health information (PHI), by removing the previous risk of harm standard. This modification to the definition of breach will

---

3 The current three exceptions to the definition of breach still remain under the revised standard. The breach requirements also continue to apply only to “unsecured PHI” (i.e., PHI which has not been sufficiently encrypted or destroyed in accordance with federal standards).

© National Hospice and Palliative Care Organization, 2013
make it more difficult for covered entities and business associates to justify a decision not to provide notification following a suspected breach incident.

Under the current breach standard, an incident is considered a breach only if it poses “a significant risk of financial, reputational, or other harm to the individual.” The new standard introduces a presumption that any impermissible acquisition, access, use or disclosure of PHI under the Privacy Rule is a breach unless a covered entity or business associate can demonstrate that there is a low probability that the PHI has been compromised. Covered entities must determine whether there is a low probability that PHI has been compromised by performing a risk assessment. All risk assessments must be documented and must address, at a minimum, the following four factors:

- The nature and extent of the PHI involved—this may include an evaluation of the types of identifiers involved and the likelihood of re-identification;
- The unauthorized person who used or received the PHI—such as whether the unauthorized person had an obligation to protect the privacy or security of the PHI;
- Whether the PHI was actually acquired or viewed—this may require the use of forensics or other investigative methods; and
- The extent to which the risk to the PHI has been mitigated—this may include considering such things as whether the recipient has agreed to destroy the information.

If the facts indicate more than a low probability of compromise, notification regarding the breach is required, regardless of the likelihood of harm to the affected individual.

Following a breach, covered entities are still required to notify affected individuals, the Secretary of HHS, and the media (if a breach affects more than 500 residents of a State or jurisdiction). The current timing, content and methods for notification also remain unchanged.

In the Final Rule, HHS states that it intends to issue guidance to aid covered entities and business associates in performing risk assessments and to assist with the individual notification requirements.

**Expanded Individual Rights**

The Final Rule expands individuals’ rights with respect to their PHI in two important ways—(1) it provides them with the right to receive certain PHI electronically; and (2) it allows them to restrict certain disclosures of PHI to their health plans. Hospice providers will have to revise their current policies and procedures and evaluate current system capabilities to ensure compliance with these new requirements.

*Electronic Access*

The Final Rule provides individuals with the right to obtain an electronic copy of their PHI maintained in a “designated record set” electronically. A designated record set includes medical and billing records maintained by or for a covered entity provider, as well as any other records used in whole or part by or for a covered entity provider to make decisions about patients. Under the Final Rule, covered entities must provide individuals with access to their electronic information upon request and in the electronic format requested, if that format is readily producible. If the requested format is not available, then a mutually agreed upon format (e.g., Microsoft Word or Excel, text-based PDF) must be provided. Covered entities are not required to provide individuals with unlimited choices in terms of the available electronic forms. Notably, HHS clarifies that if requested by the individual, covered entities may provide the electronic copy of PHI through unencrypted e-mail, provided that the covered entity advises the individual of the risk of

---

doing so. In such a case, the covered entity would not be responsible for any unauthorized access of PHI while in transmission or for safeguarding PHI once delivered to the individual.

The Final Rule also provides individuals with the right to request that covered entities and business associates provide a copy of their PHI directly to a designated individual. This right applies to both paper and electronic information. Any such request must be in writing, signed by the individual, and must clearly identify the designated recipient and where the information should be sent. Reasonable verification procedures should be used by hospice providers to verify the identity and authority of the requesting individual prior to disclosing any information.

As permitted under the current Privacy Rule, covered entities can charge a reasonable, cost-based fee, but the fee must not be greater than the covered entity's labor and supply costs and may not include a standard “retrieval fee.” The Final Rule also tightens the time frame for providing access to records by eliminating the existing provision that allowed 60 days to provide access when records are maintained by the covered entity off-site. Under the new rule, covered entities must provide access to all paper and electronic PHI within 30 days of the individual’s request, with the option of a one-time 30-day extension available.

Right to Restrict Certain Disclosures to Health Plans

The Privacy Rule currently provides individuals with the right to request restrictions on the use or disclosure of their PHI, but covered entities are not legally required to agree to the request. The Final Rule enhances this right by requiring health care providers to honor requests by patients to restrict disclosures to health plans for purposes of carrying out payment or healthcare operations if the disclosure is not otherwise required by law and the PHI relates solely to a health care item or service for which the individual has paid the covered entity out of pocket in full. Payment can also be made by a family member, other person or other health plan on behalf of an individual to qualify as “out of pocket” payment.

Providers are not obligated to notify downstream providers of an individual’s request for a restriction; however, HHS does encourage providers to counsel individuals that they need to separately exercise this right with other providers. It is important to note that individuals may not exercise this right where a provider is required by State or other law to submit a claim to a health plan for services provided to an individual and such law does not include an exception for individuals paying out-of-pocket.

In order to implement this new requirement, hospice providers will likely need to develop a method to flag or include a notation in the record of any individual who has exercised this right to restrict disclosures regarding services paid for out of pocket, in order to ensure that specific records are not sent or made accessible to health plans. HHS provides additional operational guidance in the Final Rule for implementing this requirement, including:

- How to handle payment for bundled services;
- Treatment of dishonored payments; and
- Requests for follow-up care that is not paid for out-of-pocket.

Modifications to Notices of Privacy Practices Required

The Final Rule requires several changes to covered entities’ notice of privacy practices (“Notice”). Notices must now include a statement regarding the right of affected individuals to be notified following a data breach and must describe certain uses and disclosures of PHI that require patient authorization

---

5 78 Fed. Reg. at 5626.
related to psychotherapy notes, marketing, and the sale of PHI. The Notice must also inform patients of their right to restrict certain disclosures of PHI to health plans where the individual pays out of pocket in full.

HHS makes clear that these new Notice requirements are material changes and will require covered entities to provide new Notices to individuals. The Final Rule does not amend the Notice distribution requirements for providers issuing revised Notices. Under the current Privacy Rule, direct treatment providers must make the revised Notice available upon request on or after the effective date of the revision, and if there is a physical delivery site, must make the Notice available at the site and post the revised Notice in a clear and prominent location.

Direct Liability for Business Associates and Amendments to Business Associate Agreements Required

Business associates and all downstream business associate subcontractors will now be directly subject to applicable HIPAA rules, including the HIPAA Security Rule and certain provisions of the Privacy Rule. HHS expands the reach of the rule by modifying the definition of business associates to specifically include several new entities, including subcontractors that create, receive or transmit PHI on behalf of business associates and entities that provide data transmission of PHI (e.g., health information exchanges, e-prescribing gateways). HHS also provides additional guidance regarding who is a business associate. Significantly, the agency makes clear that data storage vendors that maintain PHI (both hardcopy and electronic), are business associates even if the vendor never actually views or accesses the PHI. This would include entities such as cloud service providers and document storage vendors. Hospice providers contracting with any types of entities falling within the definition of “business associate” will need to ensure that they have a HIPAA compliant business associate agreement in place. Compliance by business associates is required regardless of whether a business associate agreement is executed.

Business associate agreements will need to be modified to meet additional requirements. The Final Rule requires that business associate agreements obligate business associates to report breaches of unsecured PHI and comply with the entire Security Rule. To the extent a covered entity delegates its obligations under the Privacy Rule then the Final Rule requires that the business associate agreement also obligate the business associate to comply with all Privacy Rule requirements that apply to the covered entity with respect to the performance of those obligations. The Final Rule provides an extended transition period up to September 22, 2014 for amending existing business associate agreements. This additional period is available only for an existing business associate agreement meeting the following conditions:

- was in place prior to January 25, 2013 and complies with current HIPAA business associate agreement requirements; and
- is not modified or renewed during the period from March 26, 2013 to September 23, 2013.

Business associate agreements not eligible for the extended transition period must be compliant with the Final Rule as of the September 23, 2013 compliance date.

HHS recently issued guidance on the revised business associate agreement requirements and provided sample terms. This guidance is available at:

http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html

---

7 78 Fed. Reg. at 5597.

© National Hospice and Palliative Care Organization, 2013
New Fundraising Requirements\textsuperscript{8}

The Final Rule expands the type of information covered entities may use to target fundraising appeals to include the department of service, the treating physician and outcome information. This is a significant expansion of the current HIPAA rules which permit the use only of demographic information and dates of health care provided to the patient. Fundraising communications must provide recipients with a clear and conspicuous opportunity to opt-out and the method provided for the opt-out may not cause undue burden or more than nominal costs.

New Limitations on the Protection Afforded Decedents Information\textsuperscript{9}

The protections afforded individuals’ PHI under the Privacy Rule will no longer apply to the PHI of individuals who have been deceased for more than 50 years. A covered entity only has an obligation to comply with the requirements of the Privacy Rule with respect to the PHI of a deceased individual for 50 years following the individual’s death.

The Final Rule also permits covered entities to disclose PHI to a family member or other individual involved in a decedent’s care or payment for such care, unless such a disclosure is inconsistent with a prior expressed preference of the decedent.

New Enforcement Authority\textsuperscript{10}

HHS is required by the HITECH statute to move toward a penalty-based system and away from the voluntary compliance framework used in the past. The Final Rule provides that:

- Civil and criminal penalties can now be applied directly to business associates.
- HHS must investigate any complaint and conduct compliance reviews in all cases where a preliminary review of the facts indicates a possible violation due to willful neglect.
- HHS must impose a civil money penalty for violations due to willful neglect.
- HHS is not required to attempt to resolve cases of noncompliance due to willful neglect by informal means.
- The tiered penalty structure based on different levels of culpability has been finalized. Penalties now range from $100 to $50,000 per violation depending on the level of knowledge/willfulness with a US$1.5 million cap per calendar year for multiple violations of identical provisions.
- Covered entities and business associates can be subject to liability for a violation by their business associate agents and subcontractor business associate agents respectively. Detailed guidance for determining when an entity is an agent is provided in the Final Rule.
- HHS may disclose PHI obtained in connection with a compliance review or investigation if permitted under the Privacy Act, thereby giving it the ability to share information with other law enforcement agencies (e.g., state attorneys general or the Federal Trade Commission).

These modifications to the Enforcement Rule are effective as of March 26, 2013.

\textsuperscript{8} 78 Fed. Reg. at 5618.
\textsuperscript{9} 78 Fed. Reg. at 5613.
\textsuperscript{10} 78 Fed. Reg. at 5577.
Other Important Changes

- **Expansion of Prohibited Marketing Activities**. HIPAA prohibits the use or disclosure of PHI for marketing to individuals without obtaining an authorization, with certain important exceptions. The Final Rule further narrows the permissible exceptions by requiring individual authorization for all treatment and health care operations communications for which financial remuneration (i.e., direct or indirect payment) is received in exchange for the communication from a third party whose services are being promoted. For example, under the Final Rule an authorization would be required before a covered entity health care provider could send a communication (using its patient list) to its patients about a new, beneficial drug, where the communication was sponsored by the pharmaceutical manufacturer and the manufacturer provided money to the provider in exchange for sending the communication.

- **Prohibition on the Sale of PHI**. The Final Rule prohibits the receipt of direct or indirect remuneration (including in-kind benefits) in exchange for PHI. This new restriction includes several exceptions, including disclosures to business associates, as required by law, and for treatment and payment purposes.

- **New Research Authorizations Permitted**. The Final Rule now allows researchers to obtain authorizations to use PHI for future research, provided that the future research is adequately described. In addition, covered entities are now permitted to combine conditioned and unconditioned authorizations for research (e.g., authorization for research activities where treatment is conditioned on signing the authorization and activities where treatment is not conditioned on signing the authorization), provided that the authorization meets certain specified conditions.

NHPCO has engaged Hogan Lovells as counsel in preparing information on HIPAA. Hogan Lovells lawyers are assisting their clients implement the privacy and security requirements of HITECH. We have extensive experience advising on HIPAA, consumer protection, and international data privacy and security requirements and compliance programs. If you would like additional information on the HITECH requirements, need assistance developing, or implementing privacy or data protection programs, or require support in preparing for or managing a data breach, please contact the Hogan Lovells lawyer with whom you work, or any of the contacts listed below.

**Brooke Bumpers**
Counsel, Washington, D.C.
brooke.bumpers@hoganlovells.com
+1 202 637 5800

**Nadine Peters**
Partner, Washington, D.C.
nadine.peters@hoganlovells.com
+1 202 637 6572

---