The Wait is Over: The HIPAA Final Rule Has Arrived

Significant Changes That Will Impact Providers and Practical Tips to Stay on Track

Erin Fleming Dunlap / Rebecca L. Frigy

Those of us who work in the world of HIPAA (the Health Insurance Portability and Accountability Act of 1996) anxiously awaited the arrival of the HIPAA Final Omnibus Rule for months —actually, years. Finally, the final rule was published on January 25, 2013, causing a shift in the HIPAA landscape overnight and creating a concern among health care providers as to "What do I need to do now?" Many of the changes were expected; others were not. In this article, we highlight the significant changes impacting health care providers and offer some practical tips to help providers stay on track — and in compliance with the final rule.

For purposes of reassurance but also as words of caution, the compliance date for most of the changes to HIPAA made by the final rule is September 23, 2013. This means that health care providers have plenty of time to understand what is required by the final rule and to adjust their operations or get appropriate processes and procedures in place prior to the compliance date. This does not mean, however, that health care providers can and should put off thinking about compliance with the final rule until September because, as discussed below, many of the changes will require a careful review of, and most likely revisions to, a number of forms and documents (including policies and procedures). Changes to the final rule where the compliance date is not September 23, 2013, are specifically noted within this article.

Erin Fleming Dunlap is counsel at Polsinelli PC. She can be reached at edunlap@polsinelli.com.

Rebecca L. Frigy is an associate at Polsinelli PC. She can be reached at rfrigy@polsinelli.com.

An Impermissible Use or Disclosure of Protected Health Information is Now Presumed to be a Breach

Among the most notable changes, the final rule reshaped how health care providers will determine their breach notification obligations in the future. Resulting from the

last round of changes to HIPAA in 2009 (under an interim final rule resulting from the Health Information Technology for Economic and Clinical Health (HITECH) Act), if a health care provider was faced with an unauthorized use or disclosure of protected health information (PHI) (a defined term under HIPAA), the provider could evaluate whether there was a risk of harm to the individual subject of the PHI in determining whether or not there was a "breach" — which then would trigger mandatory notification requirements by the health care provider to the affected individual, the Secretary of the U.S. Department of Health and Human Services (HHS), and the media, if applicable. However, HHS became concerned that the "risk of harm standard" was too subjective and set a much higher threshold for notification than it intended to set. Thus, in the final rule, the "risk of harm standard" was removed, and a more objective test was added.

Under the final rule, any unauthorized use or disclosure of PHI that does not meet one of the exceptions, as described below, is presumed to be a "breach" unless the provider can demonstrate (through a written risk assessment) that there is a "low probability that the PHI has been compromised." The four factors that must be considered include: (1) the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification; (2) the unauthorized person who used the PHI or to whom the disclosure was made; (3) whether the PHI was actually acquired or viewed; and (4) the extent to which the risk to the PHI has been mitigated. A provider may consider other factors (as appropriate), but the risk assessment must be documented, thorough, completed in good faith, and the conclusions reached must be reasonable.

Under the final rule, the following types of uses or disclosures continue to be excepted from the definition of "breach" and the breach notification requirements:

- any unintentional acquisition, access, or use of PHI by a workforce member or individual acting under the authority of a covered entity or a business associate if such access or use was made in good faith and within the scope of authority and does not result in a further unauthorized use or disclosure;
- any inadvertent disclosure by a person who is authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the same covered entity or business associate, and the information is not further used or disclosed in an impermissible manner; and
- a disclosure of PHI where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

What does this mean for health care providers? Because a "breach" is presumed to have occurred, notification will be required in more cases — particularly those cases that would fall into a gray area because the likelihood of harm resulting from the impermissible use or disclosure is low. In response to these changes, health care providers should (i) evaluate whether or not encryption is feasible for the PHI they maintain (if PHI is encrypted, then there are no breach notification requirements following an impermissible use or disclosure); (ii) implement or revise their current policies and procedures to ensure that when workforce members are evaluating the risk of an impermissible use or disclosure, they consider all of the factors set forth above and other factors if necessary; and (iii) train and educate workforce members and other agents on the importance of prompt reporting of potential impermissible uses or disclosures of PHI.

Providers Will Need to Review and Update Their Business Associate Agreements (Yet Again)

In response to the changes made by the HITECH Act and the interim final breach notification rule in 2009, many health care

providers amended and required their business associates (BAs) to re-execute business associate agreements (BAAs). Even though such amendments were made in response to the HITECH Act, as a result of the changes made by the final rule, health care providers will need to revisit and review their BAAs for compliance with the final rule and will likely have to go through the amendment and re-execution process again.

The final rule requires that the following elements be included in a BAA:

- The BA must comply with Subpart C, of Part 164 of the HIPAA security rule.
- The BA must report breaches of unsecured protected health information to covered entities.
- The BA must obtain satisfactory assurances (in the form of a written BAA) from any subcontractor that creates or receives protected health information on behalf of the BA that the subcontractor agrees to the same restrictions and conditions that apply to the BA with respect to such information.
- To the extent the BA is delegated to carry out a covered entity's obligations under the HIPAA privacy rule (*e.g.*, responding to accounting of disclosures or providing an individual with a notice of privacy practices), the BA must comply with the requirements of the HIPAA privacy rule that apply to the covered entity in the performance of such delegated obligations.

In addition to these required elements, health care providers should consider including details related to breach notification (*e.g.*, the time period to report, to whom the breach should be reported, and in what manner), details regarding responding to requests for PHI, amendments, and accounting of disclosures and indemnification clauses. Health care providers also may want to consider including a provision in their BAAs which clarifies that the BA is providing services as an independent contractor rather than an agent; this is important as HHS clarified in the final rule that while BAs will now be directly liable for their noncompliance with the BAA and certain provisions of the privacy and security rules, covered entities will be responsible for and may still be held liable for a BA's actions if the BA is an agent (*i.e.*, if the covered entity has direct control over the BA's actions and how the BA renders services on behalf of the covered entity).

The final rule does offer a bit of help from a time perspective for health care providers that went through the HITECH Act BAA update process but still need to make additional amendments as a result of the final rule. For those providers, and related only to BAAs in place prior to January 25, 2013, if such BAAs are not renewed or modified between March 26, 2013, and September 23, 2013, they will be "grandfathered," and the health care provider will have up to an extra year to make the required amendments (*i.e.*, by September 22, 2014).

This same "extension" does not apply to "new" BAAs which were and are entered into post-January 25, 2013. Such "new" BAAs must contain the elements required by the final rule by September 23, 2013. This creates a contract management nightmare for health care providers, and many providers may choose to address the issue by merely going through the entire amendment and re-execution process again prior to September 23, 2013, regardless of when their BAAs were executed. From a practical perspective, health care providers also should consider including the required final rule elements in all BAAs entered into between now and September 23, 2013.

Related to updating BAAs to comply with the final rule, the final rule also made some clarifications and additions to those types of entities that meet the HIPAA definition of a "business associate." For instance, health information organizations, e-prescription gateways, data transmission services that require routine access to PHI, and entities that maintain PHI but do not actually view the PHI or only do so on a random or infrequent basis, such as storage companies or cloud-computing companies, are now explicitly included in the HIPAA definition of a BA. While health care providers are reviewing and inventorying the BAAs they have entered into, it is also

suggested that health care providers examine all relationships that they have with third parties in order to identify *all* BA relationships and to get an executed BAA in place.

Patients Have the Right to Receive an Electronic Copy of Their Medical Record

Patients currently have the right to review or obtain copies of their protected health information (a defined term under HIPAA) to the extent such information is maintained in a designated record set (*e.g.*, a patient's medical and billing records). Under the final rule, a health care provider will be required to give a patient, upon the patient's request, an electronic copy of PHI that is maintained electronically in a designated record set. For health care providers this means that if a provider maintains its medical records electronically, the provider must be able to provide a patient with his or her records on a disc or via secure email formatted as a PDF or Word file, or through a secure Web-based portal.

Times have changed, and so has technology. HHS expects providers to make it easy for patients to access their health information and to give patients a copy of their health information in a readable electronic form or format within 30 days of the patient's request (or within 60 days if the provider gives the patient proper notice of its need for an extension). A provider can charge the patient a "reasonable, cost-based fee" to provide the electronic copy of the PHI. This fee may include (i) technical staff time spent creating and copying the electronic file, such as compiling, extracting, scanning, and burning PHI to media; (ii) the cost of supplies for creating electronic media (*e.g.*, discs, flash drives, et cetera); and (iii) the cost of postage if the patient requests that the portable media be sent by mail or courier. Please note, however, that charging the patient a "handling" fee for a copy of his or her records is still not permitted, and health care providers still must comply with relevant state law requirements related to charging patients for copies of their medical records — regardless of whether the copy is provided in paper or electronic form. Providers should consider how they will handle these requests, implement appropriate policies and procedures, and train workforce members on this new requirement.

Providers Must Abide By a Patient's Request to Restrict Disclosures To a Health Plan

Under the final rule, if a patient asks a health care provider to restrict the disclosures of his or her PHI to a health plan made for payment and health care operations purposes and the PHI pertains solely to a health care item or service for which the patient (or someone acting on the patient's behalf) has paid the provider in full, the health care provider *must* agree to the restriction. While a provider is not required to create a separate medical record or otherwise segregate PHI subject to such a restriction, a provider will need to flag or use some other method to identify portions of the record that contain PHI subject to the restriction in order to ensure it is not inadvertently sent or made accessible to the health plan for payment or health care operations purposes (*e.g.*, during audits by the health plan).

In order to comply with this new requirement, providers must determine how they are going to "flag" data subject to this type of restriction and then implement the protocol by September 23, 2013. A provider also must include a statement about this new right (and other new rights) in its NPP, which means that as a result of the final rule, health care providers also will need to review and revise their NPPs.

An Authorization is Required Before Providers Can Send Marketing Communications if the Provider is Paid for Making the Communication

Under the final rule, if a health care provider receives financial remuneration from a third party in exchange for using PHI to make a communication about a health-related product or service, the communication is considered "marketing," and the provider must

obtain a patient's HIPAA-compliant authorization prior to actually making the communication. Further, the authorization must include an acknowledgment that the provider is receiving financial remuneration from a third party for making the communication.

Previously, if such a communication were made for treatment or health care operations activities, such communications were excluded from the definition of "marketing." But, under the final rule, that is no longer the case. Providers are still allowed to use PHI to make a communication about a health-related product or service (and to be paid for it) if the communication is made face-to face or the communication consists of a promotional gift of nominal value provided by the health care provider. Providers are also permitted to send refill reminders or other communications about a drug or biologic that is currently prescribed to the patient, but the health care provider may only be paid for the actual cost of making the communication (*e.g.*, costs for labor, supplies, and postage).

Communications promoting health in general that do not promote a product or service from a particular provider are also acceptable. This means that health care providers must be very careful before using PHI for marketing purposes — especially if the provider is being paid by a third-party. Current agreements or business arrangements need to be reviewed and may need to be restructured (*i.e.*, patient authorizations may need to be obtained) or the arrangement terminated prior to September 23, 2013.

Patients Must Be Provided the Opportunity to Opt-Out of Receiving Fundraising Communications

Under the final rule, a health care provider can use a patient's PHI for purposes of making a communication about raising funds for the provider; however, the patient receiving the fundraising communication (in writing or over the phone) must be provided with a clear and conspicuous opportunity to opt-out of receiving any further fundraising communications. If the patient opts-out of receiving future fundraising communications, the provider must treat the patient's choice to opt-out as a revocation of the patient's authorization to use his or her PHI for fundraising communications. This requirement only applies if a patient's PHI is used to make the communication (*e.g.*, a provider may use a public directory to mail communications to all residents in a particular geography and would not be required to provide the patient with an opt-out).

The provider is given flexibility in determining the process for patients to opt-out of receiving fundraising communications, but the method cannot cause a patient to incur undue burden or more than nominal cost. HHS has clarified that requiring a patient to write a letter to the provider in order to opt-out imposes an undue burden on the patient; however, asking a patient to call a toll-free phone number, send an email to a specific email address, or mail a pre-printed, pre-paid postcard to the provider does not. In short, if a provider wants to use PHI to send fundraising communications to its patients, it must have a system in place to "flag" patients who have exercised their right to opt-out of receiving fundraising communications to ensure that such patients are not sent future communications.

Further, the final rule requires a health care provider to include a specific statement in its NPP that it intends to contact the patient to raise funds and that the patient has the right to opt-out of receiving such communications.

Providers Cannot Sell PHI without an Authorization, Unless an Exception Applies

Under the final rule, a health care provider cannot receive direct or indirect remuneration in exchange for the disclosure of PHI unless a HIPAA-compliant authorization is obtained from the patient and the authorization states that the provider is receiving direct or indirect remuneration in exchange for the PHI, or a relevant exception otherwise applies. HHS made clear in the final rule, however, that the remuneration must be directly for the PHI (or access thereto) and not related to a service involving access to the PHI. For

instance, the fees paid by a provider to participate in a health information exchange (HIE) is for the services provided by the HIE and not for the PHI itself.

There are a handful of exceptions to the prohibition on the sale of PHI, including if the sale of PHI is for (i) public activities; (ii) the treatment of the patient or payment; (iii) the sale, transfer, merger, or consolidation of all or part of the provider; (iv) research (if the remuneration is cost-based); or (v) as required by law. Again, a health care provider should be careful (and confirm an exception applies) before it accepts any remuneration for the disclosure of PHI. Health care providers also should ensure that their NPPs include a statement that disclosures that constitute a sale of PHI require a patient's authorization and will be made only in accordance with the patient's authorization.

Providers are Permitted to Disclose Decedent's PHI to Family Members and Immunization Records to Schools

The final rule did include a few changes that make things easier on health care providers. First, pursuant to the final rule a health care provider may disclose a decedent's PHI to family members and others who were involved in the decedent's care, unless doing so would be inconsistent with any prior expressed wishes or preferences of the decedent.

Second, pursuant to the final rule, a health care provider may disclose proof of immunizations to schools in states that require the school to have such information prior to admitting a student. While written authorization for the disclosure is not required, providers are encouraged to obtain written or oral agreement from a parent, guardian, or other person acting in *loco parentis* for the minor patient, or from the patient himself or herself, if the patient is an adult or emancipated minor. These changes should be incorporated into a provider's policies and procedures so workforce members know how to handle these types of requests.

Summary

In conclusion, the final rule is here. It is prudent for health care providers to understand their obligations under the final rule and to take all necessary steps to ensure their compliance with the final rule by the applicable compliance dates. While it may seem there is plenty of time to takes steps toward compliance, it is never too early to get started reviewing internal forms, policies, and processes and to make all necessary changes to comport with the final rule. We waited a long time for the final rule to make its appearance — but the date to comply with most of the provisions (September 23, 2013) will be here before you know it!