For just over a year now, covered entities and business associates have been digesting, implementing, and living with the myriad new and revised requirements of the HIPAA/HITECH Omnibus Rule (“Omnibus Rule”).¹ Compliance enforcement with most of the Omnibus Rule provisions began on September 23, 2013. This outline and the accompanying paper by Marilyn Lamar address some of the ongoing practical challenges and questions associated with Omnibus Rule compliance, including conundrums arising from preparing and negotiating business associate agreements, evaluating breach notification obligations in integrated systems and health information exchange organizations (“HIEs”), operationalizing patients’ restrictions on disclosures of protected health information (“PHI”) to their health plans where such patients have paid out-of-pocket for the service, sharing of PHI containing substance abuse information, and assessing the impact of health information technology and the use of electronic health records (“EHRs”) upon safety.

I. BREACH NOTIFICATION IN A CONNECTED UNIVERSE

The Health Information for Economic and Clinical Health (“HITECH”) Act² for the first time required covered entities to provide written notification to the Secretary of the Department of Health and Human Services (“HHS”), to affected individuals, and in some cases to the media, after the discovery of a breach of unsecured PHI. Where a business associate was responsible for a breach, the business associate was required to notify the covered entity of the breach. On August 24, 2009, HHS published an interim final rule (“IFR”) clarifying the specific requirements for breach notification by covered entities and business associates.³ These regulations became effective on September 23, 2009.

A. Interim Final Rule

The IFR defined the term “breach” as “the acquisition, access, use, or disclosure” of PHI, in a manner not permitted by the HIPAA privacy rule, which “compromises” the security or

¹ 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 Rule; Final Rule, 78 Fed. Reg. 5566 (Jan. 25, 2013).


privacy of the PHI.\(^4\) “Compromises the security or privacy” of the PHI was defined to mean “poses a significant risk of financial, reputational, or other harm to the individual.”\(^5\)

The IFR included three narrow exceptions to the definition of “breach.” A “breach” did not include:

1. An unintentional acquisition, access, or use of PHI by a member of the work force or an agent of the covered entity or business associate, if the acquisition, access, or use was made in good faith, within the scope of authority, and did not result in a further impermissible use or disclosure;\(^6\)

2. An inadvertent disclosure by a person authorized to access PHI at a covered entity or business associate to another authorized person at the same covered entity or business associate or organized health care arrangement, if the PHI received was not further used or disclosed impermissibly; or

3. A disclosure of PHI where the covered entity or business associate believed in good faith that the unauthorized person to whom the PHI was disclosed would not reasonably have been able to retain the information.\(^7\)

In addition to the above-noted exceptions, a use or disclosure of a limited data set\(^8\) that also excluded dates of birth and ZIP codes was not considered to be a breach of PHI because the use or disclosure of this limited information was not deemed to compromise the security or privacy of the PHI.\(^9\) If, however, a limited data set that still contained date of birth and ZIP code was impermissibly accessed, acquired, used, or disclosed, then the IFR proposed that a covered

\(^4\) 45 C.F.R. § 164.402.
\(^5\) Id.
\(^6\) Id. The IFR offered, as an example of this exception, a billing employee who receives and opens an e-mail containing PHI about a patient which a nurse mistakenly sent to the billing employee. Once the billing employee notices that he is not the intended recipient of the e-mail, he alerts the nurse of the misdirected e-mail and then deletes the message. See 74 Fed. Reg. at 42747.
\(^7\) 45 C.F.R. § 164.402. The IFR offered, as an example of this exception, a covered entity that sends several EOBs to the wrong individuals. A few of the EOBs are returned by the post office, unopened, as undeliverable, but several of the EOBs which the covered entity knew were misaddressed were not returned. Under these circumstances, the covered entity may conclude that the EOBs that were returned could not reasonably have been retained by the addressees; however, the covered entity may not reach that conclusion with respect to those EOBs that were not returned as undeliverable. See 45 Fed. Reg. at 42748.
\(^8\) A “limited data set” is created by removing sixteen (16) direct identifiers, set forth in 45 C.F.R. § 164.514(e)(2), from PHI. Even with these identifiers removed from the PHI, however, a limited data set is not completely de-identified, because the elements of dates (including birth dates) and ZIP codes increase the possibility that the information may be re-identified; accordingly, the HIPAA privacy rule treats limited data sets as PHI.
\(^9\) 45 C.F.R. § 164.402, definition of “breach.”
entity or business associate would be required to perform a risk assessment to determine whether
the risk of re-identification of the information posed a significant risk of harm to the individual.10

As indicated above, the IFR specified that not every impermissible acquisition, access, use or disclosure of PHI constituted a “breach” for which notification must be made. However, in circumstances where a covered entity or business associate determined that an impermissible acquisition, access, use or disclosure of PHI did occur, the covered entity or business associate then must conduct a fact-specific risk assessment to determine whether the impermissible acquisition, access, use or disclosure of PHI posed a significant risk of financial, reputational, or other harm to the individual.

In performing the risk assessment, covered entities and business associates were required to consider the following types of factors:

- Who impermissibly used the PHI, or to whom was the PHI impermissibly disclosed?
- In what form was the PHI accessed used, or disclosed?
- Was the impermissible access, use, or disclosure of PHI intentional?
- What steps, if any, were taken to mitigate the potential harm of the impermissible access, use, or disclosure?
- What type of PHI was impermissibly accessed, used, or disclosed?

If, following the risk assessment, a significant risk of harm was determined to exist, then notification of the breach was required to be made. If the risk assessment resulted in a determination that no significant risk of harm existed, then the investigation could be concluded without breach notification.

Significantly, the covered entity or business associate had the burden of demonstrating that it made all breach notifications required by the HITECH Act or that the acquisition, access, use or disclosure did not constitute a breach.11 Accordingly, covered entities and business associates were required to carefully document and maintain their risk assessment processes so that they could later demonstrate, if necessary, that no breach notification was required following a given impermissible acquisition, access, use, or disclosure of PHI.12

10 See 74 Fed. Reg. at 42746.
11 45 C.F.R. § 164.414(b).
12 A covered entity or business associate is required to maintain documentation sufficient to meet its burden of proof for a period of six years. 45 C.F.R. § 164.530(j)(2).
B. Omnibus Rule

The Omnibus Rule was issued nearly three and a half years after the IFR was published, and many in the industry speculated that the lengthy delay was due (at least in part) to a reconsideration of the harm standard. Such speculation appears to have been accurate. In the preamble to the Omnibus Rule, HHS noted that 60 of the 70 commenters who specifically addressed the IFR’s definition of “breach” supported the proposed risk of harm standard and risk assessment approach. These commenters believed that this approach enabled the appropriate parties—covered entities and business associates—to assess the likely impact of impermissible uses or disclosures of PHI and then to strike a proper balance between enabling individuals to protect themselves from likely negative consequences of a breach without unnecessarily flooding individuals with notifications about inconsequential events.\(^\text{13}\) Other commenters, however, suggested that the subjective risk of harm standard gave too much discretion to covered entities and business associates and appeared to set a higher threshold for breach notification than the HITECH Act or HHS intended.\(^\text{14}\)

1. Definition of “Breach” and Risk Assessment Approach

HHS agreed with this smaller group of commenters. In the Omnibus Rule, it revised the definition of “breach” and the risk assessment approach to create what HHS described as a “more objective standard.”\(^\text{15}\) Now, an impermissible acquisition, access, use or disclosure of PHI is presumed to be a breach, and notification is required, unless either the disclosing covered entity or business associate demonstrate that there is a low probability that the PHI was “compromised” or one of the other exceptions to the definition of breach applies.\(^\text{16}\) Thus, the risk assessment now focuses on the potential “harm” to the data rather than the potential risk of harm to the individual. The covered entity or business associate retains the burden of proving that there was not a breach, but the burden of proof now requires overcoming a presumption of breach.

The overall probability of compromise\(^\text{17}\) to PHI must be determined based upon a risk assessment of at least the following factors:

- The nature and extent of the PHI involved, including the types of identifiers and the likelihood that the information may be re-identified;
- The unauthorized person who impermissibly used the PHI or to whom the PHI was impermissibly disclosed;

\(^{13}\) See 78 Fed. Reg. at 5640.

\(^{14}\) 78 Fed. Reg. at 5641.

\(^{15}\) Id. at 5566.

\(^{16}\) Id. at 5641.

\(^{17}\) The Omnibus Rule eliminated the definition of “compromise,” which arguably leaves some uncertainty as to the final conclusion derived from the risk assessment factors.
• Whether the PHI was actually accessed or viewed; and

• The extent to which the risk to the information has been mitigated.\(^{18}\)

If a thorough, good-faith assessment of these and perhaps other factors “in combination” fails to demonstrate that there is a low probability that the PHI was compromised, then breach notification is required.\(^{19}\)

In further discussing these factors, the Omnibus Rule provided numerous examples suggesting that a finding of a low probability that the data was compromised will be the exception rather than the rule. For example, if a covered entity mails information to the wrong individual, who opens the envelope and then contacts the entity to advise that she received the information in error, the unauthorized recipient viewed and acquired the information. Accordingly, HHS suggested that the covered entity’s consideration of the third factor should weigh in favor of notification.\(^{20}\) HHS also indicated that the identity of the recipient of the PHI may affect “whether the covered entity can conclude that an impermissible use or disclosure has been appropriately mitigated.”\(^{21}\) For example, a covered entity may be able to rely on an assertion by another covered entity or business associate employee that the entity or person destroyed a misdirected communication containing PHI, whereas that type of assurance from some other third parties may result in a finding that the risk to PHI was not sufficiently mitigated.\(^{22}\)

The revised standard effectively removes the fairly broad discretion that covered entities and business associates had under the risk of harm standard to determine whether to make notification of breaches. This appears to have been HHS’s intent, as it agreed with commenters who suggested that the risk of harm standard “would lead to inconsistent interpretations and results across covered entities and business associates.”\(^{23}\)

2. Exceptions to Breach and Implications of Revised Approach

The Omnibus Rule maintained the three narrow exceptions proposed in the IFR, but it eliminated the IFR exception for impermissible uses or disclosure of limited data sets which also exclude dates of birth and ZIP codes; instead, entities now will have to perform a risk assessment to determine whether breach notification is required.\(^{24}\) HHS

\(^{18}\) 78 Fed. Reg. at 5642.

\(^{19}\) Id. at 5643.

\(^{20}\) See 78 Fed. Reg. at 5643.

\(^{21}\) 78 Fed. Reg. at 5643.

\(^{22}\) Id.

\(^{23}\) Id. at 5642.

\(^{24}\) Id. at 5643.
also clarified that violations of the minimum necessary standard are subject to the risk assessment requirement outlined above.\textsuperscript{25} HHS acknowledged that risk assessments surrounding both of these types of privacy violations frequently may result in determinations that breach notification is not required.\textsuperscript{26} Nonetheless, HHS’s commentary on the new risk assessment standard plainly illustrates its expectation that covered entities and business associates devote significantly more time and thought to performing risk assessments, and evaluate a wider variety of potential breach scenarios, than these entities may have done pursuant to the IFR’s risk assessment process.

Somewhat ominously, HHS noted in the preamble that covered entities and business associates may skip the risk assessment if they decide to proceed directly to breach notification.\textsuperscript{27} In other words, the risk assessment is necessary only if the covered entity or business associate seeks to try to avoid providing notification. Because the presumption now is that a breach has occurred following each and every impermissible use or disclosure of PHI, entities may determine to proceed with notifications instead of spending the time and resources to perform a risk assessment.

HHS indicated that it will issue specific guidance to assist covered entities and business associates in performing risk assessments in certain frequently-occurring scenarios.\textsuperscript{28} As of the date this outline was submitted however, such guidance had not yet been received.

C. \textbf{Practical and Operational Considerations}

Without the benefit of additional guidance from HHS following publication of the Omnibus Rule, covered entities and business associates have been struggling to determine how to revise their policies, and how to evaluate impermissible uses and disclosures of PHI under HIPAA, to comply with the new breach notification standard. Given the Omnibus Rule’s revisions to the definition of “business associate,” its clarifications about who is an agent and about covered entity and business associate liability for the acts of agents, and its adoption of the IFR’s more stringent enforcement provisions, determining whether or not to make notification following an impermissible use or disclosure of PHI has become a high-stress proposition. Specific examples of potential breaches and possible resolutions will be addressed during the presentation, but the discussion below outlines some considerations for the investigation and risk assessment processes and notes some of the special issues that arise in integrated health systems with common EHR platforms and in HIEs.

\textsuperscript{25} \textit{Id}.

\textsuperscript{26} \textit{See} 78 Fed. Reg. at 5644.

\textsuperscript{27} \textit{See id}. at 5643.

\textsuperscript{28} 78 Fed. Reg. at 5643.
1. **Investigate, Evaluate, and Notify of Breaches Within the Required Time Frame**

Because of the substantially increased penalties for HIPAA violations, all covered entities and business associates should be familiar with the required timeframe within which breaches must be investigated and evaluated and, if necessary, notifications made. Not only should entities remember that 60 days following discovery of a breach is the outside limit within which the covered entity (or business associate, if requested by the covered entity) is required to make notifications, but they should very carefully consider which, if any, of their business associate arrangements give rise to an agency relationship. For any arrangements that likely involve business associate agents, covered entities and business associates alike should require more limited breach notification timeframes within their business associate agreements (“BAAs”), and they also should ensure that they have policies and processes in place that enable them to complete their own investigation and notification processes within the required time period. Applicable state breach notification laws may further limit the reporting period and impose additional requirements, so covered entities and business associates must be aware of such requirements in states in which they do business.

2. **Decide Whether to Notify Without Performing a Risk Assessment Under Certain Circumstances**

Covered entities and business associates also should determine whether there are certain types or categories of situations involving impermissible uses or disclosures of PHI that will result in the entity’s proceeding directly to breach notification without first spending the time and effort to engage in a thorough risk assessment. For example, intentional disclosures of an individual’s information by an employee to an unauthorized third party might almost always be determined to pose more than a low probability of compromise to the information, as might impermissible uses or disclosures of Social Security numbers or of communicable disease, alcohol and drug abuse treatment, or other “sensitive” clinical information. Creating, maintaining, and updating from time to time a list of such circumstances ultimately may allow entities to save precious time, staff, and financial resources. Although this suggestion may sound counterintuitive, there is little doubt that the number of reported breaches will increase substantially as a result of the Omnibus Rule’s revised approach. While many patients will be unhappy upon learning that their information has been compromised, they will be less unhappy than if their medical identity or retirement savings had been stolen based upon a breach incident that was not reported. Moreover, the increasing incidence and reporting of breaches over time likely will have some desensitization effect, and the circumstances of each breach and the responsible entity’s handling of the breach can impact affected individuals’ responses to learning of a breach.

3. **Focus on Mitigation and Response**

Even where a covered entity or business associate determines that the four risk assessment factors in combination pose more than a low probability that the affected PHI has been compromised, efforts taken to mitigate any risk, along with other applicable
factors, may serve to lessen the probability that PHI was compromised to a low probability. For example, if a tablet containing PHI on it is lost but the entity is able to remotely wipe the device, or if the device is encrypted but the encryption technology does not meet NIST standards, depending upon all relevant factors, the entity may be able to determine that there is a low probability of compromise to the data. Notwithstanding HHS’s example in the Omnibus Rule preamble—that an individual who receives the wrong patient’s information by mail or fax, opens the envelope or reviews the fax, and then contacts the entity to advise that she received the information in error, viewed and acquired the information—other factors, such as the covered entity obtaining a certificate of destruction signed by the recipient, may permit the entity to determine that there is a low probability of compromise in a given instance. Alternatively, a written assurance that an impermissible use or disclosure was very limited—for example, to another member of a group therapy class—may result in a similar determination. As noted in the preamble, covered entities and business associates should consider all of the required and any additional relevant factors, if and as applicable, and make a reasonable and good faith determination about the overall probability that the PHI has been compromised.

4. What Constitutes a Breach in a Health System Using a Single EHR Platform or in an HIE?

In an integrated health system where many or all of the provider entities share a common EHR platform, there can be a temptation to assume that any use or disclosure of PHI “within” the system does not result in a breach of unsecured PHI. This is a dangerous assumption. For purposes of determining whether a breach has occurred, uses and disclosures of PHI among entities in an EHR-connected network of provider entities generally are no different than uses or disclosures of PHI within a single entity or between unrelated covered entities. Integrated health care systems may function as an organized health care arrangement (“OHCA”) or have designated themselves as an affiliated covered entity (“ACE”); in either case, their common enterprise (OHCA) or joint ownership or control (ACE) permits them to use a joint Notice of Privacy Practices (“NPP”) and share PHI among the entities for purposes of treatment, payment, and health care operations. However, such systems still must abide by the minimum necessary standard (except for uses or disclosures of PHI for treatment purposes). Additionally, if an ACE combines the functions of a health care provider with those of a health plan and/or those of a health care clearinghouse, the ACE must comply with the standards applicable to each type of entity, and a single entity within an ACE that performs multiple covered functions must restrict its uses and disclosures of an individual’s PHI to those purposes related to the covered function being performed for that individual.

Whether acting as an OHCA or an ACE, an integrated system must maintain and enforce appropriate policies and procedures on role-based access to electronic PHI in the system, and all entities within the system must comply with the minimum necessary standard when using or disclosing PHI for purposes of payment or health care operations. Because violations of the minimum necessary standard are violations of HIPAA, any improper access or disclosure to PHI through an integrated system—just like improper access or disclosure within a single covered entity—now must be reviewed to determine whether the improper access or disclosure created more than a low probability that the
PHI was compromised. Because such uses or disclosures among covered entities are by definition made or received by persons or entities who have an obligation to safeguard the PHI, in many instances the entities involved may determine that breach notification is not required. Nonetheless, because integrated health systems typically have hundreds and in some cases many thousands of users who can electronically access, use and disclose PHI, such systems must pay particular attention to HIPAA security controls and implement robust privacy policies that minimize the likelihood of such PHI being improperly used or disclosed, whether within or outside of the health system entities.

HIEs can be compared to health systems, as both are comprised of multiple covered entities; a significant distinction, however, is that the entities participating in an HIE often are not under joint ownership or control. Rather, they are often competitors who nonetheless desire to securely exchange PHI of common patients for purposes of treatment and, in some cases, payment and other approved reasons. Generally speaking, improper uses or disclosures of PHI among participants in an HIE should be evaluated as any improper use or disclosure of PHI among separate covered entities would be, and breach notifications under HIPAA must be made where appropriate. State breach notification laws add a layer of complexity to the assessment, especially for HIEs that operate in multiple states.

Having said this, participants in HIEs sometimes confuse HIPAA breach notification requirements with the HIE’s internal breach notification requirements, particularly in cases in which a state or federal government entity is operating or facilitating the HIE. The eHealth Exchange (formerly the Nationwide Health Information Network) and several statewide HIEs require participants in the HIE to make notifications of information breaches over the network to a governing board or other designee of the HIE entity within as little as one hour for suspected breaches and 24 hours for confirmed breaches. It is important to distinguish these HIE breach notification requirements—which arise through contract and serve to alert other participating covered entities whose patients’ PHI may have been compromised as a result of the improper use or disclosure over the network so that such entities may decide whether to temporarily suspend their participation in the HIE—from the HIPAA breach notification requirements (which are memorialized in statute and regulations) to individuals, the Secretary of HHS, and in some cases the media. Each type of notification is important, and entities must comply with the applicable notification time frames in each situation, but as noted above the notifications have distinct purposes.

II. INDIVIDUALS’ RIGHT TO REQUEST RESTRICTIONS ON USES AND DISCLOSURES OF PHI

The provisions of the Omnibus Rule that may have created the greatest concern among health information managers and compliance officers were the revisions strengthening patients’ rights to restrict PHI from their health plans about items or services for which they pay out-of-pocket and in full.
A. The Privacy Rule

Under the Privacy Rule, covered entities may allow individuals to request restrictions on uses or disclosures of their PHI, including for purposes of treatment, payment, and health care operations, as well as restrictions on disclosures of PHI to family members and certain others involved in the individual’s care. Although covered entities are not required to agree to such requests (and typically do not do so), if a covered entity agrees to a restriction, it must document the restriction in writing and abide by the restriction, except in emergency circumstances when the information is required for treatment of the individual. A covered entity may terminate its agreement to a restriction if the individual agrees to or requests the termination in writing; if the individual orally agrees to the termination and the oral agreement is documented; or if the covered entity informs the individual that it is terminating its agreement to a restriction but the termination is only effective for PHI created or received after the individual has been informed of the termination.

B. The HITECH Act

The HITECH Act amended HIPAA to require covered entities to agree to certain requested restrictions. Specifically, a covered entity must agree to an individual’s requested restriction, unless disclosure of the information is otherwise required by law, if: (1) the restriction pertains to disclosures of PHI to a health plan for the purpose of carrying out payment or health care operations; and (2) the restriction applies to PHI that pertains solely to a health care item or service for which the health care provider has been paid out-of-pocket and in full. This amendment gives the individual patient more control over uses and disclosures of his or her PHI, so long as the individual’s request meets the noted requirements.

C. The HITECH Act Proposed Rule

In the HITECH Act Proposed Rule, HHS sought several changes to the Privacy Rule to implement §13405(a) of the HITECH Act. First, recognizing that family members or others often may pay for an individual’s treatment, HHS proposed to add a new subsection to require a covered entity to agree to a request by an individual to restrict disclosure of PHI to the individual’s health plan if: (1) the disclosure is for the purpose of carrying out payment or health care operations and is not otherwise required by law; and (2) the PHI pertains solely to a health

29 45 C.F.R. § 164.522(a).
30 Id. at § 164.522(a)(2).
31 HITECH Act § 13405(a), codified at 42 U.S.C. § 17935(a).
33 45 C.F.R. §164.522(a)(1)(vi).
care item or service for which the individual (or someone else on behalf of individual (e.g., a family member, but not the health plan)) has paid the covered entity in full.\textsuperscript{34}

Second, HHS proposed to modify 45 C.F.R. § 164.522(a)(1)(ii) to require a covered entity to agree to a requested restriction under those circumstances. On a related note, HHS stated that when an individual has exercised a right to restrict a disclosure of PHI from his or her health plan, the covered entity is not permitted to disclose such PHI to a business associate of the health plan. This is because a covered entity may only disclose PHI to a business associate of another covered entity if the disclosure would be permitted directly to that other covered entity. HHS clarified, however, that this new provision does not permit covered entities to require an individual, as a condition of taking advantage of this right, to pay out of pocket for all services received by the individual from that provider. For example, a patient who receives both asthma and diabetes treatment from the same provider may pay out-of-pocket for the diabetes treatment and therefore have a right to have the provider restrict disclosure of diabetes-related treatment information to the health plan, without also having to pay out-of-pocket for asthma treatment in order to have the provider honor the request about the diabetes treatment information.\textsuperscript{35}

Third, HHS sought to clarify that a covered entity may not unilaterally terminate an agreed-upon restriction to a health plan under 45 C.F.R. § 164.522(a)(1)(ii).\textsuperscript{36}

D. The Omnibus Rule

In the Omnibus Rule, HHS adopted the modifications outlined in the HITECH Act Proposed Rule and offered commentary on numerous questions (on which it had solicited comments) about how to operationalize these requirements. Due to a broad variety of logistical issues, putting these requirements into practice has proven quite challenging, but some operational suggestions are included in the discussion below.

1. Payment Out-of-Pocket and In Full

For several reasons, covered entities should clearly describe to individuals what it means to pay “out-of-pocket and in full.” Patients may see this language in a covered entity’s Notice of Privacy Practices (“NPP”) and believe that payment of their copayment, coinsurance, or deductible amount satisfies such payment. This is not the case. Payment out-of-pocket and in full requires payment of the covered entity’s full charge for the item or service restricted. Having said this, payment out-of-pocket may include payment on an individual’s behalf by someone other than the insurance company to which disclosure is restricted. For example, HHS noted that patients may pay for restricted items or services using a flexible spending or health savings account, so long as

\textsuperscript{34} 75 Fed. Reg. at 40899.

\textsuperscript{35} Id.

\textsuperscript{36} Id. at 40890.
the account used is not through the same health insurance plan to which the restriction applies.37

Where an individual’s payment is dishonored, HHS emphasized that it expects covered entities to make “reasonable” efforts to secure payment from an individual. Simultaneously, HHS indicated that it intends this expectation not to serve as an additional burden on providers but rather to align with an entity’s current policies for contacting individuals to obtain alternative forms of payment when the initial form is dishonored.38 HHS specifically noted that a provider is not required to place a person’s debt in collection before the provider may bill the health plan for the item or service. Contrary to what many were suggesting in the months leading up to the September 23, 2013 Omnibus Rule compliance deadline, HHS also clarified in the preamble that providers “may require payment in full at the time of the request for a restriction to avoid payment issues altogether.”39 In other words, requiring payment in full at the time of service is a satisfactory alternative to making reasonable efforts to obtain payment after such payment is dishonored. Along the same lines, nothing in the Omnibus Rule preamble suggests that providers must accept personal checks or other forms of payment that may subsequently be dishonored as payment for these items or services. Similarly, if precertification is required for an item or service an individual wishes to restrict, the provider may require the individual to pay for the care before providing the service in order to assure that it receives payment.

2. Creation of Separate Records Is Not Required

Commenters to the HITECH Act Proposed Rule expressed concerns that covered entities either may have to: (a) create separate records to ensure that restricted data is not inadvertently sent to or accessible by the health plan; or (b) manually redact information from the medical record before disclosing information to a health plan. In response, HHS clarified that covered health care providers are not required to create separate medical records or otherwise segregate PHI that is subject to a restricted health care item or service. However, providers will need to somehow flag or otherwise highlight in the record the PHI that has been restricted.40 Doing so will ensure that restricted PHI is not inadvertently sent or made accessible to a health plan for payment or health care operations purposes, such as future audits by the health plan. From a practical standpoint, however, many covered entities, especially providers using EHRs that do not permit them to segregate such data electronically, will in fact have to implement a manual process for segregating this information and then assuring that the restricted information is not released to the applicable health plans.

38 Id. at 5629-30.
39 Id. at 5630.
40 Id. at 5628.
3. **Exceptions to Restriction Requirement**

HHS also emphasized in the preamble that covered entities are not required to honor requests for restriction where a disclosure is otherwise required by law. Some commenters asked whether this means that providers may not receive cash payment from individuals (a) for items or services covered by Medicare and Medicaid, or (b) where a state law prevents providers from billing and receiving cash payment from individuals for covered services over and above permissible cost-sharing amounts. HHS responded that in such situations, if a provider is required by law to submit a claim to a health plan for a covered service provided to the individual, and individuals are not permitted to pay out-of-pocket for the service, then the disclosure is required by law and constitutes an exception to the individual’s right to request a restriction to the health plan.\(^{41}\) There is, however, an exception to this exception: if a Medicare beneficiary or his or her legal representative refuses to authorize the submission of a bill to Medicare, a provider is not required to submit a claim to Medicare for the covered service and may instead accept an out-of-pocket payment from the beneficiary. If the provider accepts the out-of-pocket payment, it must refrain from disclosing to Medicare the PHI related to the item or service paid for.\(^{42}\)

In the HITECH Act Proposed Rule, HHS acknowledged that under most HMO contracts with providers, individuals may not be permitted to pay the provider in full for the treatment or service received, and HHS sought comment on how the restriction right would apply to HMO beneficiaries. Based upon comments it received, in the Omnibus Rule HHS clarified that HMO providers must abide by an individual’s restriction unless state or other law actually prohibits the provider from doing so. Thus, if a state law prohibits an HMO provider from accepting an individual’s payment above the individual’s cost-sharing amount, then the provider should counsel the individual to use an out-of-network provider for the item or service about which the person seeks to restrict information from the HMO. However, if the prohibition against accepting an individual’s payment is simply a term of the HMO’s contract with the provider, then the provider should abide by the individual’s requested restriction. To avoid breaching such contracts, HHS recommends that providers update their contracts with HMOs as needed to comply with this requirement.\(^{43}\) This suggestion to revise HMO contracts sounds easier than it most likely will be, in practice, for health care providers.

Additionally, if a patient does not make a request for restriction until the health care item or service already has been provided or initiated (for example, the restriction is sought midway through a hospital stay), a covered entity already may have disclosed PHI pertaining to that item or service to the patient’s health plan. As agreeing to the individual’s request is not possible under these circumstances, the provider will not be found to be in violation of the Privacy Rule for having disclosed PHI to the patient’s

\(^{41}\) *Id.*

\(^{42}\) *Id.*

\(^{43}\) *Id.* at 5629.
health plan up to that point, but the covered entity should honor the request going forward if feasible and if the patient wishes. In the interest of preserving good patient relations, covered entities should consider addressing these issues with patients prior to treatment.

4. Bundled Services and Downstream Providers

Some commenters to the HITECH Act Proposed Rule expressed concern that individuals may seek to request a restriction on, and pay for, a single item or service in a single patient encounter where that item or service typically is bundled together with other items or services for billing purposes. In such cases, HHS indicated that it expects providers to advise patients whether the provider can unbundle the items or services (e.g., whether the provider’s EHR system is able to blind or flag and restrict from disclosure a single line item or service in an encounter), and whether doing so will nonetheless permit the health plan to understand, based upon context, that the restricted item or service was provided.\textsuperscript{44} If, after counseling the patient, the provider is able to unbundle the items or services to accommodate the patient’s wish, and the patient wishes the provider to do so notwithstanding the health plan’s potential awareness of the restricted item or service, the provider should do so. If the provider is unable to accommodate the individual’s wish, HHS expects providers to inform individuals of this fact and provide such individuals an opportunity to pay out-of-pocket for the entire bundle of items or services.\textsuperscript{45}

Many commenters expressed concern about HHS’s request for comments in the HITECH Act Proposed Rule addressing whether restrictions placed on PHI should apply and attach to such PHI as it moves downstream (e.g., the individual requests a provider to forward treatment records to another provider and the individual has restricted much of the information in those records from disclosure to the individual’s health plan). In response to these concerns, HHS clarified in the Omnibus Rule that providers are not required to notify an individual’s “downstream” providers (e.g., specialists or providers offering follow-up care) that the individual has sought to restrict his or her PHI about an item or service from a health plan and accordingly may wish to do the same at the “downstream” provider. For example, if a physician is ordering tests and refers the patient to a cardiologist, then it is the patient’s responsibility to request a restriction from the cardiologist if the patient wishes to pay out-of-pocket for services the cardiologist provides that may be related to an item or service that the patient received from the first physician and restricted from disclosure to the patient’s health plan. However, HHS expects providers, “in the very least,” to discuss the implications of restrictions with patients so patients become aware that they will need to request a restriction and pay out-of-pocket with “downstream” providers in order for a restriction to extend to disclosures about care given by those providers, as well.\textsuperscript{46} Alerting patients to these nuances is particularly important where care is being provided outside of an integrated facility or system, as the providers involved may not necessarily share a common EHR.

\textsuperscript{44} Id.
\textsuperscript{45} Id.
\textsuperscript{46} Id.
Where individuals seek follow-up care related to the restricted item or service within an integrated facility or health system, the facility or system may be required to disclose information about the follow-up care in order to receive payment for the follow-up treatment or to obtain a determination that the follow-up services are medically necessary. Covered entities should consider whether they will require patients to request a restriction on and pay out-of-pocket and in full for such follow-up services, and how they will address the situation if a patient does not make a restriction request or payment for the follow-up services. In these circumstances, some covered entities have determined that they will disclose only the minimum necessary amount of information in order to obtain payment or a determination that the follow-up treatment is medically necessary. Although patient authorization would not be required for such a disclosure, covered entities should consider informing patients in advance about the possibility of this scenario arising if patients do not request restrictions on and pay for related follow-up care.

Additionally, if a provider who e-prescribes learns that a patient wishes to pay out-of-pocket and restrict disclosure of the patient’s prescription information, HHS suggested that the prescriber offer the patient a paper prescription so that the patient may request a restriction and pay out-of-pocket at the pharmacy; otherwise, the pharmacy most likely will have received the e-prescription and billed the patient’s health plan before the patient arrives at the pharmacy. HHS does not offer guidance on how providers may learn which patients may be interested in seeking a restriction on information about drugs or medical equipment before they are prescribed, but it may be helpful for providers to include in their NPPs a statement asking individuals to advise the provider of any requested restriction as early in the patient encounter as possible.

5. Effect of Restriction

HHS clarified that the restriction on disclosure does not prohibit providers from disclosing the PHI to persons or entities other than the applicable health plan or insurance company for purposes permitted by HIPAA (for example, disclosures of information to family members involved in the individual’s care would still be permitted, as would disclosures of information to subsequent providers). However, if an entity accepts a person’s requested restriction, it may not release the PHI in the future to the individual’s health plan for any future payment or health care operations purpose. For example, if in performing an audit a health plan requests records of all treatment provided to an individual who has an accepted restriction, a provider may not give the health plan any PHI related to the item or service to which the restriction applies.

6. Termination of Restriction

Covered entities may not unilaterally terminate restrictions to which they previously agreed and for which they have received payment out-of-pocket and in full. Termination of such restrictions is appropriate only where the patient requests or agrees

47 Id.
to the termination in writing. If the patient orally requests or agrees to terminate a restriction, the oral agreement should be documented.

E. **Practical and Operational Considerations**

Assuring compliance with the restrictions requirement will require a clear policy addressing these issues and training for a variety of employees within a covered entity’s organization who may need to be aware of and help implement the restriction. For example, if a provider accepts a patient’s requested restriction, it must train all staff who might be involved in a later audit by the patient’s insurance plan on the requirement to not disclose information related to the restricted item or service during any such audit. Covered entities also must determine how they will implement a process that follows the data and enables the organization to afford patients a meaningful opportunity to restrict such information and then comply with patients’ requested restrictions.

1. **Statement about Restrictions in NPP**

Initially, providers should consider how to notify patients of their right to request restrictions on release of PHI to their health plans about items or services for which patients have paid out-of-pocket. HHS’s clarifications in the Omnibus Rule about individuals’ right to request restrictions may leave covered entities thinking that they should include a statement in their NPPs indicating that they are required to agree to requested restrictions that meet the requirements noted above. Based upon an informal review of NPPs available on the Internet, this is exactly how many covered entities appear to be addressing this issue. Due to the variety of exceptions to and limitations on this individual right, however, there are good risk management reasons to qualify any such NPP statement. For example, NPPs could provide that where a patient requests a provider to restrict disclosure of PHI to the patient’s health plan about an item for which the patient has paid out-of-pocket and in full, the covered entity is “generally required to agree” to the individual’s request, noting exceptions if the disclosure is for treatment purposes or is required by law. A second sentence could note that there may be additional limitations upon the covered entity’s ability to comply with the requested restriction, along with a brief listing of those limitations.

2. **Receipt, Review, and Approval or Disapproval of a Request**

Covered entities next should consider whether they will wait for patients to ask questions about restricting information from their health plans before addressing these issues with patients, or whether they will provide patients with information or counseling to educate patients about their right upon registration or at some other point during the patient encounter. If the latter, will the entity educate all staff about the detailed nuances of this patient right, or will it prepare a brief summary of the right and the exceptions, provide that summary to patients, and ask patients to direct questions to registration staff, the health information management (“HIM”) department, or the business office, and train only the appropriate individuals in the applicable department? From a risk management standpoint, directing all inquiries to HIM staff both can assure that patients are provided
appropriate information about their rights and streamline the restrictions process, but whatever process is chosen must be documented and training provided on it.

Regardless of what person or persons is responsible for evaluating restriction requests, the entity must have a form upon or an electronic process through which patients can document their requested restriction. Entities that have a separate HIM department and business office may wish to have HIM evaluate whether the entity is required and able to accept a restriction (including issues such as whether the EHR system permits the entity to unbundle an item or service if requested) and then notify the patient of the acceptance or denial and the reasons therefor. If the restriction is accepted, the HIM department should notify the business office promptly so that the patient’s health plan is not notified of the restricted information, and the business office in turn must have processes to follow if the patient’s payment is dishonored.