AIS Special Report

Final Rule: Modifications to the HIPAA Privacy, Security, Enforcement, and HITECH Act Breach Notification Rules, 78 Fed. Reg. 5566 (Jan. 25, 2013)

By Francie Fernald, Editor, AIS's Report on Patient Privacy

Almost four years after the Health Information Technology for Economic and Clinical Health Act (the HITECH Act) became law, the Office for Civil Rights, Department of Health and Human Services, published its final rule implementing provisions of the act, amending the breach notification rules that were issued in August 2009, modifying other sections of the HIPAA privacy and security rules that have been in effect for more than a decade, and implementing the provisions of the Genetic Information and Nondiscrimination Act of 2008 (GINA) affecting the privacy of genetic health information. The rule finalizes four separate proposed or interim final rules. The rule was published in the *Federal Register* on Jan. 25. Its effective date is March 26, 2013, but its compliance deadline is Sept. 23, 2013.

The rule amends many provisions in the privacy rule and the breach notification rules, but perhaps its most significant impact is the direct application of many of the provisions of the security rule, as well as some provisions of the privacy rule, to business associates and their subcontractors.

This special report summarizes the amendments to the regulatory language and highlights the clarifications that HHS discusses in the preamble to the rule. It has two parts: (1) revisions to the breach notification rules, and (2) revisions to the HIPAA privacy and security rules and the HHS OIG enforcement rules mandated by the HITECH Act.

Note that the final rule does not address the HITECH accounting for disclosure provisions. These are the subject of a separate rulemaking.

I. Modifications to the Breach Notification Rules (45 CFR Part 164, Subpart D)

HHS promulgated an interim final rule addressing the HITECH Act's breach notification requirements on Aug. 24, 2009. The modifications to the rule make it clear that its requirements apply to business associates as well as covered entities. (In this part, the term "covered entities" encompasses business associates.)

The final rule also makes two significant changes to the interim final rule's definition of "breach" in §164.402. First, the language now specifies that *any* impermissible use or disclosure is presumed to be a breach, and the standard to determine the likelihood that the PHI has been or would be compromised has changed. HHS removed the phrase "poses a significant risk of financial, reputational, or other harm to the individual" (the harm standard) and replaced it with a finding by the covered entity related to the probability that the PHI has been compromised. Thus, covered entity must provide notification of a breach unless an exception applies or demonstrates through a risk assessment that there is a low probability that the PHI has been or will be compromised.

The 'Low Probability' Standard

The rule sets out four specific factors covered entities must assess to determine the low probability of compromise:

(1) The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification. The factor refers to the sensitivity of the breached information. The standard is the degree to which the breached information could be used "in a manner adverse to the individual or otherwise used to further the unauthorized recipient's own interests." For example, did the breached information include data that could lead to identity theft or financial fraud, such as financial information or Social Security numbers? How sensitive and how detailed was the clinical information (e.g., the type of services provided, treatment plan, diagnosis, medication, medical history and test results)?

In addition, if the information contains direct identifiers, the covered entity must determine the likelihood that the information could be re-identified. For example, if the breached PHI was a list of patient names, addresses, and hospital identification numbers, the information is clearly identifiable and likely would be assessed as more than a low probability that the information has been compromised. On the other hand, if the information was a list of patient discharge dates and diagnoses, the covered entity would assess whether any of the patients could be identified based on the specificity of the diagnosis, the size of the community service by the covered entity, or whether the recipient could combine the information with other information to re-identify affected individuals.

(2) The unauthorized person who used the PHI or to whom the disclosure was made. According to the preamble to the final rule, the covered entity should determine whether the unauthorized person is subject to HIPAA or other federal privacy rules as this may reduce the probability of compromise. However, with regard to information that is not immediately identifiable, an assessment also must be made as to whether the unauthorized person has the ability to re-identify the information. For example, if the unauthorized disclosure of discharge dates and diagnoses was made to the individual's employer, the information has a more than low probability of compromise.

(3) Whether the PHI was actually acquired or viewed or whether the opportunity existed to acquire or view but actual viewing or acquisition did not occur. For example, if a stolen laptop is later recovered and forensic analysis shows that the PHI was never accessed or otherwise compromised, the covered entity may conclude that the PHI was never actually acquired even though the individual had the opportunity. However, if an explanation of health care benefits was mailed to the wrong person and the individual opened it, the PHI has been breached.

(4) The extent to which the risk has been mitigated. The rule requires covered entities to attempt to mitigate any risks as soon as possible and determine the extent and efficacy of the mitigation to assess the degree of compromise. For example, the covered entity may seek assurances from the recipient that the information will not be used or disclosed by obtaining a signed confidentiality agreement or an affidavit that the information has been destroyed. Again, the covered entity must weigh who or what the unauthorized recipient is to gauge whether the assurances are satisfactory.

All four of these factors must be addressed in the risk assessment to determine the level of probability of compromise of the PHI, but covered entities also may assess other factors. Once all the factors have been assessed, the covered entity evaluates the overall probability based on the findings as to whether the level of compromise to the PHI is low. If the assessment leads to

a conclusion that the risk of compromise is not low, the covered entity must notify the affected individuals in accordance with the breach regulations.

HHS acknowledged that violations of the minimum necessary requirements could trigger the breach notification provisions and would be assessed in light of the four factors. For example, if the PHI sent to a business associate contained more than the minimum necessary information, its risk assessment level would be lower than if it had been sent to an outside third party.

The final rule notes that a covered entity or business associate may choose to notify the individuals without conducting risk assessment. It also advises covered entities to review their policies and procedures to be sure they reflect the four factors that must be considered in the risk assessment. Covered entities should document their risk assessment and their decision-making carefully and thoroughly.

The Exceptions

The interim final rule, in the definition of "breach" in §164.402, included three statutory exceptions, which, if present, would exempt the covered entity from conducting a risk assessment and providing notice because no breach would have occurred:

(1) Unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of the covered entity as long as the disclosure was made in good faith (which does not include employee snooping) and within the scope of authority and does not result in further unauthorized use or disclosure.

(2) Inadvertent disclosure by one person at a covered entity or business associate who is authorized to access PHI to another person authorized access to PHI, albeit not necessarily the same type of PHI, at the same covered entity, business associate, or organized health care arrangement in which the covered entity participates, as long as the PHI is not again used or disclosed without authorization. The final rule clarifies that this disclosure must occur onsite to a person who is not a member of the workforce, for example, to a physician with staff privileges; if the PHI is "used" impermissibly by workforce members, the rule says the covered entity should determine whether the first exception applies.

(3) A good faith belief that the unauthorized recipient of the information would not have reasonably been able to retain the information, for example, if a misdirected piece of mail with PHI was returned unopened or a nurse is able to retrieve the wrong discharge papers from a patient before the patient has had a change to read the papers.

HHS added a fourth exception in the interim final rule for the impermissible use or disclosure of a limited data set as long as dates of birth and ZIP codes were not included in the data. However, HHS removed this exception in the final rule, and a covered entity now must perform a risk assessment with regard to unauthorized use or disclosure of a limited data set.

The final rule clarifies that if the breach fits into an exception at the time the breach is discovered, the covered entity/business associate does not need to notify the individuals but should take steps to assure that there is no further use or disclosure. However, if at a later time this PHI is used or disclosed in an impermissible manner, the covered entity/business associate must treat this as a separate breach.

Other Changes

HHS made no significant changes to the breach notification requirements, timeliness, content, and method of notification provisions, but it did provide some clarifications. The breach rules in §164.404(b) require a covered entity to provide written notice to all individuals whose

PHI has been compromised no later than 60 days after the breach has been discovered, and §164.404(d) requires the covered entity to provide a substitute notice if the contact information is out-of-date and the direct written notification is not successful. HHS clarified that within the 60-day period covered entities may attempt to cure any notice that is returned because of out-of-date contact information and not send a substitute notice. If the covered entity realizes that it will not be able to reach 10 or more individuals with direct written notice because of outdated information, it must provide a Web or media notice as soon as possible.

According to the preamble, notice to the media required in §164.406 neither requires the covered entity to incur costs to print a media notice nor requires the media outlet to publish any information about the breach. The agency also notes that posting a press release on the covered entity's website does not meet the media notification requirement. The notice must be provided directly to the media outlet.

HHS also clarified that in the case of notice to HHS for breaches affecting fewer than 500 individuals (§164.408(c)), the covered entity must report those breaches within 60 days of the end of the calendar year in which they were discovered, not the year they occurred.

II. Modification to the HIPAA Privacy and Security Rules and the HHS OIG Enforcement Rules

In addition to breach notification provisions, the HITECH Act mandated changes to the HIPAA privacy and security rules to increase their effectiveness and strengthen their enforcement. In this final rule, HHS amended the existing regulations to incorporate the HITECH requirements and made other changes "to increase the workability and flexibility, decrease the burden, and better harmonize" the rules with other HHS regulations.

Business Associates

The HITECH Act extended to business associates liability for compliance with certain provisions of the HIPAA privacy and security rules. Where liability is not extended directly, the business associate agreement may make the entity contractually liable for compliance. HHS made one important revision that effects business associates in a hybrid entity. As of Sept. 23, 2013, all business associate components of a hybrid entity must be included within the health care component of the entity.

Business Associates and the HIPAA Security Rule

Sec. 13401 of the HITECH Act makes business associates, which under the final regulations include subcontractors, directly liable for complying with the following requirements of the security rule as of Sept, 23, 2013, the compliance deadline set in the rule:

- §164.308, Administrative safeguards
- §164.310 , Physical safeguards
- §164.312 , Technical safeguards
- §164.316, Policies and procedures and documentation requirements

HHS also added certain provisions of §164.314, "Organizational requirements," to the list.

If these provisions are violated, the business associate or its subcontractor is subject to the same civil and criminal penalties as the covered entity.

Other security provisions in the HITECH Act also apply to business associates and its subcontractors but are enforceable through the business associate contract.

As the starting point, the definition of "business associate" in §160.103 of the regulations (which applies to both the HIPAA privacy and security rules) has been amended to expand the meaning of the term and to include the exceptions that do not create a business associate relationship.

Of most significance is the designation of a subcontractor to a business associate as a business associate. In that capacity the subcontractor is directly liable for violations of any applicable HIPAA provisions. A new definition defines a "subcontractor" as "a person to whom a business associate delegates a function, activity, or service other than in the capacity of a workforce member," and it is the business associate, not the covered entity, that must obtain "satisfactory assurances," (i.e., the business associate agreement) from the subcontractor that it will protect PHI as required by the HIPAA rules. Likewise, a subcontractor must obtain these satisfactory assurances from any entity with which it subcontracts to handle functions or activities involving PHI. With this chain of liability, an individual's PHI is protected "no matter how far 'down the chain' the information flows."

Business associates now include patient safety organizations when they receive reports of patient safety events or concerns from providers and analyze the events to reporting providers. Health information organizations, e-prescribing gateways, or other persons or entities that provide data transmission services with PHI for a covered entity also are business associates if their functions require "routine" access to PHI. A determination as to whether the entity has routine access will be fact-specific based on the nature of the services provided and the extent to which the entity needs access to the PHI to perform the service for the covered entity. If they do not have routine access, they are considered "conduits" providing mere courier services. Examples of conduits include the U.S. Postal Service or United Parcel Service or internet providers that offer data transmission only. The conduit exception, the final rule says, is a narrow one and is limited to transmission services, including temporary storage. On the other hand, an entity that maintains PHI on behalf of the covered entity is a business associate, even if it does not actually view the PHI.

Finally, vendors of personal health records are business associates when a covered entity hires them to provide and manage a personal health record service for its patient. The vendor is not a business associate solely by entering into an interoperability relationship with the covered entity, for example to transmit data from the covered entity's EHR to the patient's personal health record maintained by the vendor.

With regard to the exceptions, §164.308(b)(2) and §164.502(e)(1)(ii), each provided circumstances where the disclosure of PHI would not require a business associate contract, such as the transmission or disclosure of PHI for treatment purposes. The exceptions in these provisions have been moved to the definition of "business associate." According to the preamble to the final rule, one reason for relocating the exceptions was to make clear that a person or an entity is a business associate if the person or entity meets the definition of "business associate," regardless of whether the parties have entered into the required business associate contract.

Section 164.314 has been amended to make clear that contracts between the covered entity and business associate must now require the business associate to comply with the relevant provisions of the security rule and to report breaches of unsecured PHI to the covered entity. It also

requires that business associates enter into a similar agreement with subcontractors, and that the contracts between business associates and their subcontractors meet the section's requirements.

Overall, the final rule makes only a few amendments to the actual provisions of the security rule. It makes the provisions applicable to business associates by inserting "business associate" before "covered entity" in the relevant provisions. The preamble emphasizes that covered entities and business associates must review their security measure to assure protection of electronic PHI and review their policies and procedures to be sure they reflect the revised requirements.

Finally, in its discussion of revisions to the definition of "electronic media," to make the definition better reflect technology, HHS clarified that PHI stored, whether intentionally or not, in photocopiers, faxes, and other devices is subject to the privacy and security rules.

Business Associates and the HIPAA Privacy Rule

The majority of the amendments to the privacy rule (45 CFR Part 164, Subpart E) address the expansion of certain privacy provisions of the HITECH Act to business associates; however HHS made other modifications to "improve the workability and effectiveness of the Rule" and to conform the privacy rules with the requirements of the Patient Safety and Quality Improvement Act (PSQIA).

Section 13404 of the HITECH Act does not require the business associate to comply with all the requirements of the privacy rules. Instead, it requires business associates to comply with all of the provisions in the business associate contract described in §164.504(e) and requires the business associate agreement to include the new provisions in the HITECH Act that relate to privacy, including breach notification. Therefore, if a covered entity wants a business associate to be liable for additional provisions of the privacy rule, compliance with the provision must be included in the business associate agreement.

Because of the required content of the agreement, the business associate is liable for the following:

◆ Uses and disclosures of PHI that are not in accord with its business associate agreement or the privacy rule

◆ Failing to disclose PHI when required by HHS/OCR in order to investigate and determine the business associate's compliance with the HIPAA rules

◆ Failing to make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request

◆ Failing to enter into business associate agreements with subcontractors that create or receive protected health information on their behalf

◆ Failing to disclose PHI to the covered entity, individual, or individual's designee, as necessary to satisfy a covered entity's obligations with respect to an individual's request for an electronic copy of protected health information

◆ Failure to provide electronic access in accordance with their business associate agreements

◆ Failure to provide an accounting of disclosures

◆ Failure to take reasonable steps if the business associate knew of a pattern of activity or practice of its subcontractor that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement and, if such steps were unsuccessful to terminate the contract or report the problem to HHS.

The regulations implementing the preemption of state law also apply to business associates.

Among the provisions business associates are not required to follow by statute or regulation are issuance of the notice of privacy practices and appointment of a privacy officer. (In contrast, business associates under the security rule's administrative safeguards (§164.308(a)(2)) must appoint a security officer responsible for development and implementation of the policies and procedures of the security regulations.)

With regard to uses and disclosures of PHI, a business associate must comply with the requirements in §164.502 of the privacy rule as if it were a covered entity; and if it is not in compliance, it is subject to the same civil and criminal penalties as a covered entity. HHS amended §164.502 to add the permitted and required uses and disclosures for business associates.

The final rule also adds new prohibited uses and disclosures that apply to both the covered entity and its business associates to implement privacy provisions in the Genetic Information Nondiscrimination Act.

HHS makes clear that a business associate's liability for violations of the use and disclosure requirements of privacy regulations attaches immediately, that is, as soon as a person creates, receives, maintains, or transmits PHI in violation of the rules. The type of PHI has no bearing on whether the business associate is in compliance; if the data are tied to the covered entity, then they are PHI and must be protected.

HHS amended §164.504(e) to add provisions that must be included in the contract between the covered entity and the business associate, the business associate and the subcontractor, and the subcontractor and a second subcontractor as prescribed by the HITECH Act. As summarized by HHS, under the amended regulations, "each agreement in the business associate chain must be as stringent as or more stringent than the agreement above with respect to permissible uses and disclosures."

Now the agreement must state that the business associate will:

◆ Comply with the provisions of the security rule;

◆ Report breaches of unsecured protected health information under the breach reporting rules;

◆ Ensure that a subcontractor agrees to the same restrictions and conditions that apply to the business associate with respect to such information; and

◆ Comply with the privacy requirements that apply to the covered entity in the performance of an activity the business associate is carrying out on behalf of the covered entity.

The amendments do contain a transition rule in new §164.532(d) and (e) allowing covered entities and business associates to operate under existing contracts for up to one year beyond the rule's compliance date. Contracts that were in effect before Jan. 25, 2013, and that are not renewed or modified between March 26, 2013, and Sept. 23, 2013, qualify for the transition rule.

Marketing, Fundraising, and Sale of PHI

Apart from the amendments necessitated by the expansion of liability to business associates, the other significant changes in the privacy rules affect marketing, fundraising, and the sale of PHI.

Marketing

Section 164.508 of the privacy regulations currently requires covered entities to obtain valid authorizations before using or disclosing PHI to market a product or service, subject to certain

exceptions, including communications for a covered entity's product or service, for treatment of the individual, and for alternative therapies.

Section 13406 of the HITECH Act requires an authorization for health-related communications that are part of health care operations if the covered entity or business associate receives direct or indirect payment unless the communication describes only a drug or biologic currently being prescribed to the individual. If the communication meets this exception, any payment received must be "reasonable."

In the final rule, HHS made a significant change to its proposed revisions to the definition of "marketing" in §164.501. It had proposed to retain the exceptions for certain health care operations where the covered entity did not receive financial payment and for treatment communications even if the covered entity received payment, as long as the notice of privacy practices stated that the individual may receive such communications and the treatment communication itself disclosed receipt of remuneration and provided the individual with a clear and conspicuous opportunity to elect not to receive any further such communications.

In the final rule, marketing now requires a valid authorization for all treatment and health care operations communications if the covered entity receives a financial payment from a third party for the product or service being marketed. The only exceptions are for refill reminders and drugs and biologics currently prescribed to the individual but the remuneration must be reasonable and related to the cost the covered entity incurred to make the communication. All other health care-related communications for which the covered entity receives payment, regardless of whether they are considered treatment or health care operations, require a valid authorization.

The refill reminders and current drugs and biologics exceptions include communications about generic equivalents as well as communications encouraging the patient to take the medication as directed. For self-administered drugs, communications regarding administration of the drug and necessary equipment also fall under the exception. "Reasonable" payment in this exception means the cost of labor, supplies, and postage.

This provision also applies to business associates if they are permitted in the business associate agreement to make these communications. Again, the payment must be for the purpose of marketing the product or service of a third party to encourage individuals to purchase or use the product or service.

To be valid, the authorization must state that the covered entity is receiving payment for the communication. However, these revisions do not affect the exceptions in §164.508 that do not require an authorization if the communication is face-to-face by the covered entity or consists of a promotional gift of nominal value. Note that email, phone, and mail communications are not considered face-to-face communications.

HHS addressed the distinction between direct and indirect payment:

◆ Direct payment means financial remuneration that flows from the third party whose product or service is being described directly to the covered entity.

◆ Indirect payment means financial remuneration that flows from an entity on behalf of the third party whose product or service is being described to a covered entity.

Financial payment or remuneration does not include non-financial benefits, such as in-kind benefits.

Fundraising

The final regulations also amend the fundraising provisions in §164.514. The HITECH Act requires a covered entity to give a recipient of a fundraising communication a "clear and conspicuous" opportunity to opt-out. Any opt-out must be treated as a revocation of an authorization, and the covered entity must not send any fundraising material to the individual. The opt-out method may not be burdensome or expensive, and the covered entity may not condition treatment or payment on an individual's choice to receive fundraising communications. The opt-out must be offered on phone contacts as well as in written material. The opt-out is effective for all forms of fundraising.

Section 164.514(f)(2)(v) allows covered entities to establish an opt-back-in process.

The final rule expands the information that may be used and disclosed for fundraising. Under the current regulations, the covered entity may use or disclose only the individual's demographic information and dates of health care. Under this final rule, covered entities now may use or disclose department of service, such as cardiology or pediatrics, treating physician information, and outcome information, which includes information regarding the death of the patient and any suboptimal results. Minimum necessary still applies.

The privacy notice must state that the covered entity may contact a patient to raise funds for the covered entity and the individual has the right to opt out.

Sale of Protected Health Information

The final rule adds to §164.508, "Uses and disclosures for which an authorization is required," a prohibition on the sale of PHI without an authorization, but the provision includes a number of exceptions. First, the rule defines "sale of protected health information" in §164.502(a)(5)(ii) as "a disclosure of protected health information by a covered entity or business associate, if applicable, where the covered entity or business associate directly or indirectly receives remuneration from or on behalf of the recipient of the protected health information in exchange for the protected health information." A "sale," HHS says, is not limited to transactions where there is a transfer of ownership, but includes transactions such as payment for access, a license, or lease agreements.

HHS also does not consider remuneration to a covered entity in the form of grants, contracts, or other arrangements to perform programs or activities, such as research studies, a "sale" of PHI. Thus a research sponsor may pay a covered entity to conduct the research, and the covered entity may accept a grant from the federal government without violating the prohibition on the sale of PHI. Fees paid to a health information exchange by the HIE participants who receive PHI also are not a sale of PHI.

The rule has eight disclosures of PHI that are excepted from the prohibition:

(1) For public health purposes (§ 164.512(b) or § 164.514(e));

(2) For research purposes (§ 164.512(i) or § 164.514(e)), where the only remuneration received by the covered entity or business associate is a reasonable cost-based fee to cover the cost to prepare and transmit the protected health information for such purposes;

(3) For treatment and payment purposes (§ 164.506(a));

(4) For the sale, transfer, merger, or consolidation of all or part of the covered entity and for related due diligence (§ 164.506(a));

(5) To or by a business associate for activities that the business associate undertakes on behalf of a covered entity, or on behalf of a business associate in the case of a subcontractor, pursuant to §§ 164.502(e) and 164.504(e), and the only remuneration provided is by the covered entity to the business associate, or by the business associate to the subcontractor, if applicable, for the performance of such activities;

(6) To an individual to allow access to protected health information (§ 164.524) or to provide an accounting of disclosures of protected health information (§ 164.528);

(7) Required by law as permitted under § 164.512(a); and

(8) For any other purpose permitted by and in accordance with the applicable requirements of this subpart, where the only remuneration received by the covered entity or business associate is a reasonable, cost-based fee to cover the cost to prepare and transmit the protected health information for such purpose or a fee otherwise expressly permitted by other law.

Three of the exceptions have conditions regarding the payment. In the research exception, the payment may only be a reasonable cost-based fee to cover the cost to prepare and transmit the protected health information. The covered entity-to-business associate exception limits the fee to reimbursement for performing the activity on behalf of the covered entity. The last catch-all exception also limits the payment to a reasonable, cost-based fee to cover costs associate with preparation and transmission of the PHI or to the amount permitted by state law.

The final exception also applies to business associates. As such a business associate is permitted to receive reasonable, cost-based fees from a third party to prepare and transmit data on behalf of the covered. The business associate also may reimburse a subcontractor in the same manner as the covered entity reimburses the business associate.

The types of costs that may be included in the reasonable cost-based fee to prepare and transmit the data include both direct and indirect costs, such as labor, materials, and supplies for generating, storing, retrieving, and transmitting the PHI; labor and supplies to ensure the PHI is disclosed in a permissible manner; and related capital and overhead costs. No profit margin is allowed.

HHS distinguishes the term "remuneration" in the "sale of PHI" definition from the term "payment" in the marketing definition. The term "payment," HHS says, refers only to financial reimbursement, not to in-kind reimbursement. "Remuneration," however, is not so limited and encompasses both financial and nonfinancial benefits.

To be valid, the authorization for the sale of PHI must state that the covered entity will receive remuneration for the PHI. However, if a covered entity obtained a valid authorization from an individual before the rule's compliance date of Sept. 23, HHS will grandfather in these authorizations, even though they do not state that the covered entity received remuneration. This grandfather rule applies to research studies and any other permissible purposes under the privacy rule. Thus covered entities may release PHI and receive reimbursement even without an authorization that meets the provision of the new final rule as long as the authorization was obtained before the rule's compliance date; they also may rely on an institutional review board's waiver of authorization prior to the compliance date of the rule.

Covered entities also may continue to use or disclose limited data sets under a data use agreement until the agreement is renewed or modified or until one year from the rule's compliance date, whichever is earlier.

Research

In the final rule, HHS again confirmed that researchers are not business associates unless they are acting in a business associate capacity for the covered entity.

The amendments in the final rule benefit researchers by permitting combined authorizations. Before the amendments of this final rule, §164.508(b)(3) had a general prohibition on "compound authorizations," that is, authorizations for use or disclosure of PHI combined with any other legal permission. One exception to this prohibition is an authorization for a research study that includes other permissions for the same study. However researchers still may not combine an authorization that conditions treatment, payment, enrollment in a health plan, or eligibility for benefits (conditioned authorization) with an authorization for another purpose for which treatment, payment, enrollment, or eligibility may not be conditioned (unconditioned authorization). As an example, HHS cites a research study that includes both treatment (conditioned authorization) and tissue banking of specimens, which would require an unconditioned authorization.

The final rule amends §164.508(b)(3)(i) and (iii) to allow a covered entity to combine conditioned and unconditioned authorizations for any type of research study except those involving psychotherapy notes, provided that the authorization clearly differentiates between the conditioned and unconditioned research components and clearly allows the individual the option to opt in to the unconditioned research activities. A provision allowing an individual to opt-out of the unconditioned research activities (instead of an opt-in) will not satisfy this requirement.

If an individual revokes a part of the authorization, the revocation, as long as it is clear as to what the revocation pertains to, does not affect the rest of the authorization. However, if it is unclear as to what the individual intended to revoke, the entire authorization must be revoked unless the individual clarifies the request in writing.

HHS also made an important change to its interpretation that the privacy rule requires the authorization to be study-specific. Under the final rule, HHS will no longer interpret the "purpose" provision at § 164.508(c)(1)(iv) as requiring a study-specific authorization for the use or disclosure of PHI. However, this change does not modify the required content of an authorization. An authorization for use or disclosure of PHI in future research must adequately describe the purpose to inform the individual that his/her PHI may be used in the future for research studies and may include information that is collected after conclusion of the original study.

Other Revisions to the Use and Disclosure of PHI

The final rule revises the permissible uses and disclosures of PHI for decedents, student immunizations, and genetic information.

Decedents

Currently the PHI of decedents is protected in the same way as the PHI of a living individual, that is, with no time limit. The final rule in §164.502(f) now specifies that the PHI of decedents will be protected for 50 years, but after that time period, the data will no longer be considered PHI. The preamble notes that state laws that provide greater protections for decedent PHI will override this HIPAA time limit.

HHS also amended §164.510(b) to allow family members and others involved in the care of the decedent to obtain PHI from the covered entity, unless it is inconsistent with an express desire or preference of the decedent.

Student Immunizations

Section 164.512(b)(1) now permits a covered entity to disclose proof of immunization to a school where state or other law requires this information before enrolling the child. While the covered entity does not need to obtain a written authorization, it still must obtain oral agreement from the responsible party; a request by the school is not sufficient. Covered entities must document the agreement, which remains effective until revoked.

HHS clarifies that the privacy rule as currently in force does not prohibit covered entities from disclosing immunization PHI to a school if this disclosure is required by state law. However, if state law permits only the disclosure of immunization records, the covered entity must comply with the new provision. Covered entities also are currently permitted to disclose immunization PHI to state registries without an authorization because this is a public health activity.

Genetic Information

The Genetic Information Nondiscrimination Act of 2006 (GINA) has added a new type of health information to the protections of the privacy rule — genetic information. The statute overall prohibits discrimination based on an individual's genetic information for both health care coverage and employment. It explicitly requires HHS to revise the privacy regulations to state that genetic information is "health information" and to prohibit health plans, health insurance issuers (including HMOs), and issuers of Medicare supplemental policies from using or disclosing genetic information for underwriting purposes. The final rule adds a definition of "genetic information" and other related terms to §160.503.

Because the privacy rule classifies additional entities as health plans, the rules apply to employee welfare benefit plans, high risk pools, public benefit programs, such as Medicare Part A and B, TRICARE and other veteran health care programs, the Indian Health Service, and any other individual or group plan that pays for medical care, such as limited dental or vision plans. The only entity not included as a health plan for purposes of GINA are issuers of long-term care policies. However, long-term care plans, while not subject to the privacy underwriting prohibition, still must protect genetic information from improper uses or disclosures of PHI.

HHS emphasizes that GINA is not applicable to providers, only to health plans. Thus a provider may disclose genetic information to a health plan for payment purposes. The provider also may disclose an individual's genetic information needed for treatment of a family member as long as the individual has not requested a restriction on the disclosure.

The expansion of the privacy rule to genetic information necessitated some additions and conforming revisions to several privacy terms: new definitions have been added for "genetic tests," "genetic services," "manifestation," and "underwriting purpose." Conforming revisions have been made to "health care operations," and "payment."

HHS revised other provisions of the privacy rule to make clear the express prohibition on the use of genetic information for underwriting purposes. Section 164.502 clarifies that an authorization may not permit the use or disclosure of genetic information for underwriting purposes; amendments to §164.504 and §164.506 make clear the prohibition on disclosure of genetic information for underwriting purposes overrides other permissible disclosures, such as by a health plan to a plan sponsor.

Notice of Privacy Practices

As might be expected, the many changes in the final rule have an impact on the content of the Notice of Privacy Practices, as set out in §164.520. The privacy notice, as of the compliance date, must contain the following additional statements:

◆ A statement that the covered entity must obtain an authorization for the use and disclosure of psychotherapy notes, marketing, and the sale of PHI (§164.508(a)(2)–(a)(4); if the covered entity does not maintain psychotherapy notes, it does not need to include the statement;

◆ A statement that other uses and disclosures not described in the notice will be made only with the individual's written authorization;

◆ A statement that the individual may revoke an authorization as provided by §164.508(b)(5);

◆ If a covered entity intends to use PHI for fundraising, a statement to that effect;

◆ A statement that the covered entity intends to contact the individual for fundraising;

◆ A statement that the individual has the right to opt out of the fundraising contacts;

◆ A statement that the covered entity will not "sell" PHI without the individual's authorization

◆ A statement that the individual may restrict disclosure of PHI to a health plan where the individual has paid out-of-pocket in full for the services (only providers need include this statement);

◆ A statement of the individual's right to be notified after a breach of unsecured PHI (a simple statement is sufficient for this requirement);

◆ For health plans (except long-term care issuers), a statement that the health plan is prohibited from using or disclosing PHI that is genetic information of an individual for underwriting purposes.

HHS did not adopt the proposed addition to the privacy notice of a statement about marketing for which it is paid and the individual's right to opt-out. This statement was no longer relevant with the more stringent authorization requirements for marketing. It also no longer requires a statement that the covered entity may contact the individual to provide appointment reminders or information about treatment alternatives or other health-related benefits and services that may be of interest to the individual.

Section 164.520(b)(3) of the regulations requires covered entities to promptly revise and distribute their privacy notice if any change is material. According to HHS, the changes made by the final rule are material. However, HHS clarifies that providers may post the revised NPP in a prominent location and have copies available. While they still must give the notice (and obtain acknowledgement of receipt) to new patients, they do not need to redistribute the notice to all patients.

Health plans have specific requirements regarding notifying individuals of material changes, including those in the final rule. A health plan that posts its NPP on its website must prominently post the material changes to the notice or its revised notice by the effective date of the change (e.g., Sept. 23, the compliance date of this final rule) and provide either 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. Health plans that do not have websites 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. These requirements apply to all material changes including, where applicable, the rule

change adopted pursuant to GINA to prohibit most health plans from using or disclosing genetic information for underwriting purposes.

One statement of interest in the preamble is HHS's acknowledgement that some covered entities may need to comply with section 504 of the Rehabilitation Act of 1973 and/or the Americans with Disabilities Act of 1990. In these cases, the covered entity may have to offer alternative formats of the notice and any material changes, such as Braille, large print, or audio.

Individual Rights

Right to Request Restrictions

Before the final rule amendments, an individual was permitted to request that the covered entity restrict disclosure of his/her PHI for treatment, health care operations, and payment and to family members (§164.522(a)). Covered entities did not need to agree to the restriction, but if they did, they must abide by it.

Section 13405(a) of the HITECH Act adds a provision requiring the covered entity to comply with an individual's request to restrict disclosure to a health plan or its business associate for payment or health care operations if the individual, a family member, or another individual has paid in full out-of-pocket for the items or services in question. Payment from a flexible spending account or health savings account is considered out-of-pocket payment. Covered entities will need to design a way to flag the required restriction.

A covered entity does not need to comply with this restriction if the disclosure is required by law. Because of this exception, covered entities still may submit PHI to Medicare or Medicaid if requested for an audit, for example. However, the restriction applies if a Medicare beneficiary expressly refuses to submit a claim to Medicare and pays out-of-pocket because the provider is not required to submit a bill. Likewise, if state law requires submission of a claim to a health plan for the service received, and there is no procedure for the individual to pay out-of-pocket, then the disclosure is required by law.

Covered entities are not responsible for conveying the restriction to downstream covered entities. Providers may require payment up front from patients who request this restriction or where precertification from the health plan is required before treatment.

Right to Access

Prior to amendment, §164.524 of the regulations allowed individuals to access either paper or electronic designated record sets to review their PHI. Section 13504(e) of the HITECH Act requires a covered entity to provide an individual with a copy of his or her electronic health record in electronic form and to transmit the copy directly to another person designated by the individual. HHS used its authority to expand this provision and apply it to all electronic designated record sets, regardless of whether the designated record set is an EHR.

As amended, under §164.524(c)(2)(ii) covered entities now must provide the individual's electronic record in the form and format the individual requests, or if the form or format is not "readily producible," in a machine readable electronic form and format agreed upon by the covered entity and the individual. Covered entities may provide the electronic form and format that is currently available on their systems. However, if the covered entity maintains an electronic medical record but its system cannot produce an electronic copy for the individual, it may have to invest in a technology upgrade to meet this requirement. If the covered entity can produce an

electronic copy, but none of these is acceptable to the individual, the covered entity must provide a hard copy. A hard copy, however, does not as a general rule satisfy the requirement.

"Machine readable data" means digital information stored in a standard format enabling the information to be processed and analyzed by computer. For example, this would include providing the individual with an electronic copy of the protected health information in the format of MS Word or Excel, text, HTML, or text-based PDF, among other formats.

Covered entities may require the request to be in writing as long as they inform the individual of the requirement. They also may accept an oral request.

The electronic copy must contain all the PHI in the record, as well as any images or other data that are linked to the electronic designated record set.

Covered entities are not required to accept an external portable device, such as a jump drive, on which to download the record, but they cannot require an individual to purchase a portable media device from them. Instead, they must propose an alternative delivery system, such as an electronic copy attached to an email. The email does not need to be encrypted as long as the covered entity has advised the individual of the risk.

An individual may direct the covered entity to send the electronic record to a third party. However, this request must be in writing and clearly identify the recipient of the transmission. This request may be combined with a written request for the record itself. Covered entities must implement reasonable policies and procedures to verify the identity of the person requesting the information (§164.514(h)), as well as safeguards for the PHI itself (§164.530(c)). For example, the covered entity must confirm that it enters the email address for the delivery as it is presented in the request, but it does not need to confirm the accuracy of the email itself.

HHS clarified that this provision preempts any state law that restricts access to the medical record.

Business associate responsibilities for this provision are governed by the business associate agreement.

The privacy rule currently allows a covered entity to recover a reasonable, cost-based fee for a copy of the individual's PHI. The charges that may be included in the fee are based on supplies, labor, and postage and if a summary is included at the individual's request, labor for preparation of the summary.

Section 13405(e)(2) of the HITECH Act allows a covered entity to charge only for the labor costs associated with producing the copy of the electronic record. Therefore, covered entities will need to identify the labor costs separately for copying either paper or electronic records. (Labor costs do not include the time searching for and retrieving the information.)

For electronic records, labor costs included in a reasonable cost-based fee could include skilled technical staff time spent to create and copy the electronic file, such as compiling, extracting, scanning and burning PHI to media, and distributing the media. Labor costs also could include the time spent preparing an explanation or summary of the PHI (§164.524(c)(4)(i)).

The cost of supplies for creating the paper copy or electronic media (such as the cost of a CD) must be accounted for separately (§164.524(c)(4)(ii)).

Covered entities may charge for postage if the individual requests the covered entity to mail the media (§164.524(c)(4)(iii)).

State law limits on fees are relevant to determining a reasonable fee for a copy of the electronic record. If the covered entity's costs are lower than the state law limit, then the reasonable fee is that which is incurred by the covered entity; if the covered entity's costs are higher than the limit, then the reasonable fee is the state limit.

Covered entities may not charge the actual labor costs associated with the retrieval of electronic information despite the indication in the proposed rule that this may be permitted.

If an individual requests an affidavit certifying that the information is a true and correct copy, usually required for litigation or other legal purposes, the covered entity may charge for the preparation as HHS does not view this as a "copying cost."

HHS revised the timeliness standard in §164.524(b) as applied to both paper and electronic records. Prior to amendment, a covered entity had to approve or deny a request for access and if approved, allow access within 30 days of the request unless the records are off site, in which case the regulations allow another 30 days and under extenuating circumstances, another 30 day extension.

Section 164.524(b) now will permit a total of 60 days for response rather than 90 — 30 days for action on the original request and another 30-day extension under extenuating circumstances.

HHS Enforcement Rules

In the final rule, HHS amends many provisions in the enforcement regulations (45 CFR Part 164, Subparts C and D) to reflect provisions in section 13410 of the HITECH Act. That section mandates stronger enforcement of HIPAA by HHS, particularly of violations due to willful neglect, and replaces the civil monetary penalty provisions with a tiered structure. The revisions state that HHS now will (rather than may) investigate any complaint when a preliminary review of the facts suggests a violation due to willful neglect (§164.306). The department also will conduct a compliance review when a preliminary review of the facts suggests that a covered entity or business associate is not in compliance due to willful neglect (§164.308). The department, HHS explains, generally uses a compliance review when the allegations of violations are not raised by a complaint. Section 160.312 also has been amended to state that the secretary *may* use informal means to resolve a violation, which allows HHS to proceed with a willful neglect determination and move directly to a civil money penalty.

The HITECH Act not only requires stronger enforcement but also establishes a four-tiered penalty scale based on the severity of the violation. HHS has amended the definition of "reasonable cause" to make clear the state of mind applicable to the second penalty tier — violations due to reasonable cause and not willful neglect. The definition now reads "an act or omission in which a covered entity or business associate knew, or by exercising reasonable diligence would have known, that the act or omission violated an administrative simplification provision, but in which the covered entity or business associate did not act with willful neglect." The revised definition captures "violations due both to circumstances that would make it unreasonable for the covered entity or business associate, despite the exercise of ordinary business care and prudence, to comply with the administrative simplification provision violated, as well as to other circumstances in which a covered entity or business associate has knowledge of a violation but lacks the conscious intent or reckless indifference associated with the willful neglect category of violations."

Section 160.402, "Basis for a civil monetary penalty," has been amended to authorize a penalty against a covered entity or a business associate for the acts of their agents, which is consis-

tent with the federal common law of agency. HHS explains in the preamble to the rule that the analysis of whether a business associate is an agent will take into account the terms of a business associate agreement as well as all the circumstances in the relationship between the parties. Four factors are important:

(1) The time, place, and purpose of a business associate agent's conduct;

(2) Whether a business associate agent engaged in a course of conduct subject to a covered entity's control;

(3) Whether a business associate agent's conduct is commonly done by a business associate to accomplish the service performed on behalf of a covered entity; and

(4) Whether the covered entity reasonably expected that a business associate agent would engage in the conduct in question. It offers the following guidance to distinguish agency from non-agency:

> The essential factor in determining whether an agency relationship exists between a covered entity and its business associate (or business associate and its subcontractor) is the right or authority of a covered entity to control the business associate's conduct in the course of performing a service on behalf of the covered entity. The right or authority to control the business associate's conduct also is the essential factor in determining whether an agency relationship exists between a business associate and its business associate subcontractor.
>
> The authority of a covered entity to give interim instructions or directions is the type of control that distinguishes covered entities in agency relationships from those in non-agency relationships. A business associate generally would not be an agent if it enters into a business associate agreement with a covered entity that sets terms and conditions that create contractual obligations between the two parties. Specifically, if the only avenue of control is for a covered entity to amend the terms of the agreement or sue for breach of contract, this generally indicates that a business associate is not acting as an agent. In contrast, a business associate generally would be an agent if it enters into a business associate agreement with a covered entity that granted the covered entity the authority to direct the performance of the service provided by its business associate after the relationship was established. For example, if the terms of a business associate agreement between a covered entity and its business associate stated that "a business associate must make available protected health information in accordance with §164.524 based on the instructions to be provided by or under the direction of a covered entity," then this would create an agency relationship between the covered entity and business associate for this activity because the covered entity has a right to give interim instructions and direction during the course of the relationship. An agency relationship also could exist between a covered entity and its business associate if a covered entity contracts out or delegates a particular obligation under the HIPAA Rules to its business associate.

The final rule makes no changes to §160.404, which sets out the amount of the penalty for each penalty tier. However, HHS explains how it intends to count violations. If multiple individuals are affected by one violation, such as a breach of unsecured PHI, then the number of affected individuals will be counted. For continuing violations, such as a lack of safeguards, the violation will be counted on a per-day basis. HHS points out that in breach cases there may

be more than one type of violation, such as an impermissible use or disclosure and a safeguard violation, and emphasizes that it may calculate separate civil penalties for each type of violation. This could result in covered entities or business associates reaching the $1.5 million penalty cap for each type of violation, which would result in a total penalty of more than $1.5 million.

The final rule also revises the list of factors in §160.408 that HHS must consider to determine the amount of the penalty. It now lists four main factors with a number of subfactors under each, as follows:

(1) The nature and extent of the violation, consideration of which may include

◆ The number of individuals affected, and

◆ The time period during which the violation occurred.

(2) The nature and extent of the harm resulting from the violation, consideration of which may include but is not limited to:

◆ Whether the violation caused physical harm;

◆ Whether the violation resulted in financial harm;

◆ Whether the violation resulted in harm to an individual's reputation; and

◆ Whether the violation hindered an individual's ability to obtain health care.

(3) The history of prior compliance with the administrative simplification provisions, including violations, by the covered entity or business associate, consideration of which may include but is not limited to:

◆ Whether the current violation is the same or similar to previous indications of noncompliance;

◆ Whether and to what extent the covered entity or business associate has attempted to correct previous indications of noncompliance;

◆ How the covered entity or business associate has responded to technical assistance from the Secretary provided in the context of a compliance effort; and

◆ How the covered entity or business associate has responded to prior complaints.

(4) The financial condition of the covered entity or business associate, consideration of which may include but is not limited to:

◆ Whether the covered entity or business associate had financial difficulties that affected its ability to comply;

◆ Whether the imposition of a civil money penalty would jeopardize the ability of the covered entity or business associate to continue to provide, or to pay for, health care; and

◆ The size of the covered entity or business associate; and

◆ Such other matters as justice may require.

The final rule amends §164.410, "Affirmative defenses," and §164.412, "Waiver," to specify the time periods to which the penalties apply.