AMA
AMERICAN MEDICAL ASSOCIATION

# The Health Insurance Portability and Accountability Act (HIPAA) Omnibus Final Rule Summary

The federal government has published its long awaited final regulations implementing the "Health Information Technology for Economic and Clinical Health (HITECH) Act," enacted as part of the "American Recovery and Reinvestment Act of 2009" (ARRA), described by the head of the Office for Civil Rights (OCR) in the Department of Health and Human Services (HHS) as "the most sweeping changes to the HIPAA Privacy and Security Rules since they were first implemented." In general, the new rules expand the obligations of physicians and other health care providers to protect patients' protected health information (PHI), extend these obligations to a host of other individuals and companies who, as "business associates," have access to PHI, and increase the penalties for violations of any of these obligations. The American Medical Association (AMA) will be publishing more detailed guidance concerning the impact of these rules on physicians. The following outlines the changes physicians will need to consider as they implement the new HIPAA requirements necessary by the September 23, 2013, compliance date.

There are three areas that physicians will need to focus on to comply with the new rules:

- Privacy, Security, and Breach Notification policies and procedures (and in some cases, new workflows and forms);
- Notice of Privacy Practices (NPP); and
- Business Associate (BA) Agreements.

The following summary provides a helpful overview of the steps physicians will need to take in each of these areas to meet the new requirements. Physicians also should be familiar with their state patient privacy and confidentiality laws, which may be more stringent than HIPAA.

## Privacy and Security Policies and Procedures

The new rules will likely require changes to a physician practice's HIPAA policies and procedures in at least the following areas:

- Breach notification requirements – The obligation to notify patients if there is a breach of their PHI is expanded and clarified under the new rules. Breaches are now presumed reportable unless, after completing a risk analysis applying four factors, it is determined, that there is a "low probability of PHI compromise." The physicians must consider **all** of the following four factors:
    - the nature and extent of the PHI involved – issues to be considered include the sensitivity of the information from a financial or clinical perspective and the likelihood the information can be re-identified;
    - the person who obtained the unauthorized access and whether that person has an independent obligation to protect the confidentiality of the information;
    - whether the PHI was actually acquired or accessed, determined after conducting a forensic analysis; and
    - the extent to which the risk has been mitigated, such as by obtaining a signed confidentiality agreement from the recipient.

This rebuttable presumption of breach and four factor assessment of the "risk of PHI compromise" replaces the previous, more subjective "significant risk of financial, reputational, or other harm" analysis for establishing a breach. The new rules further clarify that there is no need to have an independent entity conduct the risk assessment and indeed, no risk assessment need be conducted at all if the breach notification is made (although, physicians will want to undertake an appropriate review and steps to mitigate the harm and reduce the likelihood of future breaches in any case). The new rules further confirm that the breach notification requirement may be delegated to a BA, and physicians are encouraged to coordinate with their BAs so that patients receive only one notification of the breach.

The new rules do not modify the actual reporting and timeframe requirements for Breach Notification; that is, covered entities must still adhere to requirements for individual notification, HHS notification, and where applicable media posting of the breach.

- Disclosures to health plans – At the patient's request, physicians may not disclose information about care the patient has paid for out-of-pocket to health plans, unless for treatment purposes or in the rare event the disclosure is required by law. This change updates the previous HIPAA Privacy Rule governing patient requests for restrictions on the use or disclosure of their PHI. Previously, while physicians could refuse to abide by any such request, the new rule *requires* physicians and other health care providers to abide by a patient's request not to disclose PHI to a health plan for those services for which the patient has paid out-of-pocket and requests the restriction. Of all the changes made by the new rules, this change is likely to have the greatest impact on physician practice workflow both in terms of documentation and follow up to ensure the restriction is adhered to.

- Marketing communications – The new rules further limit the circumstances when physicians may provide marketing communications to their patients in the absence of the patient's written authorization. Generally speaking, the only time a physician may tell a patient about a third-party's product or service without the patient's written authorization is when: 1) the physician receives no compensation for the communication; 2) the communication is face-to-face; 3) the communication involves a drug or biologic the patient is currently being prescribed and the payment is limited to reasonable reimbursement of the costs of the communication (no profit); 4) the communication involves general health promotion, rather than the promotion of a specific product or service; or 5) the communication involves government or government-sponsored programs. Physicians are also still permitted to give patients promotional gifts of nominal value (e.g., pamphlet).

- Sale of PHI – The new rules clarify that the prohibition on the sale of PHI in the absence of the patient's written authorization extends to licenses or lease agreements, and to the receipt of financial or in-kind benefits. It also includes disclosures in conjunction with research if the remuneration received includes any profit margin. On the other hand, the prohibition on PHI sales does not extend to permitted disclosures for payment or treatment nor to permitted disclosures to patients or their designees in exchange for a reasonable cost-based fee.

- Childhood immunizations – Under the new rules, physicians may disclose immunizations to schools required to obtain proof of immunization prior to admitting the student so long as the physicians have and document the patient or patient's legal representative's "informal agreement" to the disclosure.

- Decedents – The new rules allow physicians to make relevant disclosures to the deceased's family and friends under essentially the same circumstances such disclosures were permitted when the patient was alive; that is, when these individuals were involved in providing care or payment for care and the physician is unaware of any expressed preference to the contrary. The new rule also eliminates any HIPAA protection for PHI 50 years after a patient's death.

- Copies of e-PHI – Physicians will now have only 30 days to respond to a patient's written request for his or her PHI with one 30-day extension, regardless of where the records are kept (eliminating the longer 60-day timeframe for records maintained offsite). They must provide access to EHR and other electronic records in the electronic form and format requested by the individual if the records are "readily reproducible" in that format. Otherwise, they must provide the records in another mutually agreeable electronic format. Hard copies are permitted only when the individual rejects all readily reproducible e-formats.

- Emailing PHI – Physicians must also consider transmission security, and may send PHI in unencrypted emails only if the requesting individual is advised of the risk and still requests that form of transmission.

- Charging for copies of e-PHI or PHI – The new rules modify the costs that may be charged to the individual for copies to include labor costs (potentially to include skilled technical labor costs for extracting electronic PHI and supply costs if the patient requests a paper copy, or if electronic, the cost of any portable media (such as a USB memory stick or a CD)), assuming state law does not set a lower reimbursement rate. The rules also clarify that physicians may impose a separate charge for creating an affidavit of completeness.

- Research authorizations – The new rules permit physicians to combine conditioned and unconditioned authorizations for research participation, provided individuals can opt-in to the unconditioned research activity. Moreover, these authorizations may encompass future research.

## Notice of Privacy Practices (NPP)

Physicians must amend their NPPs to reflect the changes set forth above, including those related to breach notification, disclosures to health plans, and marketing and sale of PHI. To the extent physicians engage in fundraising, they will also have to amend their NPP to inform patients of their right to opt-out of those communications. As the rules presume these are all material changes, physicians will have to post the revised NPP, and make copies available at their office, to all new patients and to anyone else on request. Physicians who maintain a website are cautioned to post the updated NPP on their website as required by the existing HIPAA Privacy rule. The new rules also eliminate requirements to include information on communications concerning appointment reminders, treatment alternatives, or health-related benefits or services in NPPs, but the rules do not require that that information be removed either.

## Business Associates (BAs)

The new rules expand the universe of individuals and companies that must be treated as business associates to include Patient Safety Organizations and others involved in patient safety activities, health information organizations like e-prescribing gateways or health information exchanges that transmit and maintain PHI, and personal health record vendors physicians sponsor for their patients. Thus, physicians must review their relationships and determine if they must enter new BA agreements with these entities or others that create, receive, store, maintain, or transmit PHI on their behalf.

These rules also modify the requirements for BA agreements:

- Physicians no longer must report failures of their BAs to the government when termination of the agreement is not feasible, as HHS has concluded that the BA's direct liability for these violations is sufficient.
- BAs are now responsible for their subcontractors.
- BAs must comply with the Security and Breach Notification Rules.
- Physicians are liable for the actions of their BAs who are agents, but not for the actions of those BAs that are independent contractors.

**Physicians have until September 23, 2014, to bring all their BA agreements into conformance with the new rules.** BA agreements that have not been renewed or modified between March 26, 2013, and September 23, 2013, will be deemed compliant until the date the BA agreement is renewed or modified or until September 22, 2014, whichever is earlier.

## Enforcement and Penalties

The new rules clarify the four penalty tiers as follows:

- Lowest tier – cases in which the physician did not and reasonably could not know of the breach.
- Intermediate tier – cases in which the physician "knew, or by exercising reasonable diligence would have known" of the violation, but the physician did not act with willful neglect.
- Highest tiers – cases in which the physician "acted with willful neglect" and either corrected the problem within the 30-day cure period, or failed to make a timely correction.

HHS must conduct a formal investigation and impose civil monetary penalties in cases involving willful neglect, and is now free to provide PHI to other government agencies for enforcement activities. The assessment of penalties must be based on five principal factors: (1) the nature and extent of the violation, including the number of individuals affected; (2) the nature and extent of the harm resulting from the violation, including reputational harm; (3) the history and extent of prior compliance; (4) the financial condition of the covered entity or business associate; and (5) such other matters as justice may require. The number of violations may be based on the number of individuals affected or by the number of days of non-compliance.

The rule further clarifies that the 30-day cure period begins when the physician knew or

should have known of the violation.

## Other Changes

The new rules also make changes that will likely affect physicians, but only indirectly. The most sweeping is the expansion of the obligations of BAs to include both direct liability under most of the HIPAA Privacy and Security Rules, and the obligation to enforce these rules with respect to their subcontractors. The new rules also implement the Genetic Information Nondiscrimination Act (GINA), which generally prohibits health plans from using genetic information for underwriting purposes.

## Next Steps

With the potential for $1.5 million fines, not to mention serious reputational injury, these new rules must be taken seriously. Clearly, physicians will need to develop a plan to make these required changes in a timely fashion. The AMA will provide more specific guidance with respect to each of these three areas, including sample NPP and BA agreements.