HIPAA Omnibus Rule: What Anesthesiologists Must Do Now

Neda M. Ryan, Esq.
Clark Hill, PLC, Birmingham, MI

On January 25, 2013, the US Department of Health and Human Services (HHS) Office of Civil Rights (OCR) issued its long-awaited Health Insurance Portability and Accountability Act of 1996 (HIPAA) final omnibus regulations (Final Rule). The Final Rule modified the HIPAA Privacy, Security, Enforcement and Breach Notification Rules (HIPAA Rules) and is comprised of four sub-rules:

1. Final modifications to the HIPAA Privacy, Security, and Enforcement Rules mandated by the Health Information Technology for Economic and Clinical Health (HITECH) Act;
2. A final rule adopting changes to the HIPAA Enforcement Rule to incorporate the increased and tiered civil money penalty structure as set forth by HITECH;
3. A final Breach Notification rule; and
4. A final rule modifying the Privacy Rule as required by the Genetic Information Nondiscrimination Act (GINA).

While the Final Rule is effective March 26, 2013, compliance with the provisions of the Final Rule is not required until September 23, 2013. This eight month window between the release date and the compliance date allows covered entities, including anesthesiologists, time to understand their roles under the Final Rule, and take action where necessary to ensure compliance by September 23. This article summarizes some of the key elements of the Final Rule applicable to anesthesiologists and their practices.

Business Associates

The Final Rule renews a focus on business associates and their subcontractors, beginning with revising the definition of "business associate." Business associates are now defined as those persons (other than members of the covered entity's work force) or entities that perform certain functions or activities that involve the creating, receiving, maintaining or transmitting of protected health information (PHI) for a specified function or activity (*e.g.*, claims processing or administration, data analysis, processing, or administration utilization review, quality assurance, patient safety activities, billing, benefit management, practice management, re-pricing). Additionally, the Final Regulations specify that a business associate includes the following:

- A health information organization, e-prescribing gateway, or other person or entity that provides data transmission services with respect to PHI to a covered entity and that requires access on a routine basis to such PHI;
- A person offering a personal health record to one or more individuals on behalf of a covered entity; and
- A subcontractor that creates, receives, maintains or transmits PHI on behalf of a business associate.

Specifically excluded are healthcare providers to whom a covered entity discloses PHI for purposes of treating the individual, plan sponsors to whom a group health plan makes disclosures, a government agency determining eligibility for or enrollment in a government health plan, and a covered entity participating in an organized health care arrangement that performs certain functions.

Consistent with previous regulations and practice, covered entities must enter into Business Associate Agreements with business associates. The Business Associate Agreements must meet specific requirements, and set forth the parameters within which business associates may use and disclose PHI. Covered entities are not required to enter into direct agreements with subcontractors of their business associates. The responsibility has been placed on the business associates to ensure a contractual relationship exists between them and subcontractors that ensure compliance with the HIPAA Rules.

In line with the new focus on business associates and subcontractors, the Final Rule specifies that business associates and their subcontractors may be *directly liable* for certain Privacy and Security Rule violations. Therefore, busi-

ness associates and their subcontractors must ensure full compliance with HIPAA.

Notice of Privacy Practices

Covered entities must modify their Notice of Privacy Practices (Notice) to comply with changes in the Final Rule. Notice is required to communicate to the individual the ways in which the covered entity may use and disclose PHI, the covered entity's duties with respect to protection of the PHI and the individual's rights relative to his/her PHI. Typically, Notices must be delivered to patients not later than on their first encounter, and must be posted in a clear and prominent place on the covered entity's website.

The Final Rule does not require the Notice to include a list of all situations requiring authorization. Rather, the Notice must contain a statement indicating that most uses and disclosures of psychotherapy notes (where appropriate), uses and disclosures of PHI for marketing purposes, and disclosures that constitute a sale of PHI require authorization, as well as a statement that other uses and disclosures not described in the Notice will be made only with authorization from the individual. Moreover, if the covered entity intends to contact an individual for the purpose of fundraising for the covered entity, the Notice must contain a statement regarding fundraising communications and the individual's right to opt out of receiving such communications. Finally, the Notice must contain a statement that affected individuals have the right to be notified following a breach of their unsecured PHI.

Pursuant to the changes in the Final Rule, anesthesiologists should review their Notices and update them as necessary to reflect the new requirements—or at least verify that the facility in whose Notice anesthesia is included is updated. Notices should also be updated on any websites that the practice may have. While existing patients do not need to receive a copy of the updated Notice, they must be made available upon request. As always, it is prudent to document in the patient's file when Notices are given to them.

Individual Access to PHI

Except for limited circumstances, individuals have the right to receive and review a copy of their PHI in a designated record set. With certain exceptions, a designated record set is made up of the records maintained by or for the covered entity that is used, in whole or part, to make decisions about that individual, or that is a provider's medical and billing records about that individual.

The Final Rule requires, for PHI maintained electronically, upon an individual's request for an electronic copy of his/her PHI, the covered entity must provide that individual with access to the electronic information, in the electronic form and format requested by the individual, if it is readily producible. If the information is not readily producible, it must be delivered in a readable electronic format (*e.g.*, MS Word or Excel, text, HTML, or text-based PDF) that is agreed to by the covered entity and the individual. Individuals must be given access to their records within 30 days of the request, regardless of whether the records are in paper or electronic format and whether paper records are stored off-site. Notwithstanding this timeframe, covered entities will have an opportunity for a one-time extension of 30 days.

Anesthesiologists maintaining electronic records should be reviewing their HIPAA policies to ensure they reflect this change in the HIPAA Rules. Moreover, anesthesiologists must ensure that they can grant patients' access to their PHI within 30 days of the request.

Requesting Restrictions on Uses and Disclosures

Individuals have the right to request restrictions on the use and disclosure of their PHI for treatment, payment or operations (reasons for which a covered entity is generally not required to obtain authorization for the use and disclosure of an individual's PHI), disclosures to those who are involved in the individual's care or payment for care, or disclosures to family members. A covered entity is not under an obligation to grant this request; however, those covered entities agreeing to comply must abide by the restrictions.

The Final Rule expands the individual's right to request restrictions without the covered entity's right to deny the request. Specifically, for individuals who have paid the healthcare provider in full out-of-pocket, healthcare providers must grant requests to restrict disclosures to the individual's health plan.

While certain uses and disclosures are required by law and thus cannot be circumvented by an individual requesting restrictions, anesthesiologists should review and revise their policies and procedures with respect to individuals' access to their own PHI. Moreover, any forms used to process such requests must also be reviewed and revised, as necessary. For those anesthesiologists who have not been in the practice of granting restrictions, they must develop a process to comply with requests by private pay patients requesting restrictions on information disclosed to their health plans.

Continued on page 10

HIPAA Omnibus Rule: What Anesthesiologists Must Do Now

Continued from page 9

Breach Notification

In addition to the modifications listed above, the rules pertaining to breach notification were considerably amended. Prior to the Final Rule, "breach" was defined as a use or disclosure of PHI that posed a significant risk of financial, reputational, or other harm to the individual. A breach was presumed if the impermissible use or disclosure resulted in harm to the individual.

However, the standard by which "breach" is measured significantly changed under the Final Rule from a "risk of harm" standard to a "low probability that PHI has been compromised" standard. In other words, an impermissible use or disclosure of PHI is presumed to be a breach unless it has been demonstrated that there is a low probability that the PHI has been compromised. Therefore, breach notification is necessary in all situations, unless it is demonstrated that there is a low probability that the PHI has been compromised or an exception applies.

To determine whether the low probability standard has been met, the OCR set four factors that must be considered when performing a risk assessment:

a. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification of the information;
b. The unauthorized person who impermissibly used the PHI or to whom the disclosure was made;
c. Whether the PHI was actually acquired or viewed or, alternatively, if only the opportunity existed for the information to be acquired or viewed; and
d. The extent to which the risk to the PHI has been mitigated.

Following consideration of the factors, the risk assessment must evaluate the overall probability that the PHI has been compromised.

In addition to revising the definition of breach, the requirement that the Secretary be notified of breaches involving fewer than 500 individuals was revised. Because some breaches may go undetected for long periods of time, notification must be made to the Secretary within 60 calendar days after the end of the year in which the breach was discovered.

Investigations and Penalties

The Final Rule requires the OCR to investigate any complaint of a HIPAA violation when a preliminary review of the facts indicates that there may be a violation due to willful neglect. Willful neglect is defined as conscious, intentional failure or reckless indifference to the obligation to comply with the provision violated. The OCR may exercise its discretion in conducting a compliance review or complaint investigation in instances where culpability may be less than a willful neglect.

Importantly, the Final Rule increases the Secretary's discretion to choose between an informal and formal resolution of investigations or compliance reviews. This change allows the Secretary to impose civil monetary penalties without pursing an informal resolution process (previously, an informal process was required to attempt to resolve issues involving noncompliance).

In 2009, the HIPAA tiered penalties were incorporated into the HIPAA Rules pursuant to HITECH. Violations of the HIPAA Rules could result in penalties of up to $1.5 million. In determining the amount of any civil monetary penalty, the Final Rule sets forth the following four factors to be considered:

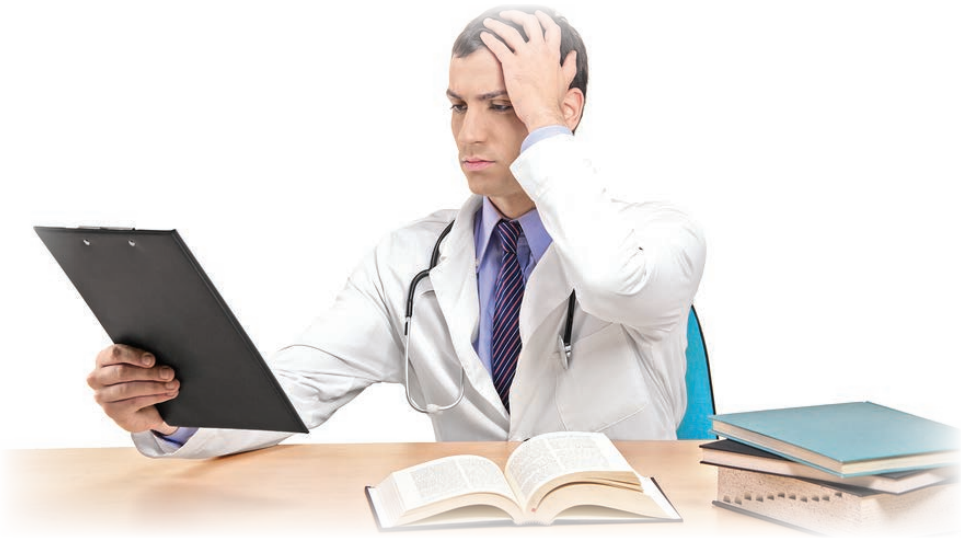
1. The nature of the violation;
2. The nature and extent of the resulting harm;
3. The history of prior compliance with HIPAA; and
4. The financial condition of the covered entity or business associate.

Reality Check – HIPAA Enforcement is On the Rise

If the increased penalties and flexibility by the Secretary to impose the

TABLE 1

Violation Category	Each Violation	All Such Violations of an Identical Provision in a Calendar Year
For violations in which it is established that the covered entity or business associate ***did not know*** and, by exercising reasonable diligence, would not have known that the covered entity violated a provision	$100-$50,000	$1,500,000
For a violation in which it is established that the violation was due to ***reasonable cause*** and not to willful neglect	$1,000-$50,000	$1,500,000
For a violation in which it is established that the violation was due to ***willful neglect and was timely corrected***	$10,000-$50,000	$1,500,000
For a violation in which it is established that the violation was due to ***willful neglect and was NOT timely corrected***	$50,000	$1,500,000



penalties is not alarming enough, enforcement is a very real issue that many covered entities face. A sampling of some of the settlements that have occurred in the last year include the following:

- January 2, 2013 – A $50,000 settlement with a hospice, arising out of a stolen laptop containing over 400 patients' PHI (notably, this settlement represents the first HIPAA breach settlement involving less than 500 individuals)
- June 26, 2012 – A $1.7 million settlement with Alaska Medicaid arising out of a report to HHS involving a stolen thumb drive containing PHI of more than 500 Alaska Medicaid beneficiaries
- May 24, 2012 – A $750,000 settlement with a Massachusetts hospital arising out of a report of disclosures made to the Attorney General regarding 473 unencrypted data tapes that were sent to a third party to be erased, but only one of the three boxes of tapes arrived
- April 17, 2012 – A $100,000 settlement with a physician group arising out of a report to HHS that the physician practice was posting clinical appointments for its patients on publicly accessible website calendar
- March 13, 2012 – A $1.5 million settlement with a private insurance company arising out of disclosures made under the Breach Notification Rule involving the theft of 57 unencrypted computer hard drives from a data closet

An in-depth review of the facts of each of these cases revealed that the main cause for the civil penalties was what the OCR found during the investigation. Most of the time, the investigation revealed significant deficiencies in compliance that may not have been directly related to the initial complaint.

In light of its recent pilot audit program and continuous press releases regarding settlements and penalties, the OCR is ramping up its HIPAA enforcement and no covered entity is immune from scrutiny.

What You Can Do Now

While the Final Rule does not significantly alter the way anesthesiologists have been operating under HIPAA in recent years, it does signal a need for groups to revisit their HIPAA policies and procedures, update them as necessary, and educate their workforce on those updates. The following are some specific steps anesthesia practices should be taking now:

- Review, revise, and update HIPAA policies and procedures as more specifically described in this article;
- Identify which relationships will fall under the definition of "business associate" and ensure that there is a Business Associate Agreement with that entity;
- For those relationships previously identified as being that of a business associate relationship, ensure the Business Associate Agreement complies with the updated regulations;
- Review and update, as necessary, the Notice to properly reflect new requirements of the Final Rule; and
- Ensure all members of your group and workforce are educated on the new requirements and policies, and be sure to document the date of the education and who attended.

While these recommendations are specific to the revisions in the Final Rule, all anesthesia groups should regularly engage in self-audits of their compliance with their HIPAA policies and procedures, update the HIPAA policies and procedures to reflect deficiencies discovered in audits, and regularly educate the group and its workforce on the HIPAA policies and procedures and any updates that have been made. Taking these steps and documenting them will best position a group if and when it is audited or investigated by the OCR.

Neda M. Ryan, Esq. is an associate with Clark Hill, PLC in the firm's Birmingham, MI office. Ms. Ryan practices in all areas of health care law, assisting clients with transactional and corporate matters; representing providers and suppliers in health care litigation matters; providing counsel regarding compliance and reimbursement matters; and representing providers and suppliers in third party payor audit appeals. She can be reached at (248) 988-5884 or at nryan@clarkhill.com.