LEGISLATION

Gerry Blass and Susan A. Miller, JD

All Aboard the Omnibus

A Look at HIPAA's First Update in 10 Years

By Gerry Blass and Susan Miller, JD

On January 25, 2013, the Office for Civil Rights (OCR) published their long-awaited updates to the Health insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules. The formal name of the rules is "Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule," known to those who must implement its provisions and deal with its enforcement as the Omnibus Rule.

The new rules are the first update of the HIPAA Privacy and Security Rules since the original regulations were published more than 10 years ago. The Omnibus Rule combines, updates, and makes final four rules:

- July 2010 Notice of Proposed Rule Making (NPRM) on HITECH [Health Information Technology for Economic and Clinical Health Act] privacy and security changes to HIPAA.
- October 2009 Notice of Proposed Rule Making (NPRM) on Genetic Information Nondiscrimination Act (GINA) changes to HIPAA.
- August 2009 Interim Final Rule (IFR) on HIPAA Breach Notification.
- October 2009 Interim Final Rule (IFR) on HIPAA Enforcement Rule.

The Omnibus Final Rule was effective on March 26, 2013, and the compliance date is September 23, 2013. Covered entities (CEs) and business associates (BAs) of all sizes will have only the 180 days beyond the effective date of the final rule to come into compliance with most of the final rule's provisions, including the modifications to the Breach Notification Rule and the changes to the HIPAA Privacy Rule under GINA. Some of the BA Agreements may have time beyond the 180 days.[1]

IMPACT

Since the publication of the Omnibus Rule, Leon Rodriguez, Director of OCR, has been out talking about the changes. He said "the most important change is that HIPAA enforcement is now directly applied to Bas, as many of the HIPAA breaches are from BAs," at the American Health Lawyers Association (AHLA) Omnibus Rule Meeting on March 22, 2013, in Baltimore. He also said "OCR sees the HIPAA Rules as fraud and abuse regulations."

So, the OCR focus in 2013 will not just be the implementation of the new and updated requirements under the Omnibus Rule, but the aggressive enforcement that began immediately with the October 2009, publication of the Enforcement Interim Final Rule (IFR); since 2009, there have been five fines between $1.5 million and $4.3 million.

Something else that has not changed—just as in the first HIPAA regulations the sections under the Omnibus Rule include new or updated definitions that are part of the scope of the HIPAA requirements and need to be considered during implementation and enforcement of the new and changed Omnibus Rule requirements.

WHAT HAS CHANGED?

The Omnibus Rule changes include:

- BAs are now directly responsible for *all* the HIPAA Security standards, implementation specifications and requirements.
  - BAs will now need to do a risk analysis by conducting a thorough assessment of the potential risks and vulnerabilities.
- BAs are now directly responsible in the HIPAA Privacy requirements, in § 164.502, Uses and disclosures of protected health

THE NEW RULES ARE the first update of the HIPAA Privacy and Security Rules since the original regulations were published more than 10 years ago.

information: General rules, including Minimum Necessary, and .§ 164.504, Uses and disclosures: Organizational requirements.

- Subcontractors are now BAs.
- BAs now face direct enforcement.
- The definition of BA has changed to an entity that "...creates, receives, maintains, or transmits [PHI, protected health information] for a function or activity regulated by [HIPAA]..." on behalf of a CE.
- BAs must notify any and all CEs of a breach. (A breach is an unauthorized acquisition, access, use disclosure of unsecured PHI in a manner not permitted by the HIPAA Privacy Rule that compromises the security or privacy of PHI).
- There is now a presumption in the breach definition—the compromise of the security or privacy is considered to be presumed, unless there is a demonstrated low probability that the PHI has not been compromised using four factors in the definition for a *breach risk assessment*.

1. What PHI: Nature and extent of PHI involved.
2. Who: The unauthorized person who used the PHI or to whom the disclosure was made.
3. Acquired: Whether the PHI actually was acquired or viewed.
4. Mitigation: The extent to which the risk to the PHI has been mitigated.

- Increased enforcement includes a new focus on willful neglect; and substantially increased fines; willful neglect is defined as the conscious, intentional failure, or reckless indifference to the obligation to comply with HIPAA.
  - OCR will now investigate all cases of possible neglect.
  - OCR will now impose penalty on all violations due to willful neglect.
- Individual rights includes two significant changes that will impact a CE's Notice of Privacy Practices.
  - A healthcare provider who is paid in full for the services provided to an individual may request a restriction and the provider must agree to not tell the health payer and any of the health plan's BAs.
  - A patient or member may request *access* not only to paper records, but to electronic PHI held in a designated record set, and the provider or health plan must also send to a third party if the individual so requests.
- Uses and disclosures—there are updates to marketing, sale of PHI, and fundraising; these are definitional changes that will have impacts on Notice of Privacy Practices.
- GINA—genetic information is a new kind of 'sensitive data'; the definitions of health plan and health information have been updated, and there are new definitions for family member, genetic information, genetic services and genetic test.

WHAT DO CES AND BAS NEED TO DO NOW?

Since 2009, the OCR has stated that CEs and BAs should have a robust HIPAA

THE AUTHORS ARE SEEING a major uptick in the numbers of CEs and BAs who are now more focused on implementing a HIPAA-HITECH program to reduce the risk of unauthorized access to PHI.

Privacy and Security Compliance Program, including:

- Periodic workforce training.
- Vigilant implementation of policies and procedures.
- A prompt plan to respond to incidents and breaches.
- Regular internal audits.

Now there is no doubt that the OCR is aggressively enforcing the HIPAA Privacy, Breach Notification and Security Rules. CEs and BAs must therefore improve their HIPAA-HITECH program with a goal of creating and maintaining a culture of compliance within their organizations. CEs and BAs should update all their policies, procedures and plans that are impacted by the updates and changes in the Omnibus Rule that affects their organization, and train their workforce. CEs and BAs who have not done so already should conduct a baseline information privacy and security risk analysis and document a risk mitigation by September 23, 2013. BAs will be subject to OCR audits beginning in 2014, if not sooner.

In addition, CEs and BAs should have a security incident breach plan that includes:

- An incident response team.
- Readiness at all times to respond to news media attention—have a designated spokesperson.
- Encryption. Make the most of the encryption safe harbor, and verify document destruction.
- Audit access to PHI and enforce policies.

ONGOING

CEs and BAs should either conduct periodic self-audits of the HIPAA-HITECH Privacy, Security, and Breach Notification rules or engage an expert to conduct them, and organize all evidence of due diligence in order to be able to quickly respond to an OCR audit.

CONCLUSION

The authors are seeing a major uptick in the number of CEs and BAs who are now more focused on implementing a HIPAA-HITECH program to reduce the risk of unauthorized access to protected health information (PHI), and to document evidence of due diligence. CEs and BAs do not want to be on the Health & Human Services (HHS) PH breach "wall of shame." Both want to be able to respond quickly to an OCR audit with good evidence of due diligence. CEs want to be able to meet the Meaningful Use measure that requires an information security risk analysis. And, if all of the above isn't enough, CEs and BAs now have the Omnibus final rule, which is not exactly final. There is more to come regarding Minimum Use guidance and Accounting of Access/Disclosures. We have heard many times that the "only constant is change." CEs and BAs will therefore need to have HIPAA-HITECH programs in place that are re-evaluated periodically to account for organizational, environmental, technological and regulation changes. **JHIM**

Gerry Blass has more than 35 years of experience in healthcare IT and compliance. Blass provides IT and compliance consulting services and software called ComplyAssistant that automates the management and documentation of healthcare compliance activities. Gerry is the President & CEO of Blass Consulting and Compliance LLC.

Susan A Miller, JD, has 40 years of professional leadership experience spanning teaching, biochemistry research and law. Since 2002, Miller has provided independent consultation and legal services to numerous healthcare entities, including the National Institute of Standards and Technology (NIST) and HHS. She has co-authored two OCR audit protocol prep-books, HIPAA Security Audit Prep Book and HIPAA Breach & Privacy Audit Prep Book. They are published here.

Blass and Miller are co-founders of HIPAA 411, a linked-in group.

REFERENCES

1. See 45 CFR § 164.532(d)+(e), Transition Provisions.