SATINSKY CONSULTING

WINTER 2013 NEWSLETTER

This newsletter summarizes the highlights of the Final Omnibus HIPAA Privacy and Security Rule announced by the Department of Health and Human Services (DHHS) on January 17, 2013 and published in the Federal Register on January 25, 2013. The Rule modifies HIPAA Privacy, Security, and Enforcement Rules, implements statutory amendments under the HITECH Act of 2009, strengthens privacy and security protection for individuals' health information, modifies the Breach Notification Rule, and strengthens privacy protections for genetic information.

Margie Satinsky

Attend our February 21, 2013, 12:00 PM EST Tele-class on HIPAA Privacy and Security Rule Compliance, sponsored by InHealth Consulting & Educational Services (Efficiency in Practice series). Register now.

FINAL OMNIBUS HIPAA PRIVACY AND SECURITY RULE

1. What is HIPAA?

In 1996, the federal government passed the Health Insurance Portability and Accountability Act (HIPAA). Its purpose was to provide assurances that the healthcare system would keep personal health information private. The Administrative Simplification portion of the law had five parts: the Privacy Rule, Transactions and Code Sets Standards, the Security Rule, the Employer Identifier Standard, and the National Provider Identifier Standards. The HITECH Act of 2009, part of the American Recovery and Reinvestment Act (ARRA), both modified some of the provisions of the Privacy and Security Rules and added requirements. Other relevant statutes are the Interim Final Regulations on implementation of Breach Notification; Federal Trade Commission (FTC) Final Regulations on implementation of Breach Notification; the Interim Final Rule addressing Breach Notification and monetary penalties; the 2010 Notice of Proposed Rule Making; and the Genetic Information Nondiscrimination Act of 2008. The intent of the Final Omnibus Rule is to eliminate inconsistencies among some of these statutes and bring everything together.

2. Who are the important parties affected by HIPAA Privacy and Security?

Covered Entities (e.g., health plans, healthcare clearinghouses, or healthcare providers that transmit health information in electronic form); Business Associates acting as agents of covered entities, and subcontractors of Business Associates. When HIPAA first went into effect, emphasis was on the responsibilities and liability of Covered Entities. By 2009, there was more emphasis on Business Associates. Now the definition of Business Associate is broader and includes a person who creates, receives, maintains, or transmits PHI on behalf of a Covered Entity on a routine (as opposed to a random) basis. Business Associates must comply with all requirements of the Security Rule and with most but not all requirements of the Privacy Rule. The requirements for Business Associates apply to their subcontractors too, and it's the responsibility of the Business Associate, not the Covered Entity, to make sure that subcontractors are in compliance.

SATINSKY CONSULTING

3. What are the civil monetary penalties for non-compliance?

Four categories of violations reflect increasing levels of culpability and four tiers of penalty amounts. The penalty for each violation ranges from $100 to $50,000, and there is a $1.5 million maximum penalty per calendar year for an identical violation. The Office of Civil Rights (OCR), the enforcing agency, does not apply the maximum penalty in all cases. It considers an entity's financial condition, number of individuals affected, reputation, and prior indications of non-compliance and compliance.

4. How has enforcement changed since HIPAA went into effect?

First, DHHS now does a preliminary investigation of every complaint. If the preliminary review indicates a possible violation of HIPAA rules due to willful neglect, the investigation automatically proceeds. If the preliminary review does not show willful neglect, DHHS has the option of trying to achieve voluntary corrective action.

Penalties apply to Covered Entities, Business Associates, and subcontractors of Business Associates.

A 30-day cure period factors into the determination of the size of the penalty. The clock starts running at the time the entity (i.e., Covered Entity, Business Associate, or Subcontractor) learns of or should reasonably know of the problem.

There's a formal and proactive audit program in place. We know of several medical practices that attested to being HIPAA compliant when they applied for the financial incentive under Meaningful Use and are now targets for audit. Questionable HIPAA compliance may jeopardize their receipt of the money that they seek.

5. What is the compliance date for the Omnibus Final Rule?

The effective date of the Omnibus Rule is March 26, 2013. Compliance for both Covered Entities and Business Associates is 180 days from the effective date – i.e., September 23, 2013.

6. Should my practice revise its Notice of Privacy Practices (NPP) and redistribute it to patients?

Yes – there have been many changes since the passage of the HIPAA Privacy and Security Rules. Here are some of them. The NPP must have language regarding patient authorization for most uses and disclosures of psychotherapy notes, uses and disclosures of PHI for marketing purposes, and disclosures regarding the sale of PHI. There must also be a statement regarding patient authorization for uses and disclosures not specifically described in the NPP. New language must mention an individual's right to opt out of fundraising communications. Healthcare providers must clearly acknowledge their obligation to restrict use and disclosure to a health plan upon request by an individual who has paid out-of-pocket in full for a specific service.

Healthcare providers are not required to print and distribute a revised NPP. They must post the new NPP in a clear and prominent location and make copies available to those individuals who wish to take them. Providers may also post a summary of the revised NPP, provided that the full notice is also available. If patients have provided permission to receive practice information by email, the practice can send the revised NPP electronically.

7. How does the Omnibus Rule enhance the rights of individuals with respect to PHI?

The limitations on the use and disclosure of PHI for marketing and fundraising are stronger. Individuals can now request electronic copies of PHI, and Covered Entities must provide it in the form requested by the individual if readily producible, or in a readable form and format agreed to by the Covered Entity. Individuals can request transmission of a copy of PHI directly to a designated person. In such cases, the Covered Entity

must verify the identity of the individual making the request and take reasonable steps to ensure that the email address of the recipient is correct. Individuals who pay out of pocket in full for a service can restrict disclosure of that information to a health plan. To help parents and guardians, Covered Entities now have an easier process for disclosing proof of immunization to schools in those states that have school entry and other similar laws. There's greater clarity in the procedures for notifying individuals of a Breach. When individuals request PHI, Covered Entities must provide the requested information within 30 days, with a one-time 30-day extension.

8. How has the definition of a Breach changed, and what are the guidelines for determining and reporting a Breach?

Although the determination of a Breach remains more subjective than many in the health industry would like it to be, the Omnibus Rule modifies and clarifies the definition of Breach and the risk assessment approach. There's a new definition of a Breach: an impermissible use or disclosure of PHI unless the Covered Entity or Business Associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised. Rather than focusing on potential harm to the individual, the new language speaks to the responsibility of a risk assessment, performed by the Covered Entity or Business Associate, to assess the nature and extent of the PHI, the unauthorized person who used the PHI or to whom it was disclosed, whether or not the PHI was actually acquired or viewed, and the extent to which the risk has been mitigated. A common example of a possible Breach is a lost or stolen laptop computer. The loss or theft itself does not necessarily mean a Breach. If the owner can retrieve the laptop and forensically show that there was no Breach, then there's nothing to report. But if the laptop can't be retrieved, there is a Breach that must be reported to the individuals affected and possibly to CMS.

9. How does the Omnibus Rule modify the HIPAA Privacy Rule to protect genetic information as required by the Genetic Information Nondiscrimination Act (GINA) of 2008?

GINA prohibits discrimination based on an individual's genetic information in health coverage and employment contexts. Genetic information is defined as the genetic tests of an individual or an individual's family members and about diseases or disorders manifested in an individual's family members. A distinction is made between genetic tests and medical tests such as HIV tests, complete blood work, cholesterol testing, and liver function tests.

10. What are good resources for additional information?

- The Final Omnibus Rule was published in the Federal Register on January 25, 2013. The link is **http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf**. The material identifies modifications and additions, citing both public comment and rationale for DHHS' final decisions.
- The North Carolina Healthcare Information and Communications Alliance (NCHICA) is working to revise the sample tools that it produces – a Notice of Privacy Practices, Business Associate Agreement, and Notice of a Breach. Satinsky Consulting, LLC will participate in the revision process. Go to **www.nchica.org** for additional information.
- The website of the Office of Civil Rights contains instructions for submitting a Breach form: **http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html**.

SATINSKY CONSULTING

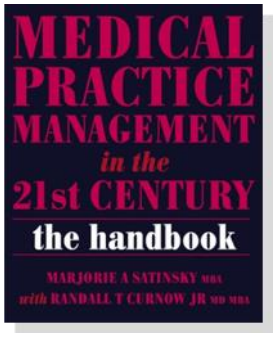
What's Next for Your Practice or Organization?

SATINSKY CONSULTING, LLC can help your practice or organization address HIPAA compliance in several ways. Contact us at 919.383.5998 or **Margie@satinskyconsulting.com** to learn more.

- **If you haven't started on HIPAA compliance**, we provide customized Privacy and Security Rule Manuals tailored to your specific needs. Both contain assessment tools that help you determine your current situation and identify next steps. The package includes staff training.
- **If you are a current client** for whom we have already prepared the Privacy and Security Manuals, completed assessments, and conducted staff training, we can update the material and re-train your staff.
- **If we did not participate in the development of your HIPAA program**, we can review current materials, make suggestions for change, and retrain your staff.

Remember to register now for the February 21, 2013, 12:00 PM EST Tele-class on HIPAA Privacy and Security Rule Compliance, sponsored by InHealth Consulting & Educational Services as part of its Efficiency in Practice series.

Ideas for Managing Your Practice



If you are looking for new ideas to improve your bottom line and practice operations, order **The Handbook for Medical Practice Management in the 21st Century**. The book and the companion website offer concrete suggestions and practical tools. Authored by Marjorie A. Satinsky, M.B.A., with Randall T. Curnow, Jr., M.D., M.B.A., the handbook can be ordered by phone from Radcliffe Press (800.247.6553, x2402) or online using this **link to it on amazon.com.**

Satinsky Consulting, LLC
201 Cedar Ridge Way
Durham, NC 27705-1981
919.383.5998
Fax 919.309.0109
www.satinskyconsulting.com