SATINSKY CONSULTING

SPRING 2013 NEWSLETTER

Margie Satinsky

As you know, in late January 2013 CMS issued the Omnibus Final Rule on HIPAA, bringing together many of the disparate pieces related to the HIPAA Privacy and HIPAA Security Rules. Since that time, we've presented webinars and on-site presentations to both organizations and individual practices. Our audiences repeatedly ask the same question: "Do we really have to take compliance seriously?" The answer is yes. Make sure you understand both the penalties and your obligations for determining whether or not Protected Health Information (PHI) has been used or disclosed in an unauthorized way in what is known as a "breach."

For additional information about HIPAA changes, listen to our **recent interview** with Information Security Media Group or refer to our **previous newsletter**.

HIPAA PENALTIES AND BREACHES – WHAT YOU NEED TO KNOW

Penalties Are Real – Ignorance Is Not Bliss

Smaller practices shouldn't be complacent, assuming that full HIPAA compliance applies only to large entities. Now that the enforcement audit program has begun in earnest, many small entities have already faced stiff fines for incidents that meet the definition of a breach. Ignorance is not bliss, and if "willful neglect" is demonstrated, the financial penalties are stiffer. Violations of the HIPAA Privacy and Security Rules have three types of associated penalties – civil monetary penalties, criminal penalties, and penalties for violation of the breach notification provision. It is possible to be "double dinged" – i.e., to receive both a civil penalty and a penalty related to breach notification.

Improper use or disclosure of PHI can result in four categories of civil monetary penalties reflecting increasing levels of culpability by individuals, employees, and/or organizations. The following civil monetary penalties apply to covered entities, Business Associates, and to subcontractors (i.e., agents) of Business Associates.

- $100-$50,000 per violation for an unknowing privacy violation by a covered entity or Business Associate, with a $1.5 million maximum/calendar year penalty for violations of an identical provision.
- $1,000 - $50,000 per violation for a violation for which it is established that the violation was due to reasonable cause and not to willful neglect, with a $1.5 million maximum/calendar year penalty for violations of an identical provision.
- $10,000 - $50,000 per violation for which it is established that the violation was due to willful neglect and was corrected in a timely manner, with a $1.5 million maximum/calendar year penalty for violations of an identical provision.
- $50,000 per violation for a violation in which it is established that the violation was due to willful neglect and was not timely corrected, with a $1.5 million maximum/calendar year penalty for violations of an identical provision.

SATINSKY CONSULTING

State attorneys general (AG) are authorized to pursue civil actions for HIPAA privacy and security violations that have threatened or adversely affected a resident of that AG's respective state. The state must notify DHHS of a suit before or as soon as feasible after filing.

HIPAA violations can result in criminal as well as civil penalties. For the violation to be criminal, the individual who committed the violation must have done so willingly, knowing the implications of divulging the PHI. As with the civil penalties, there are different levels of severity for criminal violations.

- $50,000 per violation and up to one year in jail.
- For violations committed under false pretenses, $100,000 per violation and up to five years in jail.
- For violations where there was intent to sell, transfer, or use PHI for commercial advantage, personal gain, or malicious harm, up to $250,000 per violation and up to 10 years in jail.

Risk Analysis to Determine If a Breach Has Occurred

One of the major changes in the 2013 Omnibus Final Rule applies to the definition of a "breach" – i.e., the unauthorized use or disclosure of PHI. We're talking about "unsecured" PHI – PHI that is not secured through a technology or methodology specified by DHHS that renders the PHI unusable, unreadable, or indecipherable to unauthorized individuals (e.g., encryption). An impermissible use or disclosure of unsecured PHI is now considered to be a reportable breach unless the covered entity, Business Associate, or subcontractor (agent) of a Business Associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised.

The burden of proof regarding a breach requires a four-part risk analysis. For example, a lost or stolen laptop computer isn't always a breach. The conclusion depends on answers to the following questions:

1. The nature and extent of the PHI, including the types of identification and the likelihood of re-identification
2. The unauthorized person who used the PHI or to whom a disclosure was made
3. Whether or not the PHI was acquired or viewed
4. The extent to which the risk to the PHI has been mitigated

Next Steps for Your Practice or Organization

We encourage you to take compliance with the HIPAA Privacy and Security Rules seriously. The deadline for compliance is September 23, 2013 unless the termination date of your current Business Associate Agreement (BAA) is later. In such cases you can allow the current BAA to run its full course and then revise your document. Here's how we can help:

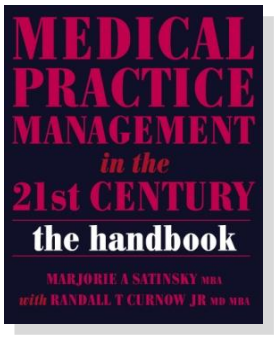
- Listen to our **recent interview** with Information Security Media Group on the challenges of HIPAA compliance for small practices.
- Read our **Winter Newsletter** for additional information.
- Contact us for help: 919.383.5998 or **Margie@satinskyconsulting.com**. We provide sample documents and/or a complete package that includes customized HIPAA Privacy and Security Manuals, sample documents, new policies and procedures, workforce training, and ongoing assistance.

SATINSKY CONSULTING

Other Resources Related to HIPAA Compliance & Breaches

- 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 is participating 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**.

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