

WINTER 2011 NEWSLETTER

This newsletter specifically addresses the important requirements of HIPAA that are set forth in the Privacy and Security Rules and also in the HITECH Act of 2009. HIPAA compliance is one of the Health Information Technology (HIT) objectives that became part of Meaningful Use when the Final Rule was issued in July 2010.¹



Margie Satinsky

It's been nine years since required compliance with the HIPAA Privacy Rule and seven since required compliance with the HIPAA Security Rule. When both Rules were new, Covered Entities such as medical practices paid a great deal of attention to them. As the years have passed, however, HIPAA compliance has dropped to the bottom of the list of priorities for many practices. More often than not, when we ask about HIPAA compliance, we are told "Yes, we're HIPAA compliant; we have a sign hanging on the wall." Hanging a Notice of Privacy Practices (NPP) on the wall does not equal compliance, so read on!

Make sure you know what's necessary, not only because HIPAA and Meaningful Use are related, but because HIPAA makes very good business sense given the ways in which we depend on protected health information (PHI), particularly information that is in electronic form (ePHI).

HIPAA – 10 THINGS TO KNOW

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), modified some of the provisions of the Privacy and Security Rules and added new requirements. If your practice submits claims electronically and/or you have an electronic health record (EHR) system, you must comply with the changes.

2. How does HIPAA define a Covered Entity?

HIPAA defines a Covered Entity as a health plan, healthcare clearinghouse, or any healthcare provider that transmits health information in electronic form. Most medical practices are Covered Entities for two reasons:

- They provide care and bill electronically, and
- They are employers that offer a health insurance plan to employees.

¹ Our previous two newsletters, accessible at www.satinskyconsulting.com/publications.htm, provided many details on Meaningful Use, the provision in the HITECH Act part of the American Recovery and Reinvestment Act (ARRA) that defines the criteria that providers must meet to qualify for financial incentives related to the use of EHR.

3. What is a Business Associate?

Business Associates are persons or entities that use or disclose Protected Health Information (PHI) to carry out certain functions or activities on behalf of Covered Entities. The HITECH Act of 2009 obligates Business Associates to comply with most of the requirements of the Privacy and Security Rules regarding Covered Entities. Relationships between Covered Entities and Business Associates are governed by Business Associate Agreements (BAA). If you are a Covered Entity and you created your BAA prior to the HITECH Act of 2009, update it.

4. How can our practice determine whether or not we are HIPAA-compliant?

With respect to both privacy and security, begin with the requirements, making sure you are clear about expectations. Document what you currently do and any gaps between your current situation and the requirements. Develop a plan of corrective action, assign responsibilities and timelines, and monitor your progress.

5. Both the Privacy and Security Rules and the HITECH Act of 2009 require that Covered Entities have specific policies and procedures. Do we have to start from scratch, or can we obtain sample policies and procedures that we can customize for our practice?

Every organization should develop policies and procedures that are appropriate for its specific needs. In response to requests from more than 60 medical practices and employers, Satinsky Consulting, LLC has developed two sets of sample policies and procedures, one for Privacy and another for Security. The material is available electronically, so you can easily customize it to suit your practice.

6. When the Privacy and Security Rules were originally passed, we trained our workforce members. How often do we need to train current and new members of our workforce?

Since the HITECH Act of 2009 made significant changes to HIPAA, we suggest you retrain your current workforce. Given the high rate of staff turnover in most medical practices, many workforce members may not have had previous training or may have forgotten what they learned. Offer annual refresher training and incorporate HIPAA training into your employee orientation program. Remember that your workforce includes salaried employees, people who do work for you on a contract basis, volunteers, and interns.

7. We know that HIPAA requires Covered Entities to designate both a Privacy Official and a Security Official. Can our practice designate one individual as the HIPAA czar for both Privacy and Security?

The designation of your two HIPAA officials depends on the capabilities of your workforce members. In some practices, the same individual serves as both the Privacy and the Security Official. Other practices delegate some of the security responsibilities to an Information Technology (IT) person within or outside the practice.

8. What is the difference between the Privacy and Security Rules?

The concepts in the two Rules are consistent with each other, and there are some areas of overlap. However, the Privacy Rule focuses on Protected Health Information (PHI), including but not limited to Electronic Protected Health Information (ePHI). The Security Rule focuses on ePHI. There are other differences between the Rules. The Privacy Rule is administrative in nature, and there's not much choice in the way in which Covered Entities (and more recently Business Associates) comply. The Security Rule has administrative, technical, and physical specifications. There is more opportunity for discretion, in that some of the specifications are required and others are addressable. Your goal for Security should be to decide what is appropriate for your practice and then document your action and your reasoning.

9. The HITECH Act of 2009 contains new HIPAA requirements. Which of the new requirements are the most important?

- Expansion of the application of both the Privacy and Security Rules to Business Associates (BAs). BAs are now required to meet most of the requirements for Covered Entities
- Expansion of the definition of Business Associates to include health information exchanges (HIEs) and regional health information organizations (RHIOs)
- Increase in the penalties for violations of HIPAA
- Provision of additional methods of enforcement, now allowing states' Attorneys General to play a role
- Requirement that medical practices that adopted an EHR system after January 1, 2009 track all disclosures of patient information, including those made for the purposes of treatment, payment, and healthcare operations. Medical practices that adopted EHR prior to January 1, 2009 have until January 1, 2014 to comply with this new Accounting for Disclosures requirement. They need extra time to modify their workflow processes and systems. This provision has the potential to create a serious administrative burden. Many practices collect and store information in multiple places, making the task of bringing the information together very challenging.
- Requirement that all Covered Entities comply with new Security Breach Notification rules
- Requirement for proactive auditing of Covered Entities by the Secretary of the Department of Health and Human Services (DHHS)

10. How can Satinsky Consulting LLC help us meet the HIPAA Privacy and Security requirements?

- **Comprehensive and Current Manuals:** Our comprehensive Privacy and Security Manuals contain clear explanations, sample policies and procedures, and forms that you can customize for your organization. Because our material changes as the requirements change, you're never out of date.
- **Training:** We've trained more than 60 medical practices and employers on the Privacy and Security Rules and on the HITECH Act of 2009. We provide training materials and do the training for you.

Articles on HIPAA

Use the links below, or visit www.satinskyconsulting.com/publications.htm to read these and other articles by Margie Satinsky.

- ["Managing the Implementation of HIPAA and the Privacy Rule"](#)
2003
- ["Implementation of the HIPAA Security Rule"](#)
North Carolina Medical Board Forum • 2004

Articles on Selecting and Implementing Information Technology

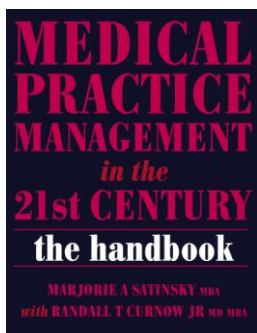
Use the links below, or visit www.satinskyconsulting.com/publications.htm to read these and other articles by Margie Satinsky.

- **[“Electronic Health Records. Is Now the Time for Your Practice?”](#)**
North Carolina Medical Board Forum • 2010
- **[“Selecting Electronic Health Records and Other Technology Solutions to Support Your Practice”](#)**
Medical Association of Georgia Journal • 2009
- **[“Medical Practice Excellence in the 21st Century: How to assess your practice before choosing the best information technology - Part 3 of a three-part series”](#)**
Skin & Aging • 2008

Upcoming Presentations

- **February 16, 2011** **“HIPAA Compliance, Meaningful Use, and Other Hot Topics for 2011”**
Winston-Salem Medical Group Managers
- **February 26, 2011** **“Meaningful Use of EHR”**
North Carolina Society of Otolaryngology and Head & Neck Surgery
Greensboro, NC

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 is available from Radcliffe Press.

To order the book, call 800.247.6553 or visit www.radcliffe-oxford.com.