SATINSKY CONSULTING

SUMMER 2013 NEWSLETTER

Margie Satinsky

This newletter is the last in a series of three that explain important changes in HIPAA compliance regulations (2013 Omnibus Final Rule) that go into effect on September 23, 2013. This edition contains tips for those who have yet to address the compliance requirements – and are perhaps looking for a "fast path" in light of the deadline.

Our **Winter 2013** newsletter provided background information. The **Spring 2013** newsletter focused on intensified HIPAA enforcement efforts and penalities.This newsletter includes answers to specific questions that clients have asked as well as suggestions for tackling the compliance challenge. For additional information, listen to our **recent interview** with Information Security Media Group and read our article in the upcoming edition of the North Carolina Medical Board *Forum* newsletter.

FREQUENTLY ASKED QUESTIONS

1. **We're a small medical practice. Do we really have to bother with all the steps needed to comply with the Privacy and Security Rules?**

   Yes! When HIPAA first passed, the Department of Health and Human Services (DHHS), and its enforcement arm, the Office of Civil Rights (OCR), focused on education and voluntary compliance rather than on enforcement. That situation has changed, and an active enforcement audit program is now in effect. If you are a covered entity or Business Associate, small size does not mean you are under the radar screen. Here's an example. On January 2, 2013 DHHS announced its first HIPAA breach settlement involving fewer than 500 patients. The Hospice of North Idaho agreed to a settlement of $50,000. The agency had reported a theft of a laptop computer containing ePHI for 441 patients, and during the course of its investigation, OCR discovered that the Hospice had not conducted a risk analysis to safeguard PHI.

2. **As a covered entity, we are required by the Omnibus Final Rule to comply with patient requests not to disclose PHI to insurers provided that the patient pays out of pocket in full for a specific service. This requirement seems to conflict with language in our managed care contracts requiring that we notify managed care providers of all services that we provide to members. Do the managed care plans expect us to report all services that we provide to members?**

   No. Health insurance plans, like healthcare providers, meet the definition of covered entities, and so this particular provision applies to them too. The plans do not expect you to report the provision of services if a patient pays in full and requests that you not inform the plan. It is possible that some of your managed care contracts were executed prior to the date when this new HIPAA provision went into effect. If that's the case, talk with the managed care folks about amending contract language.

3. **Some of our providers communicate directly with patients using non-secure email. Are these providers violating the requirements of the Privacy and Security Rules?**

   The Security Rule requires encryption of electronic PHI (ePHI). Both a secure patient portal that is linked to an organization's website or encryption software that is built in or installed on mobile devices meet that

requirement. Furthermore, the 2013 language regarding determination of a breach identifies encryption as a protection. That being said, the Omnibus Final Rule allows healthcare providers to communicate with patients by non-secure email, *provided that a disclaimer accompanies the communication*. We advise our clients to use encrypted communication rather than non-secure email with a disclaimer.

4. **Our organization uses social media like Twitter and Facebook. Are we violating the HIPAA requirements?**

   The 2013 Omnibus Final Rule does not single out social media. However, your state Medical Board may have a formal position statement on social media similar to the one adopted by the North Carolina Medical Board in March 2013. Here are highlights:

   "The Board recognizes that social media has increasing relevance to professionals and supports its responsible use. However, health care practitioners are held to a higher standard than others with respect to social media because health care professionals, unlike members of the lay public, are bound by ethical and professional obligations that extend beyond the exam room."

   The Board encourages licensees to consider the implications of at least these online activities: (1) maintaining appropriate boundaries in accordance with professional ethical guidelines; (2) "absolutely" maintaining patient privacy and refraining from posting identifiable patient information online; (3) separating professional and personal identities online by maintaining separate email accounts and separate social media presences; and (4) in private personal accounts, maintaining awareness of the posting of material that might be considered to be unprofessional, inappropriate, or unethical.

5. **We have revised our Notice of Privacy Practices (NPP) to comply with the requirements of the Omnibus Final Rule. Must we give each patient that new document?**

   Within a year after you revise your NPP, give each patient the opportunity to review the new version. As with your original NPP, document that the patient has reviewed the NPP. If the patient refuses to review the NPP, document that too. Immediately post your revised NPP on your website so it is readily available for review by existing and potentially new patients.

6. **As a practice manager with a full workload, I'm overwhelmed with the amount of work that needs to be done to bring our organization into compliance with the new HIPAA requirements. Where should I start?**

   Start with risk analyses of both HIPAA Privacy and Security that will help you match what you've already accomplished with the new requirements. List what needs to be done, and at that point, determine whether or not you can do the work internally or if you need external assistance.

SUGGESTIONS FOR SUCCESSFUL COMPLIANCE

1. **Determine the most effective way for your organization to achieve compliance.**

   Some organizations have the internal ability to assess their privacy and security risks, identify steps that need to be taken, and take those steps. Other organizations lack the internal capability and need external support. Still other organizations prefer a combination of internal and external efforts. Do what's right for you, given the size of your organization and the capabilities of your Privacy and Security Officials. One size does not fit all.

SATINSKY CONSULTING

2. **Understand the distinction between Privacy and Security Rule checklists and full risk analyses.**

   Checklists are a good starting place, but they are not a substitute for two full risk analyses that include documentation of findings, likelihood of risk, steps for correction, assignment of responsibilities, and timely execution. Shortcuts don't meet the requirements.

3. **Think of your organization as the hub of a wheel that includes your EHR vendor and your external IT support service (if you have one).**

   As a covered entity or Business Associate, you, not these other entities, are responsible for HIPAA compliance. An EHR vendor can provide help and training on the privacy and security of its product, and an IT support company can help you complete a risk assessment and take corrective action. Ultimately, however, your organization, as the covered entity or Business Associate, is the responsible party.

4. **If workforce members use mobile devices, take appropriate steps to protect these devices.**

   The Office of Civil Rights, the enforcement arm of the Department of Health and Human Services (DHHS), and the DHHS Office of the National Coordinator for Health Information Technology (ONC) have published a practical list of suggestions including but not limited to password or other user authentication, encryption, remote wiping and/or remote disabling, disabling file-sharing applications, installation and enabling of a firewall, installing and enabling security software, keeping security software up-to-date, researching mobile applications (apps) before downloading, maintaining physical control, use of adequate security to send or receive health information over public Wi-Fi networks, and deleting all stored health information before discarding or reusing a mobile device. Visit **www.HealthIT.gov/mobiledevices**.

5. **Train your workforce thoughtfully and appropriately.**

   HIPAA Privacy and Security have many levels of detail. Everybody doesn't need to know everything. The Privacy and Security Officials need the best understanding of the requirements of the Rules, and other workforce members need to know enough to support your organization's efforts. We recommend maintaining both online Privacy and Security Manuals and one hard copy for reference purposes.

6. **Communicate positively.**

   Honey, not vinegar, will help you achieve the highest levels of understanding and compliance by your workforce, patients, and clients. Emphasize the benefits that HIPAA provides in protecting individuals' PHI rather than your inconvenience in meeting compliance requirements.

Next Steps for Your Practice or Organization

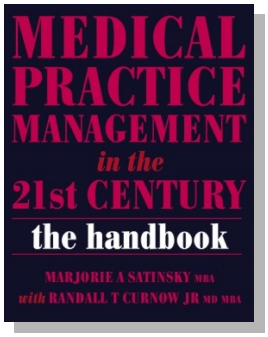
We encourage you to take compliance with the HIPAA Privacy and Security Rules seriously. The deadline for compliance is September 23, 2013 unless the termination date of your current Business Associate Agreement (BAA) is later. In such cases you can allow the current BAA to run its full course and then revise your document. If you need help, please contact us at 919.383.5998 or **Margie@satinskyconsulting.com**. These are some of the ways we can help:

- **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.

SATINSKY CONSULTING

- **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.

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