HIPAA Omnibus Rule Compliance
Frequently Asked Questions

California Medical Association

On January 25, 2013, the U.S. Department of Health and Human Services published new regulations that made significant changes to the privacy and security requirements under the Health Insurance Portability and Accountability Act (HIPAA). These new regulations, known as the HIPAA Omnibus Final Rule implement many of the key provisions of the Health Information Technology for Economic and Clinical Health Act (HITECH) Act of 2009. Covered entities and their business associates have until September 23, 2013, to comply with the new rule.

Answers to the most commonly asked questions related to the HIPAA Omnibus Final Rule compliance requirements are found below. This information does not constitute, and is no substitute for, legal or other professional advice. Physician offices should consult their personal attorneys or professional advisors for specific guidance on their HIPAA compliance plan.

Note: In this document you will find references to "CMA On-Call documents." These documents are available free to members in the California Medical Association (CMA) online health law library at http://www.cmanet.org/cma-on-call. Nonmembers can purchase documents for $2/page.

Privacy and Security Officials

1. Do I need to designate a Privacy Official and Security Official in my office?

Yes. HIPAA requires covered entities to designate a Privacy Official and Security Official who is responsible for the development and implementation of policies and procedures of the physician's office. For many offices, the Privacy Official and Security Official may be the same person.

Notice of Privacy Practices

2. Do I need to update my Notice of Privacy Practices? If so, when do I need to update it by?

Yes. The HIPAA Omnibus Final Rule requires physician practices to make material changes to their existing Notice of Privacy Practices (NPP). These changes must be made by September 23, 2013. If your office already revised its NPP in response to the 2009 HITECH Act provisions, so long as the current NPP is consistent with the new rules, you are not required to revise and distribute another NPP.

Specifically, the new rules require the NPP to include a statement informing individuals of their right to be notified following a breach of their unsecured protected health information and their right to obtain a copy of their PHI in electronic format if the covered entity maintains the PHI electronically. The NPP must also inform individuals of their right to restrict certain disclosures of PHI to a health plan when the patient pays out-of-pocket and in full for a health care item or service. Further, the new rules require changes to NPP provisions related to the use and disclosure of psychotherapy notes, the sale of PHI, marketing and the right to opt-out of fundraising solicitations. For an updated sample NPP, see CMA On-Call document #4101, "HIPAA ACT SMART: Introduction to the HIPAA Privacy Rule."

3. Do I need to redistribute the updated NPP and have patients re-sign acknowledgments?

Providers are only required to give a copy of the updated NPP to, and obtain a good faith acknowledgment of receipt from, new patients. Physician offices must make the NPP available to all patients upon request on or after the effective date of the revision and must have the NPP available at the point of care. The updated NPP must also be posted in a clear and prominent location and on the physician practice website.

4. My NPP is long. Do I have to post the entire thing in my waiting room?

No. Providers may post a summary of the notice in a clear and prominent location in the office, such as the waiting room, so long as the full notice is immediately available (such as on a table directly under the posted summary) for individuals to pick up without any additional burden on the patient. If a summary is posted, it would not be appropriate to require a patient to ask for a copy of the full NPP.

Risk Analysis

5. My office has not conducted a risk analysis. Is this necessary to be in compliance with HIPAA?

Yes. Physician practices that maintain electronic PHI must comply with the HIPAA Security Rule requirements and perform a risk analysis of office security. A risk analysis must be an accurate and thorough assessment of the potential risks and vulnerabilities to electronic PHI and its integrity and confidentiality. A risk analysis is more complex than filling out a checklist and physician practices should obtain assistance in completing this task. For more information, see CMA's on-demand webinar "HIPAA Risk Analysis for Meaningful Use." This webinar is available free to members in CMA's online resource library at http://www.cmanet.org/webinars.

For additional guidance on complying with the risk analysis requirement, see the Office for Civil Rights website at http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidance.html. For more information on the HIPAA Security Rule requirements, see CMA On-Call document #4102, "HIPAA Security Rule."

Breach Notification

6. Do I need to update my breach notification policy and procedures?

Yes. Under HIPAA's Breach Notification Rule, covered entities must provide notification following a breach of unsecured PHI. The HIPAA Omnibus Final Rule made a significant change in assessing what is a reportable breach of PHI. The new rules now presume that there is a breach unless the practice can demonstrate that there is a low probability that the PHI has been compromised. This is a change from the previous standard where a breach was not reportable unless it posed a significant risk of harm to an individual. Covered entities must update their office breach notification policies and procedures to reflect this change and train their workforce accordingly. For more information on breach notification and a sample office policy, see CMA On-Call document #4006, "Security Breach of Health Information."

Business Associates

7. Do I need to update my business associate agreements and when do I have to it by?

Yes. All business associate agreements must be revised and updated. The HIPAA Omnibus Final Rule broadened the definition of business associate, which means that some contractors that have not been business associates in the past may now be considered business associates. Physician practices should review their third party vendors and contractors to determine whether they are business associates. Covered entities and business associates may continue to operate under existing business associate agreements for up to one year beyond the September 23, 2013, compliance date. All business associate agreements must be by the earlier of (1) the date the agreement is renewed or modified on after September 23, 2013, or (2) by September 22, 2014. For more information on business associates and an updated sample business associate agreement, see CMA On-Call document #4103, "Business Associate Agreements."

8. We contract with a health care clearinghouse to provide services on our behalf. Do we need to sign a business associate agreement with them if they are a covered entity?

A covered entity can be a business associate of a covered entity. To the extent that the health care clearinghouse performs services such as electronic billing transactions of the physician practice's behalf, it is also a business associate and there must be a business associate agreement in place.

9. Do I need to sign business associate agreement with my employees or individuals who provide janitorial services for my office?

No. A physician practice's employees are not business associates, but rather a part of the covered entity's workforce. In addition, people or organizations whose functions or services do not involve PHI and whose access to PHI would be incidental, such as maintenance or janitorial workers are not business associates.

10. I store my old paper records with a storage company. Do I need to sign a business associate agreement with them?

Yes. The definition of a business associate has been broadened to include entities that create, receive, maintain or transmit PHI on behalf of the physician office. The regulations clarify that companies that maintain or store PHI on behalf of a covered entity are business associates, even if they do not view or access the PHI.

Workforce Training

11. Do I have to retrain my staff after I update my office policies to reflect the new requirements of the HIPAA Omnibus Final Rule?

Yes. All employees, volunteers, trainees and others who work under the control of the covered entity must be trained on the policies and procedures developed to comply with HIPAA. All new employees must be trained within a reasonable time after they join the workforce and additional training must occur within a reasonable time after any material change in a policy or procedure. All training activity must be documented and kept for six years. CMA and PrivaPlan jointly publish a HIPAA Training Manual that provides general training and overview and can be used as part of your HIPAA training program. It is available on CMA's website at http://www.cmanet.org.

Email and Mobile Technology

12. I heard that the HIPAA Omnibus Final Rule prohibits emailing and texting patients after the compliance deadline. Is this true?

No. Physicians who are covered entities have always been prohibited from emailing or texting patient information without the proper privacy and security safeguards. While the patient can consent to receiving certain communications by email, this does not excuse the physician practice from implementing the proper safeguards (encryption/policies/training) to satisfy the HIPAA Privacy and Security Rules. The HIPAA Omnibus Final Rule does not change these requirements. For more information on the use of email and mobile technology, see CMA On-Call documents #0402, "Physician Websites, Internet Advice and Email," and #3301, "Physician Use of Mobile Devices and Cloud Computing."

HIPAA Compliance Resources

13. What do I need to do to get my office in compliance with the HIPAA Omnibus Final Rule?

This will depend on each physician practice and the current status of their HIPAA compliance. A practice that has already updated their policies and procedures to reflect the provisions of the HITECH Act may have very little to do in terms of the September 23, 2013, compliance deadline. Physician practices who have not updated their HIPAA policies and procedures in some time will have more work to do. At a minimum, a practice should:

- Designate a Privacy Official and Security Official
- Review and implement office policies and procedures
- Make sure a risk analysis has been completed
- Update your Notice of Privacy Practices
- Update office privacy policies
- Review third-party vendors and contractors to update business associate list
- Amend business associate agreements
- Update breach notification policies and procedures
- Train workforce

14. Where can I find more resources to assist me?

- **CMA's health law library, CMA On-Call,** is a comprehensive collection of law, ethical opinions and case law of interest to the practice of medicine in California, including chapters on eMedicine, HIPAA, and Medical Records. These documents are available free to CMA members at www.cmanet.org/cma-on-call. Nonmembers can purchase documents for $2 per page.
- **"HIPAA Compliance: The Final HITECH Rule" On Demand Webinar** is available on CMA's website at http://www.cmanet.org/webinars.
- **Office for Civil Rights website** contains guidance documents and up to date information on new regulations regarding the HIPAA Privacy and Security Rules at http://www.hhs.gov/ocr.
- **American Medical Association website** contains an extensive HIPAA Resource Page at http://www.ama-assn.org.
- **CMA/PrivaPlan ToolKit** is a comprehensive online resource to assist physicians in complying with the HIPAA Privacy and Security Rules and California law. It includes a step-by-step compliance plan and numerous California specific sample forms, policies and procedures. It also contains an audit tool designed to assess the degree of compliance in a practice. Physicians can order the CMA/PrivaPlan ToolKit by calling (877) 218-7707 or visiting http://www.privaplan.com. CMA members can purchase the CMA PrivaPlan HIPAA Online ToolKit and PrivaPlan's online HIPAA training programs at discounted prices.