

## What you need to know about the new health privacy and security requirements

Currently, privacy standards under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) require physicians to protect the privacy of patients' medical information. Physicians are required to control the ways in which they use and disclose patients' protected health information. In addition, physicians are required to offer patients certain rights with respect to their information, such as the right to access and copy this information, the right to request amendments and the right to request an accounting of disclosures. Physicians are also required to have certain administrative protections in place (e.g., staff training and implementation of appropriate policies and procedures) to further protect the privacy of patients' information. The American Recovery and Reinvestment Act of 2009 (ARRA), which was signed into law on Feb. 17, 2009, maintains and expands the current HIPAA patient health information privacy and security protections, especially as patient health information is transferred electronically.

### Compliance deadlines

Following is a summary of the new requirements that physicians should plan to comply with immediately.

#### Effective date—Sept. 23, 2009

- HIPAA-covered entities—including physicians—must comply with the new breach notification requirements effective Sept. 23, 2009. However, the Department of Health and Human Services (HHS) will use its discretion not to enforce the new breach notice requirements and will not impose sanctions or financial penalties for breaches discovered before Feb. 22, 2010. Physicians should review and revise their business associate agreements to include breach notification requirements. Visit the AMA's Web site at [www.ama-assn.org/go/hipaa](http://www.ama-assn.org/go/hipaa) for more guidance on the new breach notification requirements. You can also visit [www.hhs.gov/ocr/privacy/hipaa/administrative/](http://www.hhs.gov/ocr/privacy/hipaa/administrative/) and select "Breach Notification Rule" from the left navigation menu to view information from HHS.

#### Effective date—Feb. 17, 2010

- HIPAA-covered entities—including physicians—and their business associates are required to honor a patient's request to not disclose certain protected health information to a commercial health plan if the information solely concerns a health care item or service that the patient has paid for in full out-of-pocket (i.e., patient pays in full for a service upon delivery of that service and requests that his/her physician not submit the bill to his/her commercial health plan).
- HIPAA-covered entities—including physicians—should use a limited data set of identifiable patient information to meet the minimum necessary standard, if such use is practicable, until HHS issues guidance on what exactly constitutes the minimum necessary standard.<sup>1</sup>

---

<sup>1</sup> When using or disclosing protected health information, or when requesting protected health information from others, in general, a physician must make reasonable efforts to limit use or disclosure to "the minimum necessary to accomplish the intended purpose of the use, disclosure, or request."

To be a “limited data set,” the health information must not include any of the following identifiers of the individual and any relatives, employers or household members of the individual: (a) names; (b) all geographic subdivisions smaller than a State, including street address or precinct, other than town or city and zip code; (c) telephone numbers; (d) fax numbers; (e) electronic mail addresses; (f) social security numbers; (g) medical record numbers; (h) health plan beneficiary numbers; (i) account numbers; (j) certificate/license numbers; (k) vehicle identifiers and serial numbers, including license plate numbers; (l) device identifiers and serial numbers; (m) Web Universal Resource Locators (URLs); (n) Internet Protocol (IP) address numbers; (o) biometric identifiers, including finger and voice prints; (p) full face photographic images and any comparable images; and (q) any other unique identifying number, characteristic, or code, except as permitted by the regulation (45 C.F.R. §164.514(c)) to allow the data to be re-identified by the sender.

(45 C.F.R. §164.512(e))

- HIPAA-covered entities—including physicians—using electronic health records are required to honor a patient’s request for an electronic copy of his/her medical record, which must be transmitted directly to an entity or person specified by the patient, as long as that directive is clear, conspicuous and specific. HIPAA requires that such requests be honored within 30 days of notice. Any fee charged for the record must be reasonable and must also comply with applicable state law.
- If a HIPAA-covered entity—including a physician—is paid by an outside entity to send a communication to a patient, the communication is deemed to be marketing material, and therefore requires prior written authorization from the patient. There are limited exceptions to this requirement. Physicians must also give patients an opportunity to opt-out of receiving fundraising communications.
- Business associates of HIPAA-covered entities are required to directly comply with HIPAA requirements.

### **Effective date—Jan. 1, 2011**

- HIPAA-covered entities—including physicians—using electronic health records are required to honor a patient’s request for an accounting of disclosures, including disclosures for treatment, payment and health care operations. HHS will be adopting a technical standard so that electronic health records have the capability to account for disclosures for treatment, payment and health care operations.
- **Exception:** Physicians who adopt electronic health records on or after Jan. 1, 2009 must comply by Jan. 1, 2011 or by the date they acquire the electronic health record, whichever is later.<sup>2</sup>
- **Exception:** Physicians who adopted electronic health records by Jan. 1, 2009 must comply by Jan. 1, 2014.

### **Additional resources**

Visit [www.hhs.gov/ocr/privacy/hipaa/understanding/](http://www.hhs.gov/ocr/privacy/hipaa/understanding/) and select “For Covered Entities” from the left navigation menu for more information from HHS about the HIPAA privacy and security requirements.

For more information about the HIPAA enforcement rules, including increased civil monetary penalties for violations, visit the American Medical Association’s Web site at [www.ama-assn.org/go/hipaa](http://www.ama-assn.org/go/hipaa) and select “HIPAA Violations and Enforcement.”

HHS also provides information about HIPAA violations and their enforcement. Visit [www.hhs.gov/ocr/privacy/hipaa/administrative/](http://www.hhs.gov/ocr/privacy/hipaa/administrative/) and select “Enforcement Rule” from the left navigation menu to access this information.

---

<sup>2</sup> HHS has discretion to extend these compliance deadlines.

In addition to the new privacy and security requirements specified above, the federal regulations impose additional compliance obligations on physician practices consistent with those imposed by other HIPAA obligations, including the following requirements:

1. Review and revise the practice's policies and procedures to reflect the HIPAA Breach Notification Rule. For example, physicians should make sure that their practice's HIPAA compliance program, including record retention practices, address risk assessments for determining whether a breach of unsecured protected health information has occurred.
2. Train their workforce members on the practice's policies and procedures with respect to the notification requirements.
3. Allow individuals to complain about those policies and procedures and any violations of the notification requirements.
4. Sanction workforce members who violate the notification requirements.
5. Refrain from retaliating against those who exercise their rights.

#### **Questions or concerns about practice management issues?**

AMA members and their practice staff may e-mail the AMA Practice Management Center at [\*\*practicemanagementcenter@ama-assn.org\*\*](mailto:practicemanagementcenter@ama-assn.org) for assistance.

For additional information and resources, there are three easy ways to contact the AMA Practice Management Center:

- Call **(800) 621-8335** and ask for the AMA Practice Management Center.
- Fax information to **(312) 464-5541**.
- Visit [\*\*www.ama-assn.org/go/pmc\*\*](http://www.ama-assn.org/go/pmc) to access the AMA Practice Management Center Web site.

Physicians and their practice staff can also visit [\*\*www.ama-assn.org/go/pmalerts\*\*](http://www.ama-assn.org/go/pmalerts) to sign up for free Practice Management Alerts from the AMA Practice Management Center.

The Practice Management Center is a resource of the AMA Private Sector Advocacy unit.