

For more information, please contact:

Bridget Stratton
AHIMA
312-233-1097
bridget.stratton@ahima.org

New HIPAA Omnibus Rule Expands Patient Access to Health Data, Strengthens Patient Privacy and Security

Rule includes changes to privacy and security breach notification and enforcement

CHICAGO – March 25, 2013 – As the effective date for the sweeping changes to the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security rule nears, health information management (HIM) professionals should begin, if they haven't already, developing internal policies and putting processes in place to meet the final compliance date. The final rule becomes effective on March 26 and providers have until September 23, 2013 to comply.

The rule enhances patients' ability to access and manage their health information along with providing expanded privacy rights and protection of personal health data. A complete analysis of the omnibus rule by the American Health Information Management Association (AHIMA) privacy and security experts can be viewed [here](#).

Included in the rule is the requirement that health providers supply electronic copies of a patient's electronic health records (EHRs) when requested, allowing patients to now receive their information in a more convenient and accessible format.

"Increased access to health information empowers patients to play a more active role in managing their own healthcare," said AHIMA CEO Lynne Thomas Gordon, MBA, RHIA, CAE, FACHE, FAHIMA. "Expanded access along with stronger privacy protections represents a new era in healthcare. AHIMA already is working directly with HIM professionals to understand and comply with the new rule, and helping patients understand their increased rights."

In addition to expanded access to their health information, the rule affords patients more control of the privacy of their health data and strengthens security safeguards. Included is a patient's right to request that his or her doctor not share treatment information with their health insurance plan when they pay out-of-pocket, up front and in full for a specific service.

The omnibus rule provides a more objective standard to the Breach Notification Rule's "harm" threshold by stating that any improper use or disclosure of health information is considered a breach. This strengthens the requirement that covered entities do a risk assessment and based on the assessment report the breach to patients and U.S. Department of Health and Human Services (HHS). The rule also makes business associates of HIPAA-covered entities directly liable for compliance with HIPAA requirements.

"The rule holds business associates to the same standards as any other covered entity in terms of protecting patient information and notifying a patient in the event of a breach," said Judi Hofman, CHPS, CAP, CHP, CHSS, AHIMA Certified in Healthcare Privacy and Security Workshop faculty member and privacy and information security officer for St. Charles Health System in Bend, Ore. "This should give consumers greater confidence in the overall protection of their health information and covered entities and business associates clear criteria on what constitutes a breach."

Although similar to the interim rule, HIM professionals will need to assess their organization to ensure they are compliant and implement measures to honor patient requests such as restricting a portion of a patient's medical records.

"The final rule adds substantial modifications to safeguarding personal health information and it's up to the HIM professional to implement these safeguards in a meaningful way," said AHIMA's Director of HIM Practice Excellence Angela Dinh Rose, MHA, RHIA, CHPS. "This may seem daunting but the HIM community will meet this challenge just as we did when HIPAA was first announced."

Other key highlights of the rule include:

- Prohibits the sale of personal health information without authorization.
- Financial remuneration for marketing is defined.
- Rule limits how health information is used and disclosed for fundraising and marketing purposes.
- Access allowed to health information 50 years after the patient is deceased.
- Genetic information may not be used or disclosed for underwriting purposes, except for long term care plans
- Covered entities are now permitted to disclose a decedent's personal health information to family members and others who were involved in the care or payment for care of a decedent prior to death, unless doing so is inconsistent with any prior expressed individual preference.
- Covered entities can disclose proof of immunization to a school where a state or other law requires it prior to admitting a student. Written authorization is no longer required, but an agreement must still be obtained, which can be oral.
- Covered entities must provide the recipient of any fundraising communication with a clear and conspicuous opportunity to opt out of receiving any further fundraising communications and that the individual's choice to opt out is treated as a revocation of authorization under the privacy rule.
- The Notice of Privacy Practices must be revised and redistributed.

In addition to free webinars to members, this summer AHIMA will offer HITECH Symposiums, one and a half day meetings to take an in-depth look at these new changes as well as discuss the operational impacts and implementation challenges. For a list of dates, visit AHIMA's [website](#).

About AHIMA

Celebrating its 85th anniversary this year, the American Health Information Management Association (AHIMA) represents more than 67,000 specially educated Health Information Management professionals in the United States and around the world. AHIMA is committed to promoting and advocating for high quality research, best practices and effective standards in health information and to actively contributing to the development and advancement of health information professionals worldwide. AHIMA's enduring goal is quality healthcare through quality information. www.ahima.org