



H.R. 1, the “American Recovery and Reinvestment Act of 2009” Explanation of Privacy Provisions¹

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 copying, the right to request amendments, and the right to request an accounting. Physicians are also required to have certain administrative protections in place (e.g., staff training, implementation of appropriate policies and procedures) to further protect the privacy of patients' information.

The “American Recovery and Reinvestment Act of 2009” (ARRA) maintains and expands the current HIPAA patient health information privacy and security protections, especially as patient health information is electronically transferred through HIT systems. ARRA amends HIPAA to protect patient health information with the following key provisions that are discussed in more detail below: applies the HIPAA rules directly to business associates and other non-HIPAA covered entities; allows patients to pay out of pocket for a health care service and request non-disclosure of the rendered service; authorizes increased civil monetary penalties for HIPAA violations; defines which actions constitute a breach (including some inadvertent disclosures); requires an accounting of disclosures to a patient upon request; imposes restrictions on certain sales and marketing of protected health information; and grants authority to state attorneys general to enforce HIPAA. The Secretary of the Department of Health and Human Services (HHS), as well as other relevant agencies, will be providing details through the regulatory rule-making process on the expanded privacy and security requirements. Unless otherwise specified, the privacy provisions become effective on February 17, 2010.

Additional HIPAA Privacy and Security Requirements in ARRA

ARRA applies the current HIPAA privacy and security laws directly to business associates of covered entities (i.e., health care providers, plans, and clearinghouses). HIPAA violations can now be enforced directly against business associates rather than only against covered entities (e.g., physicians), which may ease the burden on covered entities to defend against violations by business associates. Non-covered HIPAA entities, such as Health Information Exchanges (HIE), Regional Health Information Organizations (RHIO), e-Prescribing Gateways, and personal health record (PHR) vendors are now required to have business associate agreements with covered entities (including physicians) for the electronic exchange of patient health information.

Covered entities (including physicians) are allowed to use and disclose patient health information for treatment, payment, and health care operation purposes as under current HIPAA rules. In addition, ARRA allows patients (non-Medicare) to pay out of pocket for a health care item or

¹ This summary will be updated when additional details become available during the rule-making process.

service in full at the time of service and request that their physician not submit the claim to the health plan for payment or health care operation purposes.

ARRA authorizes increased civil monetary penalties for HIPAA violations. The Act establishes tiers of penalties based upon: whether or not a covered entity (including physicians) knew of a breach of privacy; whether the breach was due to reasonable cause and not willful neglect; or whether the breach was due to willful neglect. The tiers of penalties are as follows:

- \$100/violation not to exceed \$25,000/calendar year.
- \$1,000/violation not to exceed \$100,000/calendar year.
- \$10,000/violation not to exceed \$250,000/calendar year.
- \$50,000/violation not to exceed \$1,500,000/calendar year.

The Secretary has discretion to determine the amount of penalty based on the nature and extent of the violation and the extent of the harm resulting from the violation. The Secretary continues to have discretion to use a corrective action plan in lieu of imposing a penalty for certain violations.

ARRA defines a breach of patient health information as the unauthorized acquisition, access, use, or disclosure of patient health information. Exceptions to a breach include the acquisition, access, or use of patient health information that is made in good faith and within the scope of employment (e.g., patient record accessed due to error in entering patient identifier). An inadvertent disclosure, however, is considered a breach unless the disclosure occurs within the confines of the covered entity (i.e., facility, physician office). [This “inadvertent disclosure” exception was narrowed at the last minute in the final version of the conference report over strong concerns expressed by the AMA.] If a breach occurs, the covered entity is required to notify the affected patient within 60 days after discovery. There are also requirements for the covered entity to notify the Secretary of HHS and media outlets when a breach affects more than 500 individuals. Personal health record vendors must also notify individuals of a breach of patient health information.

ARRA requires physicians to provide patients, upon request, an accounting of disclosures of health information made through the use of an electronic health record system (EHR) for such purposes as business operations (e.g., submitting insurance claims). Physicians are required to retain the accounting of disclosures for a period of three years.

ARRA prohibits the sale of a patient’s health information without the patient’s authorization, except in limited circumstances involving research or public health activities. Physicians and other covered entities are prohibited from being paid to use patients’ health information for marketing purposes without patient authorization, except limited communication to a patient about a drug or biologic that the patient is currently being prescribed.

ARRA grants enforcement authority to state attorneys general to enforce HIPAA. The total amount of damages imposed on a person for a violation cannot exceed \$25,000 for all similar violations in a calendar year. Notice of any State action must be sent to the Secretary and the Secretary has a right to intervene.