

## **TOP LINE CHANGES BETWEEN H.R. 6357 AND THE AMENDMENT IN THE NATURE OF A SUBSTITUTE TO H.R. 6357**

**Definition of Health Information Technology.** The Amendment in the Nature of a Substitute (AINS) ensures that health information technology includes Internet-based software and solutions.

**Adoption of Standards for the Electronic Exchange and Use of Information.** The AINS requires the Health Information Technology (HIT) Policy Committee to develop recommendations with regard to key HIT-related concerns. These include the technical capability to segregate sensitive health information, the nationwide electronic exchange and use of information, and the nationwide adoption of electronic medical records, and the accounting of disclosures of a person's health information.

**Breach Notification.** H.R. 6357 requires notification to an individual when there is unauthorized acquisition, access, or disclosure of a person's health information. H.R. 6357 includes a "safe harbor," by which an individual would not need to be notified if the breached information was encrypted. The AINS changes the safe harbor by allowing any technologies or methodologies that as determined by the Secretary of Health and Human Services render health information unusable, unreadable, or indecipherable to an unauthorized party. The provision takes effect 90 days after enactment.

The Secretary is required to issue guidance within 60 days, and annually thereafter, as to the technologies or methodologies that meet the standard of making information unusable, unreadable, or indecipherable. If the Secretary fails to issue guidance within 60 days, the safe harbor can only be satisfied by protecting information in accordance with encryption standards in a Federal Information Processing Standard (FIPS) Publication issued by the National Institute of Standards and Technology (NIST) or an equivalent standard developed by a standards developing organization that is accredited by the American National Standards Institute (ANSI).

The AINS also clarifies that a good faith disclosure of health information will not constitute a breach. An example of such disclosure would be letters delivered by the post office to the wrong address.

**Compliance Report.** The AINS improves the compliance report that the Secretary is required to complete by including the number of complaints resolved informally, a brief summary of the types of complaints resolved informally, and the number of covered entities receiving technical assistance from the Secretary in order to achieve compliance, as well as the types of technical assistance provided. The report will also include the number of complaints that resulted in the imposition of civil money penalties, the amount of the penalty imposed in each such case, and a summary of the basis for each such penalty.

**Accounting for Disclosures.** The AINS limits the accounting of disclosures for treatment, payment, and healthcare operations provision so that it will take effect either when an entity acquires or upgrades its electronic medical record or six months after a technical standard with regard to accounting of disclosures is developed and adopted by the Federal Government,

whichever is sooner. The AINS also reduces the amount of time that a provider must retain the information to three years, rather than six years.

**Consent.** The AINS strengthens the consent provision by reiterating that providers still must comply with the requirement that, to the extent practicable, they restrict the amount of protected health information disclosed to the limited data set. In addition, the provision clarifies (1) that the consent may be a one-time aggregated consent, (2) that revocation of consent can only be for data collected prospectively, not retrospectively, (3) that whether or not a provider receives consent, it can maintain the patient's information in an electronic medical record, and (4) that the consent shall not constitute a waiver of any privilege.

The AINS clarifies that the consent provision will take effect after 24 months. In addition, it requires the Secretary to promulgate regulations implementing the provision in a manner that protects health information and is reasonable and workable. If a patient does not provide consent, then a health plan is restricted from using a patient's information for any purpose other than the purpose for which the information was disclosed. The Secretary may exempt certain healthcare operations from the consent provision.

**Prohibition on Sale of Protected Health Information.** The AINS improves the privacy protections included in H.R. 6357 by prohibiting the sale of electronic medical records or protected health information obtained from electronic medical records. Under the AINS, no covered entity or business associate may sell an electronic medical record or protected health information obtained from an electronic medical record of a person without authorization from the person unless it is necessary for treatment or to receive payment for the treatment of that person.

**Access to Electronic Medical Records.** The AINS builds on current Federal privacy law, which permits a person to obtain a copy of his or her medical record. This provision gives a patient the right to receive his or her medical information in an electronic format without charge if a provider maintains the patient's medical record in an electronic format.

**Marketing Restriction.** The AINS improves the marketing provision in H.R. 6357 by precluding indirect payment, in addition to direct payment, in return for making certain communications about healthcare items or services without authorization from the patient. For example, a provider would be precluded from receiving direct or indirect payment for communications made for treatment purposes using a patient's protected health information.

**Security Rules.** The AINS includes language that requires entities such as Health Information Exchanges, Regional Health Information Organizations and E-prescribing Gateways, and others that help the flow of information, to comply with the HIPAA security rules, not just the privacy rules.

**Enforcement.** The AINS improves enforcement of the Federal health privacy law by the Office of Civil Rights (OCR) at the Department of Health and Human Services by requiring a formal investigation of complaints and the imposition of civil monetary penalties for violations that rise to the level of willful neglect. This provision still preserves OCR's current tools for informal resolution, technical assistance, and correction within 30 days without the imposition of a

penalty in situations where the violation was due to a reasonable cause. Currently, all complaints and violations can be handled informally and without the imposition of civil monetary penalties.

In addition, the AINS permits OCR to pursue an investigation and the imposition of civil monetary penalties against any individual for an alleged criminal violation of the Federal health privacy law if the Department of Justice has not prosecuted the individual.