

# THE HITECH ACT

The Health Information Technology for Economic and Clinical Health Act (HITECH or "The Act") is part of the American Recovery and Reinvestment Act of 2009 (ARRA). ARRA contains incentives related to health care information technology in general (e.g. creation of a national health care infrastructure) and contains specific incentives designed to accelerate the adoption of electronic health record (EHR) systems among providers.

Because this legislation anticipates a massive expansion in the exchange of electronic protected health information (ePHI), the HITECH Act also widens the scope of privacy and security protections available under HIPAA; it increases the potential legal liability for non-compliance; and it provides for more enforcement.

The following discussion will highlight some of the HITECH Act's key provisions, but only those that are HIPAA centric. For example, financial incentives (i.e. the actual numbers) for EHR adoption under Medicare and Medicaid have been widely dissected online and are not covered here (some of the websites that contain specific financial incentive information may be located in the Appendix). Consistent with the objectives of this guide, the intent is to provide an overview so that providers can obtain a "big picture" view of legislation likely to impact their practices in significant ways going forward.

Many of the HITECH Act's requirements become effective 12 months from the date of enactment, but there are other effective dates that operate on a different schedule. We will not cover the various effective dates because other resources available on the Internet capture this information in detail (see the Appendix).

We have decided not to use specific statutory references in this section for several reasons: 1) this section is intended as an overview; and 2) HHS will be forthcoming with additional guidance and therefore detailed analysis is best deferred until more clarity emerges.

## **Notification of Breach**

The HITECH Act now imposes data breach notification requirements for unauthorized uses and disclosures of "unsecured PHI." These notification requirements are similar to many state data breach laws related to personally identifiable financial information (e.g. banking and credit card data). HHS is required to define what "unsecured PHI" means within 60 days of enactment. If it fails to do so then the HITECH definition will control. Under the HITECH Act "unsecured PHI" essentially means "unencrypted PHI."

In general, the Act requires that patients be notified of any unsecured breach. If a breach impacts 500 patients or more then HHS must also be notified. Notification will trigger posting the breaching entity's name on HHS' website. Under certain conditions local media will also need to be notified. Furthermore, notification is triggered whether the unsecured breach occurred externally or internally. The notification provision is yet another example of the weight privacy and security concerns are given under the Act.

## **Electronic Health Record Access**

In the case where a provider has implemented an EHR system, the Act provides individuals with a right to obtain their PHI in an electronic format (i.e. ePHI). An individual can also

designate that a third party be the recipient of the ePHI. The Act provides that only a fee equal to the labor cost can be charged for an electronic request.

Presumably, all that needs to be done on a provider's part is to click on a few screens and transmit the necessary records, the reality is that even providers that already have an EHR system in place may not have this capability readily available. However, given the Health 2.0 consumer led movement, you can expect that electronic records will be requested significantly more often than their paper counterparts.

Any provider expecting to participate in the HITECH Act's incentives should be prepared to deliver on these requests or risk a finding that their use does not qualify as "meaningful use." Lack of meaningful use may bar incentive payments, depending on how HHS ultimately defines this term. To be clear, the Act has nothing to say regarding a link between requests of ePHI and meaningful use, this is simply a plausible inference on our part.

### **Enforcement/Penalties**

The consensus view is that HIPAA has not been rigorously enforced in the past. Time will tell how the enforcement regime will change post the HITECH Act, but certainly the Act contains language that implies lax enforcement may be ancient history. Under HITECH, mandatory penalties will be imposed for "willful neglect." Obviously what "willful neglect" means will be determined on a case-by-case basis, but speaking in the parlance of this guide, we believe that a provider with "no story" regarding compliance (or so minimal a story as to portray a cavalier attitude toward compliance) will likely be at significant risk.

Civil penalties for willful neglect are increased under the HITECH Act. These penalties can extend up to \$250,000, with repeat/uncorrected violations extending up to \$1.5 million. Legislators appear to be sending a clear message that "we are not in Kansas" anymore. Furthermore, under certain conditions HIPAA's civil and criminal penalties now extend to business associates. Like HIPAA, the HITECH Act does not allow an individual to bring a cause of action against a provider. However, it does allow a state attorney general to bring an action on behalf of his or her residents. By February of 2012 complainants can share in any fines imposed on individuals and organizations. Finally, HHS is now required to conduct periodic audits of covered entities and business associates.

Clearly, the legislative intent is to provide for "enhanced enforcement." To what degree enforcement actually increases on the ground is yet to be determined, but the HITECH Act significantly ups the ante for non-compliance.

The HITECH Act provides a tiered system for assessing the level of each HIPAA privacy violation and, therefore, its penalty:

- Tier A is for violations in which the offender didn't realize he or she violated the Act and would have handled the matter differently if he or she had. This results in a \$100 fine for each violation, and the total imposed for such violations cannot exceed \$25,000 for the calendar year.
- Tier B is for violations due to reasonable cause, but not "willful neglect." The result is a \$1,000 fine for each violation, and the fines cannot exceed \$100,000 for the calendar year.

- Tier C is for violations due to willful neglect that the organization ultimately corrected. The result is a \$10,000 fine for each violation, and the fines cannot exceed \$250,000 for the calendar year.
- Tier D is for violations of willful neglect that the organization did not correct. The result is a \$50,000 fine for each violation, and the fines cannot exceed \$1,500,000 for the calendar year.

The HITECH Act also allows states' attorneys general to levy fines and seek attorney's fees from covered entities on behalf of victims. Courts now have the ability to award costs, which they were previously unable to do.

### The Schedule

The general effective date for HITECH HIPAA provisions is February 17, 2010, a 12-month grace period. But exceptions swallow the general rule. The following chart roughs out effective dates for provisions of greatest interest to providers. Bear in mind that this list is not exhaustive and that Congress can change its mind or the Secretary of HHS may act sooner or later than anticipated.

<b>Effective Immediately</b>	<ul style="list-style-type: none"> <li>• Collected civil monetary penalties go to OCR</li> <li>• Civil monetary penalties are increased substantially</li> <li>• Civil action by state Attorneys General on behalf of aggrieved persons are authorized; statutory penalties and attorney fees are recoverable</li> </ul>
<b>On or Before September 15, 2009</b>	New security breach notification obligations effective
<b>February 17, 2010</b>	<ul style="list-style-type: none"> <li>• Business associates are directly subject to HIPAA</li> <li>• Limited Data Set standard for "minimum necessary," except as necessary to the purpose of the disclosure</li> <li>• Marketing communications further restricted</li> <li>• Business associate agreements required for "courier" entities</li> <li>• Employees of covered entities may have independent criminal liability</li> </ul>
<b>On or After January 1, 2011</b>	Accounting for treatment, payment, or healthcare operation (TPO) disclosures from EHR systems acquired <i>after</i> January 1, 2009; HHS may extend deadline by two years
<b>On or Before February 17, 2011</b>	<ul style="list-style-type: none"> <li>• New prohibitions on disclosure of PHI in exchange for remuneration</li> <li>• Mandatory civil monetary penalties for violations involving "willful neglect"</li> </ul>
<b>On or before February 17, 2012</b>	Complainants will share in collected civil monetary penalties
<b>On or After January 1, 2014</b>	Accounting required for TPO disclosures from EHR systems acquired <i>before</i> January 1, 2009; HHS may extend deadline by two years

**18 Identifiers that Constitute PHI – Protected Health Information** (Note: If all of the following 18 identifiers are removed, then the data is considered de-identified and may be used/disclosed without restriction.)

1. Names
2. All geographic subdivisions smaller than a state, including: street address, city, county, precinct, ZIP Code, and their equivalent geographical codes, except for the initial 3 digits of a ZIP Code if, according to the current publicly available data from the Bureau of the Census:
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older.
4. Telephone Number
5. Fax Number
6. E-mail Address
7. Social Security number
8. Medical Record number
9. Health Plan Beneficiary number
10. Account numbers
11. Certificate/License number
12. Vehicle Identifiers and Serial numbers (including license plates)
13. Device identifiers and Serial numbers
14. URL Address
15. IP Address
16. Biometric identifiers, like fingerprints and voiceprints
17. Full-face Photos and Any Comparable Images
18. Any other unique identifying number, characteristic or code