

The HITECH Act and HIPAA

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. 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 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.

Enforcement

As mentioned previously, and more or less widely known within the health care industry, 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. 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.

Continued...

The HITECH Act and HIPAA (cont'd)

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.

Business Associates

The HITECH Act now applies certain HIPAA provisions directly to business associates. Formerly, privacy and security requirements were imposed on business associates via contractual agreements with covered entities. As we have noted elsewhere in this guide, we suspect that many small providers do not have the requisite contracts in place. In some cases contracts exist but may not meet all the requirements of the rules. Under the lax enforcement regime of the past, lack of contractual agreements has apparently not proved problematic for the provider community as a whole. This may soon change.

Under the HITECH Act, business associates are now directly "on the compliance hook" since they are required to comply with the safeguards contained in the Security Rule (SR). The HITECH Act does not speak directly to the rationale, but even casual observers understand that a potentially massive expansion in the exchange of ePHI increases the privacy and security concerns of all stakeholders. Most, if not all, software vendors providing EHR systems will clearly qualify as business associates. Requiring vendors to comply directly ensures that more provider/vendor dialog will occur regarding the necessary contracts, and regarding other compliance issues of mutual interest. The vendors themselves will insist on it.

Continued...

The HITECH Act and HIPAA (cont'd)

Business Associates (cont'd)

The "fun" for business associates does not stop with SR compliance and contractual agreements. The Act requires business associates to report security breaches to covered entities consistent with the notification requirements. Also, they are now subject to civil and criminal penalties under HIPAA if certain conditions exist, as mentioned in the introduction of this section. Finally, the business associate requirements listed above are illustrative and not exhaustive. There are additional business associate requirements that may be imposed depending on how the relationship with the provider is defined.

The bottom line is that business associates and providers will share more joint responsibilities than they have previously. Large providers, with the help of counsel and other specialized staff, will not likely be surprised by these changes. However, for many small providers the HITECH Act may be the first real introduction to the business associate concept-yet one more regulatory requirement that will require serious attention.

Other Requirements

The HITECH Act contains additional requirements (e.g. marketing communications, restrictions and accounting) that modify HIPAA in important ways. We simply choose not to cover these because they are even more arcane than the requirements previously listed, but that should not imply that we consider them any less important.

Source: HIPAA Survival Guide (hipaasurvivalguide.com/hipaa-survival-guide-02.php)