



## Complying With HITECH Requirements

As you are likely aware, in the coming days new privacy and security requirements applicable to HIPAA-covered entities and their business associates will become effective. Below is an overview of these requirements, how they may affect you, and what actions you should take in order to ensure compliance with them.

### What is the HITECH Act?

The Health Information Technology for Economic and Clinical Health (“HITECH”) provisions of the American Recovery and Reinvestment Act of 2009 (“ARRA”, also referred to as the “Stimulus Bill”) codify and expand on many of the requirements contained in the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) and its regulations to protect the privacy and security of protected health information (“PHI”).

### What are the new requirements?

HITECH changed the privacy and security landscape by imposing a direct legal obligation on business associates (“BAs”) of entities covered by HIPAA’s requirements (“covered entities,” or “CEs”) to comply with many new and existing requirements under the HIPAA privacy regulations (“Privacy Rule”) and security regulations (“Security Rule”). Further, HITECH imposes new data breach notification obligations on CEs and BAs and enhances enforcement authority with respect to HIPAA violations.

### What organizations need to do to comply?

#### **Business Associate Agreements (“BAAs”)**

Organizations covered by HIPAA already are required to have BAAs with entities that perform certain activities for them involving the use or disclosure of PHI. HITECH explicitly requires that its new provisions be incorporated into existing BAAs. Due to these new privacy and security requirements, current agreements should be updated and amended in order to incorporate them.

- *Expanded individual rights:* The revised contracts must incorporate expanded rights granted to individuals, such as: to the extent PHI is maintained in an electronic health record (EHR), the right to obtain an electronic copy of one’s health record and have it sent to a third party; the right to an accounting of disclosures of PHI for purposes of treatment, payment and healthcare operations through an EHR<sup>1</sup>; and the right to request certain restrictions on disclosure of PHI to a health plan, if paid in full.

---

<sup>1</sup> Note that, with respect to accounting of disclosures and the prohibition on sale of PHI, these provisions are not in effect until later dates.

- *Further restrictions on uses and disclosures of PHI:* The agreements must also comply with the further restrictions on uses and disclosures of PHI imposed by HITECH, such as: additional restrictions with respect to marketing; the prohibition on the exchange of PHI for remuneration; updated best practices for de-identification of PHI; and compliance with the Privacy Rule's clarified "minimum necessary" rule, addressing the determination of the minimum amount of PHI that must be disclosed for a particular purpose.
- *Reciprocal Obligation to Cure:* Under HITECH, a business associate is deemed to have violated HIPAA if the BA knows of a "pattern of activity or practice" by a covered entity that breaches their business associate agreement ("BAA"), but fails to cure the breach, terminate the BAA or report the non-compliance to HHS. Previously, HIPAA imposed only a one-sided obligation upon CEs to cure any discovered violations.
- *BA Compliance with the Security Rule:* HITECH requires business associates to comply not only with its enhanced privacy requirements, but directly with portions of the HIPAA Security Rule, including implementation of administrative, physical and technical safeguards for electronic PHI. BAs must also develop and enforce related policies, procedures and documentation standards (including designation of a security official). As such, to the extent that you engage in the handling of electronic PHI, your BAAs will require updating.
- *Breach Notification Requirements:* Pursuant to HITECH, HHS released a regulation implementing a new federal breach notification requirement. The HHS Breach Notification Rule applies to covered entities and their business associates, and explains that a "breach," subject to certain exceptions, is the "acquisition, access, use or disclosure of PHI in a manner not permitted by the HIPAA Privacy Rule, that compromises the security or privacy of the PHI." This rule also contains what is known as a "risk of harm" standard, meaning that notification of affected individuals is only necessary if the unauthorized access, use or disclosure poses a "significant risk of financial, reputational or other harm to the individual."

In the event of a breach, individuals whose PHI was affected, the Secretary of HHS, and in limited circumstances the media (if a breach involves 500 or more individuals of a particular state or jurisdiction) must be notified. Though this rule is technically already in effect, HHS has delayed enforcement until Feb. 22, 2010.

Note that the breach notification requirement applies only to "unsecured" PHI. PHI is deemed unsecured unless rendered "unusable, unreadable, or indecipherable" to unauthorized individuals by technologies or methodologies explicitly identified in separate guidance issued by HHS (and currently limited to encryption or destruction). This guidance will be revised on an annual basis and is currently available at:

<http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/federalregisterbreachrfi.pdf>.

You should ensure that all of your BAAs are updated to include these notification requirements in the event of a breach and should be mindful of requirements with respect to the timing of notification.

## **Policies and Procedures**

To the extent your existing policies and procedures are affected by these expanded privacy and security requirements, they too should be updated, or new policies and procedures should be developed. For example, your internal policies regarding your patients' rights to access and control their health information should be revised to incorporate the expanded individual rights described above.

You should also develop or update existing breach notification policies and procedures in order to comply with your new obligations in the event that you or one of your BAs experiences a breach. These policies should explain not only how to respond to a breach, but how to identify that one has occurred and assess and document the risk of harm to individuals.

## **Enforcement**

As noted above, HITECH raises the stakes for complying with HIPAA, as potential civil monetary penalties have been increased and criminal penalties now may be levied against individuals. Previously, HIPAA violations were investigated and enforced through the federal Department of Health and Human Services and Department of Justice, but now state attorneys general also have authority to bring a HIPAA enforcement action. Note also that HITECH requires HHS to conduct mandatory periodic audits to ensure CE and BA compliance.

## **Resources**

- 45 CFR Parts 160 and 164, Breach Notification for Unsecured Protected Health Information; Interim Final Rule, Health and Human Services (HHS), August 2009
  - <http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf>
- NHPCO HIPAA information webpage
  - <http://www.nhpco.org/i4a/pages/index.cfm?pageid=5506&openpage=5506>
- Hogan & Hartson HITECH articles
  - <http://www.hhlaw.com/search/Search.aspx?qu=HITECH>
- Reinhart Boerner Van Deuren s.c. publications related to HITECH
  - <http://www.reinhartlaw.com/Publications/Pages/searchresults.aspx?k=HITECH>

Prepared by Hogan & Hartson, LLP, February 2010