



Government Mandate Bulletin

February 5, 2010
Issue 2 - West

Distributed by Producer Affairs - West

INSIDE THIS ISSUE

1 HITECH

HITECH Act puts new obligations on a business associate when there is a "breach" of (PHI)

HITECH

Health Information Technology for Economic and Clinical Health

As you may be aware, the HITECH Act puts new obligations on a business associate when there is a "breach" of protected health information (PHI). Because you are a business associate of Highmark, you should be familiar with:

- Your new obligations under HITECH
- How to determine whether the "harm threshold" has been met
- The required contents for a breach notification
- The penalties for non-compliance.

The information provided here is not intended to replace or otherwise serve as legal counsel or convey legal advice. To ensure that you and your agency are complying with the HITECH Act, you should consult your attorney or legal advisor.

What are the new obligations under HITECH?

Highmark is considered a "covered entity," as defined by the Health Insurance Portability and Accountability Act of 1996 (HIPAA). You serve as a "business associate" when you receive PHI from Highmark for your clients.

Under HITECH, business associates are required to notify their covered entities of any "breach" involving protected health information (PHI). It is Highmark's obligation, in turn, as the covered entity, to notify the impacted individuals, the Department of Health and Human Services (HHS), and, in some cases, the media of the "breach" as specified by the HITECH breach notification regulations.

Previously, as our business associate, your compliance obligations were limited to those defined in our business associate agreement. Effective February 17, 2010, business associates are required by Federal law to meet these obligations. You are also responsible to ensure that any subcontractor or agent with whom you share PHI meets these obligations.

How does HITECH define a “breach” of PHI?

*How does HITECH
define a “breach” of PHI?*

A “breach” is defined as 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. HHS considers the security or privacy of PHI to be “compromised” if the non-permitted acquisition, access, use, or disclosure poses a significant risk of financial, reputational, or other harm to the individual(s).

To determine whether the “harm threshold” has been met, HHS regulations require covered entities and business associates to consider among other things.

1. The identity of the entity or individual that impermissibly used the information or to whom the information was impermissibly disclosed;
2. The steps that were taken to mitigate harm and the immediacy with which such steps were taken;
3. Whether the information was returned before being accessed; and,
4. The type and amount of information used or disclosed.

Who needs to be notified of the breach and when?

If you become aware of a problem that may involve a breach of PHI, you need to notify us and provide the information outlined below according to the terms of your amended Business Associate agreement. Send the breach notice to:

Highmark Inc.
Privacy Department
120 Fifth Avenue
Suite 2114
Pittsburgh PA 15222



Who needs notified of a breach?

You can also e-mail this notice to privacy@highmark.com. If you think you have experienced a breach and have questions, you may call our toll-free hotline at 1-866-228-9424.

If you, as our business associate, notify Highmark of any breach of unsecured PHI, we must notify the affected individuals. If we have insufficient or out-of-date contact information for more than ten individuals, we must provide substitute notice by posting a conspicuous notice on the home page of your Web site or through a “major media outlet” in the geographic region where the affected individuals likely reside. We must also notify the HHS secretary.

Timing of the notice and additional requirements vary based on the number of individuals involved. If more than 500 individuals within a state or jurisdiction are impacted:

- We must also provide notice to a prominent media outlet within that state or jurisdiction.
- We must report the breach to the Secretary “immediately.” Breaches involving fewer than 500 individuals must be logged and reported to the Secretary annually and no more than sixty days after the end of the calendar year.

For calendar year 2009, only those breaches occurring after September 23, 2009 (the effective date of the Interim Final Rule) must be reported.

Is a notice required for all breaches of PHI?

HITECH breach notification requirements apply only to breaches of “unsecured protected health information.” If PHI is “unusable, unreadable, or indecipherable,” a notification may not be required. According to HHS, PHI can be rendered “unusable, unreadable, or indecipherable” in two ways:

- Through the use of encryption, so long as the decryption process or key is not compromised
- If the media on which the PHI is stored is destroyed in such a way that it is not subject to reconstruction, whether in paper, analog, or digital form.

What information must the notice include?

The notification of a breach needs to identify, if possible, each individual whose information was (or is believed to be) affected by the breach and should explain:

- What happened, including the date the breach happened and the date it was discovered,
- What information was involved in the breach, and
- What steps the business associate is taking to investigate the breach.

For calendar year 2009, only those breaches occurring after September 23, 2009 must be reported.

What are the penalties?

Violations of HIPAA, including the breach notification rules, due to “willful neglect” are punishable by \$10,000 to \$50,000 per violation, with an annual maximum penalty of no more than \$1,500,000. In addition, the HITECH Act provides expanded enforcement authority to state attorneys general for HIPAA violations. Under the HITECH Act, certain violations of HIPAA, such as intentional, non-permitted disclosures, are to be enforced pursuant to Sections 1176 and 1177 of the Social Security Act and may include criminal penalties (including incarceration) in addition to monetary fines.

Penalty provisions are effective for violations of the breach notification rule that occur on or after February 17, 2010

The penalty provisions are effective for violations of the breach notification rule that occur on or after February 17, 2010.

More Information

Additional information about the obligations of business associates and covered entities under the Breach Notification Rule is available in Title 45 of the Code of Federal Regulations (CFR) Parts 160, 162, and 164. Refer to www.hhs.gov.

Reginald Brown

Director, Producer Affairs West

Phone:

412-544-2031

E-mail:

reginald.brown@highmark.com