MIEC

SPECIAL REPORT

MIEC Claims Alert

Number 43
March 2010

HITECH Act expands HIPAA requirements

INSIDE

Special Report Claims Alert

A publication of the Loss Prevention Department, Medical Insurance Exchange of California, 6250 Claremont Avenue, Oakland, CA 94618. Articles are not legal advice.

"...information should follow the patient, and artificial obstacles – technical, business-related, bureaucratic – should not get in the way...the goal is to have information flow seamlessly and effortlessly to every nook and cranny of our health system, when and where it is needed...If we are to reap the benefit of information exchange, Americans must also be assured that the most advanced technology and proven business practices will be employed to secure the privacy and security of their personal health information, both within and across electronic systems, and that persons and organizations who hold personal health data are trustworthy custodians of the information."
- Dr. David Blumenthal, National Coordinator for Health Information Technology

On February 17, 2009, President Obama signed into law the American Recovery and Reinvestment Act of 2009 (ARRA). This stimulus package included provisions known collectively as the Health Information Technology for Economic and Clinical Health Act (HITECH),[1] the goal of which is to expand the current U.S. healthcare IT infrastructure to allow for the electronic use and exchange of information while safeguarding patient privacy.

[1] ARRA Title XIII, and Title IV of Division B are collectively referred to as the HITECH Act.

Unless otherwise noted, the provisions go into effect on February 17, 2010.

Physicians who are "covered entities" under HIPAA (Health Insurance Portability and Accountability Act of 1996) will need to incorporate HITECH provisions into their existing privacy and security policies and procedures (including sanctions for violations) and train staff accordingly. The new requirements involve: (1) notifying patients (and the Department of Health and Human Services) when their protected health information (PHI) is improperly accessed or disclosed; (2) greater patient control over how their PHI is accessed and used; (3) mandated changes to agreements between covered entities and business associates; and (4) accounting of *all* disclosures of PHI for those patients whose medical records are electronic.

Physicians should be aware that Congress recently allocated more HIPAA compliance enforcement dollars to the Centers for Medicare and Medicaid Services (CMS) and the Office of the Inspector General (OIG). HIPAA compliance has traditionally been a complaint-driven process, but funds are intended to facilitate audits of HIPAA compliance. There are as yet no details as to what the audits will entail, or what will trigger an audit. The Office of the National Coordinator of Health Information Technology (ONC) will appoint a Chief Privacy Officer to oversee multiple changes to the HIPAA privacy and security provisions that are included in the bill.

Data-breach notification required

Protected health information (PHI) is individually-identifiable documentation maintained in any form or medium (including paper and electronic) of mental or physical medical conditions, the treatment of those conditions and the payment for that care. In other words, PHI is confidential patient information.

As of February 22, 2010,[2] physicians covered under HIPAA must notify each patient whose "unsecured" PHI has been, or is reasonably believed to have been, accessed, acquired, used, or disclosed inappropriately, unless the breach essentially poses no risk of harm to the patient.[3] Physicians will be held accountable for breaches that, through the exercise of reasonable diligence, would have been known to them. This means that physicians must have reasonable systems in place to detect breaches.

"Unsecured" PHI is that which has not been rendered unusable, unreadable, or indecipherable to unauthorized individuals. Essentially, "unsecured" PHI is any PHI that isn't encrypted and/or destroyed in accordance with federal guidelines. HHS has published specific standards pertaining to the strength of the encryption algorithm and the security of the decryption key or process necessary to render electronic PHI "secure" and notes that covered entities and business associates that encrypt PHI should keep encryption keys on a separate device from the data that they encrypt or decrypt.

With respect to the destruction of electronic PHI, electronic media must be cleared, purged or destroyed consistent with NIST (National Institute of Standards and Technology) Special Publication 800-88, *Guidelines for Media Sanitization,*[4] such that the PHI cannot be retrieved. PHI in paper format is "unsecured" by nature, and must be destroyed in such a way that the information can not be read by unauthorized individuals, such as by burning or shredding.

It is the physician's responsibility to disclose the breach or establish that the breach poses no risk of harm to the patient, even if the breach is the fault of a business associate (such as a billing company) acting on behalf of the physician.

Risk assessment

Notification of a data breach is not required if it does not pose a significant risk of harm to the patient. Upon discovery of a breach, physicians and business associates involved in the breach should perform a risk assessment to determine if notification is required, and document the details of that assessment. When determining whether or not notification is required, consider the following:

Would an unauthorized person reasonably be able to access and/or retain the PHI? – If electronic PHI is rendered unusable, unreadable or indecipherable through the use of technology such as encryption (that meets federal standards), there is no breach, even if the information is accessed by an unauthorized individual. In addition, HHS has provided several examples of how there may be no breach even if *unsecured* information is inappropriately accessed or disclosed:

1) If the information has *not* been rendered unusable, but it is possible to determine forensically that the information has not been accessed (such as through a stolen laptop), the information has not been accessed or retained, and therefore there has been no breach.

2) This question applies to PHI in paper format as well: HHS gives the example of an Explanation of Benefits (EOB) mailed to the wrong address and returned, unopened, as undeliverable by the post office. It is reasonable to assume in this situation that the information has not been accessed by an unauthorized individual, and no breach has occurred.

3) A nurse mistakenly hands a patient the discharge papers belonging to another patient, but she quickly realizes her mistake and recovers the information. If the

[2] Section 13402(j) of the HITECH Act states that the breach reporting obligations become effective on September 23, 2009. In the comments to the new Breach Notification Rules, the Secretary stated that HHS "will use [its] enforcement discretion to not impose sanctions for failure to provide the required notifications for breaches that are discovered before 180 calendar days from the publication [of the HHS regulations]," which will be the middle of February 2010.

[3] Of note: the State of California has recently enacted similar requirements for *all* physicians licensed in the state, regardless of whether or not a physician is a covered entity under HIPAA.

[4] Available at http://www.csrc.nist.gov/.

nurse can reasonably conclude that the patient could not have read or otherwise retained the information, then this would not constitute a breach.

In whose hands did the PHI land? – HHS specifically exempts from the notification requirement unintentional access of PHI by a workforce member[5] (both covered entities and business associates) or inadvertent disclosure to a workforce member acting in good faith within the scope of his or her duties, so long as the PHI is not further used or disclosed improperly.

Can the information disclosed cause "significant risk of financial, reputational, or other harm" to the individual? – HHS has provided some guidance to assist physicians and business associates in making this determination. Similar to the workforce member exemptions above, there may be less risk of harm to the individual(s) if PHI was impermissibly disclosed to another entity governed by the HIPAA Privacy and Security Rules or to a Federal agency. This is because the recipient entity is obligated to protect the privacy and security of the information it received in the same or similar manner as the entity that disclosed the information. For example: you inadvertently fax PHI to the wrong doctor's office, and a staff member from that office subsequently informs you that they received the information in error and have shredded it. It would be reasonable to assume in this situation that the patient is not at risk of significant harm as a result of this breach; therefore, notification of the breach would not be required.

Of course, if the staff member informs you that she saw the patient name, realized it was her brother-in-law and read the fax, this could constitute a breach, depending on the nature of the information. According to HHS: "The risk assessment should be fact specific, and the covered entity or business associate should keep in mind that many forms of health information, not just information about sexually transmitted diseases or mental health, should be considered sensitive for the purposes of the risk of reputational harm – especially in light of fears about employment discrimination." (*Breach Notification for Unsecured Protected Health Information; Interim Final Rule)*

Method of notification

If it is determined that the breach poses a risk of harm and notification is required, the covered entity will notify the affected patient(s), HHS, and, in some cases, the media. Annual notice to the Secretary of HHS suffices for breaches involving fewer than 500 individuals. For breaches affecting 500 or more individuals, HHS must be notified "without reasonable delay" and media outlets must be notified of the breach.

A breach is considered discovered on the first day a covered entity or BA knows or *should have known* about it. Victims of breaches must be notified without unreasonable delay but in no case later than 60 calendar days after discovery of the breach. Delays in notification must include evidence demonstrating the necessity of the delay.

When notifying individuals (or their next of kin if an individual has died) about a breach, the covered entity or BA giving notification must:

- Provide written notification by first-class mail or, if the individual has indicated a preference, via e-mail (consent must be obtained for e-mails) and send follow-up mailings, if necessary, as more information becomes available.
- If the contact information is outdated or insufficient, substitute notice reasonably calculated to reach the individual must be made.
- If there is outdated or insufficient information for fewer than ten individuals, substitute notice may be provided by an alternative written notice, telephone, or other means.
- If contact information for ten or more affected individuals is outdated or insufficient, the covered entity must provide substitute notice either by conspicuous posting on the home page of the covered entity's web site (for at least 90 days) or in major print or broadcast media likely to be seen by the patients. A toll-free number must be provided for at least 90 days where individuals can learn

[5] Workforce member is a defined term in 45 CFR 160.103 and means "employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not hey are paid by the covering entity."

whether their unsecured PHI was included in the breach.

Contents of notice

Notification to patients must include a brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known; the type of protected health information disclosed (such as full name, Social Security number, date of birth, home address, account number, or disability code); the steps the patient should take to protect himself or herself; what the covered entity is doing to investigate and mitigate the breach; and contact information, including a toll-free telephone number, e-mail address, Web site, or postal address by which patients can ask follow-up questions and obtain additional information.

Law enforcement exception

If a law enforcement official states that notification of a breach would impede a criminal investigation or cause damage to national security, the covered entity shall delay notification until the time specified in writing by the law enforcement official. If the statement is oral, document the request, including the name of the official, and delay notification no longer than 30 days unless the official submits a request in writing during this period specifying a longer delay.
(45 CFR §164.412)

Business Associate Agreements

Business Associates are those who use health information as they are performing services on behalf of a covered entity, such as legal, accounting, consulting or administrative work. The HIPAA privacy rules already require covered entities to have "Business Associate Agreements" with such entities for the purpose of protecting patient information. These agreements must be updated to incorporate the data-breach notification requirements, including a detailed description of the time frame, method and content of the notification.

Penalties and enforcements

HITECH imposes penalties for noncompliance due to willful neglect and authorizes HHS to investigate any complaint of suspected noncompliance. In the event of noncompliance, the violating party may be subject to tiered civil monetary penalties – based on the amount of neglect and intent—from $100 to $1.5 million per violation. HITECH also requires HHS to perform periodic audits to ensure that covered entities and business associates are in compliance. The legislation also empowers state attorney generals to enforce some HIPAA elements, which could lead to more scrutiny from prosecutors looking for high-profile cases.

Patient control of access to PHI strengthened

The HITECH Act strengthens protections for patients who want to limit how their information is shared. If a patient requests that a covered entity restrict the disclosure of his or her information, the entity must comply with the request under certain circumstances.

Patient access to medical records in electronic format

If a covered entity uses an electronic medical record (EMR), patients have a right to obtain a copy of their records in electronic format. HITECH specifically states that covered entities may receive remuneration in exchange for PHI when providing copies electronically to the patient or a third party if the choice is clear and specific; however, the cost for such copying and transfer cannot exceed the entity's cost.

Marketing and fundraising materials

Patients are allowed to opt out of their information being used in fundraising and marketing materials. Covered entities should obtain patient authorization before using PHI for such purposes.

Limit disclosure of PHI to "minimum necessary," including to health plans

Limit the disclosure of PHI to a "limited data set," or to the "minimum necessary" to fulfill an intended purpose (as defined under the HIPAA Privacy Rule), including those disclosures you make to health plans.

The covered entity makes the determination of the minimum necessary to accomplish the intended purpose. The following exceptions to the minimum necessary requirement continue to apply under (*45 CFR §164.502(b)(2)*:)

- Disclosures/requests by a health care provider for treatment;
- Uses/disclosures to the patient;
- Uses/disclosures made pursuant to an authorization;
- Disclosures to the HHS Secretary;
- Uses/disclosures required by law; and
- Uses disclosures required for HIPAA compliance.

According to HHS, uses or disclosures of PHI that involve more than the minimum necessary information may qualify as breaches under the data breach notification regulations.

"Meaningful use" of EHRs tied to Medicare/Medicaid incentive payments

In addition to the changes to HIPAA, HITECH established programs to provide incentive payments to eligible professionals participating in Medicare and Medicaid that adopt and make "meaningful use" of certified EHR technology. Incentive payments for physicians may begin in January 2011. MIEC will publish additional information as the definition of "meaningful use" when the certification process is clarified. The CMS proposed rule and fact sheets may be viewed at http://www.cms.hhs.gov/Recovery/11_HealthIT.asp

Requests to withhold PHI from health plans

If an individual requests that there be no disclosure to a health plan for health care operations or payment purposes and the health care provider has been paid out-of-pocket in full, the covered entity must grant the request.

On the horizon: Accounting of disclosures requirement expanded for EMR

Under HIPAA, covered entities have been required to produce, upon patient request, an accounting of "non-routine" disclosures of the patient's protected health information for the three years prior to the request. Such disclosures are those that do *not* fall under the categories of treatment, payment or operations. Covered entities have maintained logs of non-routine disclosures in order to be able to produce an accounting of such disclosures as needed. This requirement is still in effect for paper records.

HITECH has expanded this requirement in the respect that covered entities that use EMRs must, upon patient request, produce an accounting of *all* disclosures within the past three years, including non-routine disclosures *and* those that fall under treatment, payment or operations. This provision does not go into effect until January 1, 2014, if the covered entity used an EMR as of January 1, 2009. For those who obtain an EMR after January 1, 2009, the effective date is the later of January 1, 2011 or the date the covered entity obtained the EMR. Physicians who use an EMR in their private practices should ensure that the capability exists to produce an accounting of disclosures.

Upon request of an accounting, a covered entity has the choice of either providing an accounting of disclosures of information made by the covered entity and by business associates acting on behalf of the covered entity, or it must provide a list of all business associates (and their contact information) acting on behalf of the covered entity. (This decision should be predetermined and stated in the Business Associate Agreement.)

Resources:

HIPAA Privacy Rule info from HHS and OCR
http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html
HIPAA Security Rule guidance and educational papers from CMS
http://www.cms.hhs.gov/SecurityStandard/
http://www.cms.hhs.gov/EducationMaterials/04_SecurityMaterials.asp#TopOfPage
Full text of the HITECH Act
http://en.wikisource.org/wiki/Health_Information_Technology_for_Economic_and_Clinical_Health_Act
HHS guidance on data breach notification
http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html

We thank Phillip Goldberg, Esq. of Hassard Bonnington for his review of this newsletter.

TO REACH MIEC

Phone:
Oakland Office: 510/428-9411
Honolulu Office: 808/545-7231
Boise Office: 208/344-6378
Outside: 800/227-4527

Fax:
Loss Prevention: 510/420-7066
Oakland: 510/654-4634
Honolulu: 808/531-5224
Boise: 208/344-7903

Email:
Lossprevention@miec.com
Underwriting@miec.com
Claims@miec.com

This newsletter is available in a **podcast** on MIEC's website at: **www.miec.com**

HIPAA Security Rule

The HIPAA Security Rule, which complements the Privacy Rule, has been in effect since April 21, 2005. While the Privacy Rule pertains to all Protected Health Information (PHI) including paper and electronic, the Security Rule deals specifically with Electronic Protected Health Information (ePHI). It lays out three types of security safeguards required for compliance: administrative, physical, and technical. For each of these types, the Rule identifies various security standards, and for each standard, it names both "required" and "addressable" implementation specifications. Required specifications must be adopted and administered as dictated by the Rule. Addressable specifications are more flexible. Individual covered entities can evaluate their own situation and determine the best way to implement addressable specifications. (See **Resources** for more information.)