McCONVILLE CONSIDINE COOMAN & MORIN PC
ATTORNEYS & COUNSELORS AT LAW

IN CONFIDENCE LEGAL NEWS

Work With Us. In Confidence.

Breach Notification Requirements For HIPAA Covered Entities and Business Associates

Author:

AMY L. VAREL

Practice Areas
Business
Health Care
Employment

September 18, 2009 — The Health Information Technology for Economic and Clinical Health Act (the "HITECH Act") (enacted on February 17, 2009) requires that all HIPAA covered entities ("Covered Entities") that access, maintain, retain, modify, record, store, destroy, or otherwise hold, use, or disclose "Unsecured Protected Health Information" shall, in the event of a breach of such information that is discovered by the Covered Entity, notify each individual whose Unsecured Protected Health Information has been, or is reasonably believed by the Covered Entity to have been, accessed, acquired, or disclosed as a result of such breach.

The HITECH Act also requires that a Business Associate of a Covered Entity notify the Covered Entity in the event of any such breach. "Unsecured Protected Health Information" or "Unsecured PHI" is defined in the HITECH Act as protected health information that is not secured as specified by guidance to be issued by the Secretary of the Department of Health and Human Services ("HHS").

The April 17, 2009 Guidance

On April 17, 2009 HHS issued guidance that stated that if Protected Health Information ("PHI") is rendered unusable, unreadable or indecipherable to unauthorized individuals by one of the following methods, then it is not "Unsecured PHI":

i) Encryption of electronic PHI as specified in the guidance, and;
ii) Destruction of the media on which the PHI is stored or recorded as described in the guidance.

Covered Entities are not required to follow the April 17, 2009 guidance. However, it is recommended that Covered Entities and Business Associates comply with the April 17, 2009 guidance since the breach notification requirements that are contained in the HITECH Act apply only to breaches of Unsecured PHI.

If PHI is not Unsecured PHI, then Covered Entities and Business Associates are not required to comply with the notification requirements for breaches of such PHI.

The Interim Final Rule

HHS issued an Interim Final Rule entitled "Breach Notification For Unsecured Protected Health Information" on August 19,2009. The new regulations require that a Covered Entity shall notify each individual whose Unsecured PHI has been, or is reasonably believed by the Covered Entity to have been, accessed, acquired, used, or disclosed as the result of such breach no later than sixty (60) calendar days after the discovery of the breach. For breaches of Unsecured PHI involving more than 500 residents of a state or jurisdiction, notification to the media is required.

25 East Main Street
Rochester, NY 14614

Phone: 585-546-2500
Fax: 585-546-7218
www.mccmlaw.com

McCONVILLE CONSIDINE COOMAN & MORIN PC
ATTORNEYS & COUNSELORS AT LAW

IN CONFIDENCE LEGAL NEWS

Work With Us. In Confidence.

(Continued from page 1)

The Interim Final Rule provides that a breach is treated as discovered by a Covered Entity as of the first day on which such breach is known to the Covered Entity, or, by exercising reasonable diligence would have been known to the Covered Entity. The Covered Entity shall be deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent of the Covered Entity.

The commentary to the Interim Final Rule states that if a Business Associate is acting as an agent of a Covered Entity, then the discovery of the breach by the Business Associate would be imputed to the Covered Entity. In those cases, the Covered Entity must provide notification of the breach within sixty (60) days after the Business Associate discovers the breach.

In contrast, if the Business Associate is an independent contractor of the Covered Entity (i.e., not an agent), then the Covered Entity must provide notification based on the time the Business Associate notifies the Covered Entity of the breach. Therefore, HHS recommends that Covered Entities may wish to address the timing of the notification in their Business Associate Agreements.

For breaches of Unsecured PHI involving less than 500 individuals, a Covered Entity is required to maintain a log or other documentation of such breaches and, not later than sixty days after the end of each calendar year, notify the Secretary of HHS of the breaches. For breaches of Unsecured PHI involving 500 or more individuals, the notice to HHS must be provided within sixty days of discovery of the breach.

The Interim Final Rule applies to breaches that are discovered for a Covered Entity or a Business Associate on or after September 23, 2009. However, HHS has stated that it will use its enforcement discretion to not impose sanctions for failure to provide the required notification for breaches that are discovered before February 22, 2010. During that initial time period HHS has stated that it expects Covered Entities to comply with the Interim Final Rule and will work with Covered Entities, through technical assistance and voluntary corrective action, to achieve compliance.

New Requirements For Business Associates

The HITECH Act provides that, effective as of February 17, 2010, Business Associates will be directly subject to certain HIPAA provisions as well as all of the new requirements that are contained in the HITECH Act. The HITECH Act further requires that the provisions of the HITECH Act be incorporated into the Business Associate Agreements between the Business Associates and Covered Entities.

The HITECH Act and the Interim Final Rule require that a Business Associate shall, following the discovery of a breach of Unsecured PHI, notify the Covered Entity of such breach. The Interim Final Rule details the requirements of that notice.

25 East Main Street
Rochester, NY 14614

Phone: 585-546-2500
Fax: 585-546-7218
www.mccmlaw.com

McCONVILLE CONSIDINE COOMAN & MORIN PC
ATTORNEYS & COUNSELORS AT LAW

IN CONFIDENCE LEGAL NEWS

Work With Us. In Confidence.

(Continued from page 2)

What Needs To Be Done Now?

The Interim Final Rule and the HITECH Act require Covered Entities and Business Associates to:

- Implement policies and procedures with respect to PHI that are designed to comply with the HITECH Act and the Interim Final Rule (the "Policies and Procedures").
- Train all members of its workforce on the Policies and Procedures as necessary and appropriate.
- Provide a process for individuals to make complaints concerning the Policies and Procedures or its compliance with the Policies and Procedures.
- Have and apply appropriate sanctions against members of its workforce who fail to comply with the Policies and Procedures, the HITECH Act and the Interim Final Rule.

We also recommend that Covered Entities consider taking the following actions:

- Ensure compliance with the April 17, 2009 guidance so that any PHI is not "Unsecured PHI" that will require compliance with the notification requirements of the HITECH Act in the event that a breach occurs.
- Amend the Covered Entity's Business Associate Agreements that it has entered into with agents of the Covered Entity to address the timing of the notification of a breach by a Business Associate.
- Amend the Covered Entity's Business Associate Agreements to require the Covered Entity's Business Associates to comply with the April 17, 2009 guidance.

Business Associates should expect that the Covered Entities with which they do business may begin to require their Business Associate Agreements to be updated.

What Needs To Be Done In The Near Future?

In order to comply with the HITECH Act, all Business Associate Agreements need to be amended by February 17, 2010 to incorporate the provisions of the HITECH Act.

For questions regarding the new HIPAA breach notification requirements, contact Amy Varel at (585) 546-2500 or avarel@mccmlaw.com.

25 East Main Street
Rochester, NY 14614

Phone: 585-546-2500
Fax: 585-546-7218
www.mccmlaw.com