SMITH ANDERSON

September 2009

Client Alert

# Evolving Beyond State Law: New Federal HIPAA Requirements for Breaches of Protected Health Information Effective September 23, 2009

On August 24, 2009, the Department of Health and Human Services (HHS) published an interim final rule requiring HIPAA covered entities *and* business associates to provide certain written notification in response to "breaches" of "unsecured protected health information." The rule was issued pursuant to the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act"), passed by Congress as part of the American Reinvestment and Recovery Act of 2009. Where, previously, data breach notification has been a matter of state law, this new rule marks the first federal data breach notification requirement.

The breach notification requirements become effective September 23, 2009, and apply to breaches that occur *on* or *after* September 23, 2009. Steps to take *prior to* September 23, 2009 are included in this Client Alert.

## WHAT ENTITIES ARE COVERED BY THE RULE?

The interim final rule (the "Rule") applies to *covered entities* and *business associates* subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

## WHAT DOES THE RULE REQUIRE?

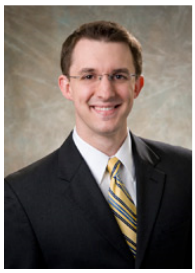
Following discovery of a "breach" of "unsecured protected health information" (as described below), HIPAA *covered entities* are required to notify *each individual* whose unsecured protected health information (PHI) has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of a breach of unsecured PHI. In addition, HIPAA *business associates* are required to notify HIPAA *covered entities* following the business associate's discovery of a breach of unsecured PHI.

### *What Constitutes a Breach?*

The Rule defines a *breach* as the acquisition, access, use, or disclosure of PHI that (a) is not permitted under HIPAA and (b) poses a significant risk of financial, reputational, or other harm to the individual.

Bo Bobbitt
BIO | 919.821.6612
bbobbitt@smithlaw.com

Alicia Gilleskie
BIO | 919.821.6741
agilleskie@smithlaw.com



Frederick Zufelt
BIO | 919.821.6727
fzufelt@smithlaw.com

***What is Unsecured PHI?***

The notification requirements apply only to breaches of *unsecured PHI*. The Rule defines unsecured PHI as PHI that is *not* rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary of HHS (the "Secretary"), in guidance available on the HHS website.

The 2 methods of rendering PHI unusable, unreadable, or indecipherable specified by the Secretary are (a) encryption, and (b) destruction. Detailed guidance from the Secretary regarding each of these methods may be accessed at: http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/federalregisterbreachrfi.pdf.

**THE NOTIFICATION REQUIREMENTS**

Covered entities must notify affected individuals without unreasonable delay, but no later than 60 days following the covered entity's *discovery* of the breach. A "breach" is deemed to have been *discovered* when the covered entity actually knows of the breach, or, with the exercise of reasonable diligence *would have known of* the breach.

The covered entity's notification to affected individuals must include: (a) a description of what happened, (b) a description of the types of unsecured PHI involved, (c) any steps affected individuals should take to protect themselves, (d) a description of what the covered entity is doing to investigate the breach, mitigate harm to individuals, and protect against further breaches, and (e) contact procedures for affected individuals, which must include a toll-free telephone number, an email address, website, or postal address.

Business associates are required to notify the covered entity "to which the breached information relates" without unreasonable delay, but no later than 60 days following the business associate's discovery of the breach. As with covered entities, a breach is deemed to have been discovered when the covered entity actually learns of the breach, or, with the exercise of reasonable diligence *would have known* of the breach. To the extent possible, the business associate's notice to the covered entity must identify the affected individuals and include any other information available to the business associate that the covered entity is required to provide in its notice to affected individuals.

***Method of Notification***

Covered entities must notify affected individuals as follows:

> Directly, by first-class mail at the individual's last known address, or by electronic mail if the individual has agreed to electronic notice.
>
> Where there is insufficient or out-of-date contact information for written notification, covered entities may use "substitute notice," as follows:
>
> - For *less than 10* individuals, substitute notice must be provided by an alternate form of written notice, telephone, or other means;
> - For *10 or more* individuals, substitute notice must be given by (a) conspicuous posting for a period of 90 days on the home page of the covered entity's website, or (b) conspicuous notice in major print or broadcast media – both of which must also include a toll-free number that is active for at least 90 days.

***Who Must Be Notified?***

Covered entities must notify individuals who are the subject of the breach. In addition, if more than 500 residents of a particular state or jurisdiction are affected, the covered entity must notify prominent media outlets serving the state or jurisdiction. Such notice must be made without unreasonable delay, but in no event later than 60 days after the covered entity's discovery of the breach.

Covered entities are also required to notify the Secretary of all breaches of unsecured PHI. If a breach affects 500 or more individuals, the notice to the Secretary should be made contemporaneously with the notice to affected individuals. If less than 500 individuals are involved, the covered entity is required to maintain a log of the breach, and provide notification to the Secretary within 60 days after the end of the calendar year.

**STEPS TO TAKE PRIOR TO SEPTEMBER 23, 2009**

In connection with the breach notification requirements described above, covered entities must:

- Implement policies and procedures to address the new breach notification requirements that include sanctions for failure to comply;
- Train members of their workforce on these polices and procedures, as necessary and appropriate for the members of the workforce to carry out their employment functions; and
- Implement a process for individuals to make complaints regarding the covered entity's compliance with the breach notification requirements.

Business associates should also take measures to ensure that they are able to comply with the new breach notification requirements. While not expressly required by the Rule, such measures include implementing policies and procedures and training programs as described above.

If you need assistance implementing measures that comply with these new requirements, or have questions about any privacy matter, please contact the Smith Anderson lawyer with whom you work or one of the Smith Anderson lawyers featured on the front page.

**SMITH, ANDERSON, BLOUNT, DORSETT, MITCHELL & JERNIGAN, L.L.P.**

**Offices:**
2500 Wachovia Capitol Center
Raleigh, North Carolina 27601
**Mailing Address**:
Post Office Box 2611
Raleigh, North Carolina 27602
**Telephone**: 919-821-1220
**Facsimile**: 919-821-6800
**Email**: Info@smithlaw.com **Website**: www.smithlaw.com