GROOM LAW GROUP

Christy Tinnes, Groom Law Group
202-861-6603 / cat@groom.com

CHART YOUR HIPAA COURSE . . .

HHS ISSUES SECURITY BREACH NOTIFICATION RULES

PUBLISHED IN FEDERAL REGISTER 8/24/09
EFFECTIVE 9/23/09

The Department of Health and Human Services ("HHS") has issued interim final rules on HIPAA's new security breach notification requirement, which was adopted under the HITECH Act in February as part of the stimulus bill. The HITECH Act made significant changes to the HIPAA privacy and security rules, including imposing a new requirement that covered entities notify individuals when their "unsecure" protected health information ("PHI") is breached.

Generally, the HITECH Act requires that covered entities (health plans and health care providers, such as doctors and hospitals) notify individuals if their unsecure protected health information is breached. The notice must be provided to individuals within 60 days after discovery by first class mail (or email if specified as a preference by the individual). If the breach is large enough (generally, involving 500 people), the covered entity must notify the media and HHS, which will list the covered entity on its website.

HHS issued interim final rules on the new requirement August 24, 2009 and specifically asked for comments on certain areas. Comments are due October 23, 2009. (Note that HHS informally has indicated that it will issue proposed regulations on other HITECH Act requirements before the end of the year.)

The HITECH Act also required the FTC to issue security breach notification rules for personal health records ("PHR") vendors. The FTC's rules are published in the August 25, 2009 Federal Register (a day after the HHS rules). While similar, the FTC rules are different, so entities that perform PHR functions should review both rules to determine which would apply. This summary focuses on the HHS rules.

New HHS Rules

When is this Requirement Effective?

The HITECH Act mandates that the security breach notification requirement goes into effect 30 days after HHS publishes final regulations in the Federal Register. The rules were published August 24, 2009, so are effective September 23, 2009.

However, HHS says it understands that it may take time for covered entities to build systems and procedures to come into compliance, so it will not impose sanctions for failure to provide notifications that are discovered before 180 days from date of publication – or February 22, 2010. HHS says that, during this period, it still expects covered entities to comply with the

rule and that it will work with them to achieve compliance through technical assistance and voluntary corrective action.

What Information is Subject to New Notification Rule?

The security breach notification rule only applies to "unsecure" PHI. On April 17, 2009, HHS issued guidance regarding what information it would consider "secure" and thus, exempt from the new notification rule. Generally, HHS said that, in order to be considered "secure," information must be encrypted or completely destroyed.

As a part of the new rules, HHS restated its former guidance – to be secure, information must either be encrypted under specific standards adopted by the National Institute of Standards and Technology ("NIST") or must be destroyed so that it cannot be read or reconstructed. If electronic, the information must be "cleared, purged, or destroyed" consistent with specific NIST standards.

HHS specially said that additional means of safeguarding information, such as access controls, firewalls, or redaction would not cause information to be "secure." This means that, unless a covered entity's PHI is encrypted under the standards adopted by HHS, or completely destroyed, it will be subject to the security breach notification requirement. Such information might include information on paper, information in use, information transferred internally, or information that has been redacted or aggregated, but not fully de-identified.

What is a Breach?

The HHS regulations provide that a breach will occur if 4 requirements are met:

1. Information is "unsecure" under the guidance discussed above (that is, not encrypted or destroyed).

2. Information was used or disclosed in an "unauthorized" manner. HHS says this means that the information was used or disclosed in a manner that is not permitted under the HIPAA privacy rules and notes that this includes a violation of the minimum necessary rule.

3. The use or disclosure poses a "significant risk of financial, reputational, or other harm to the individual." HHS says covered entities must perform a risk assessment to determined if harm has occurred and review factors such as to whom the information was disclosed, the type of information disclosed, and what steps were taken upon discovery of the use or disclosure. HHS noted that information kept in a limited data set generally is not exempt from the breach rule, although disclosure of this information may not pose as great a risk under the "harm" requirement.

4. The use or disclosure does not fall under an exception listed in the statute. The HITECH Act offered 3 exceptions, which the regulations explain further.

    - *Unintentional access by an covered entity's or business associate's employee*. HHS says the access must be in good faith, within the employee's course and scope of employment, and not result in further use or disclosure. HHS gives an example of a nurse mistakenly sending an email with PHI to a hospital's

billing employee, who opens it in the normal course of business. The billing employee deletes the email and notifies the nurse.

- *Inadvertent disclosure from one covered entity or business associate employee to another similarly situated employee*. HHS says the information must not be further used and that "similarly situated" means both employees must be authorized to access the information. For example, a doctor and billing employee may be similarly situated in that they are both authorized to view PHI, but a doctor and receptionist may not be.

- *The recipient would not reasonably have been able to retain the information*. HHS gives an example where a health plan sends out explanations of benefits ("EOBs") to the wrong individual. If the EOB envelope is returned unopened, the plan could determine that the recipient did not retain the information (for EOBs that are not returned, HHS says this likely would be a "breach"). HHS gives another example of a nurse giving out incorrect discharge papers but immediately discovering the error and taking them back.

When is Individual Notice Required?

If there is a breach, the covered entity must notify the individual "without unreasonable delay," but no later the 60 days after discovery of the breach. The breach will be considered discovered on the first day it is known to any member of the covered entity's workforce (other than the person who committed the breach), or the date it would have been known if the covered entity exercised reasonable diligence. HHS notes that 60 days is the "outer limit" and, depending on the circumstances, it may be an unreasonable delay to wait until the 60th day to provide the notification. HHS also notes that if a business associate is an "agent" of the covered entity, the business associate's discovery of the breach will be imputed to the covered entity; otherwise, the business associate must report the breach to the covered entity within 60 days after discovery, at which time the breach will be considered known to the covered entity.

The notice must be written in "plain language" and contain:

- A brief description of what happened, including the date of the breach and date of discovery;

- The types of PHI involved (such as whether full name, SSN, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);

- Any steps individuals should take to protect themselves from potential harm;

- A brief description of steps the covered entity is taking to investigate, mitigate losses, and protect against further breaches.

- Contact information for individuals to ask questions, including a toll-free telephone number, email address, website, or postal address.

Notice must be sent to the individual's last known address, or by email if the individual agrees. HHS notes that notices to minors generally can be sent to parents and notices to deceased individuals generally can be sent to next of kin or a personal representative, consistent with the HIPAA privacy rules.

What if a Covered Entity Has Insufficient Contact Information or Notification is Returned?

If insufficient or out-of-date contact information precludes individual notice, the covered entity must provide a substitute form of notice. The HHS rules provide that:

- *If fewer than 10 individuals are involved* – The substitute notice may be an alternative form of notice that is reasonably calculated to reach the individuals, such as by telephone, email, or posting on the covered entity's website.

- *If 10 ore more individuals are involved* - The covered entity must either post the notice on its homepage for 90 days or provide notice in major print or broadcast media in the geographic areas where affected individuals are likely to reside. Note that a covered entity can choose which approach to take. Under either approach, the covered entity must maintain a toll-free number for 90 days so individuals can ask questions.

  For website posting, HHS says the notice must be prominent so that it is noticeable given its size, color, and graphic treatment in relation to the other parts of the page, and worded to convey the nature and importance of the information. The notice should be included both on the homepage and "landing page" for existing account holders.

  For media notice, HHS says that what constitutes major media will depend on the geographic area and that a covered entity may need to utilize multiple media outlets to reach affected individuals.

When is Media Notice Required?

Outside of the substitute notice above, the regulations also require a covered entity to notify the media where the breach involves more than 500 residents in a state. The notice must be made to "prominent media outlets" serving the state, include the same content as the individual notice, and be provided within the same timeframe (i.e., 60 days). Rather than the more "legal" form of the substitute notice, HHS says this media notice may be in the form of a press release (which presumably, the media may choose to report on or not).

HHS says what constitutes a prominent media outlet will differ depending on the state. HHS also clarifies that the notice requirement only is triggered if the breach involves more than 500 residents of a particular state. If the breach involves 200 residents each of three neighboring states, no notice would be required.

When is Notice to HHS Required?

The HITECH Act requires covered entities to notify HHS of any security breach, based on the number of individuals involved.

- *Where a breach involves 500 or more people* - The statute requires a covered entity to notify the Secretary of HHS immediately. HHS notes that requirement applies regardless of an individual's state, so a breach that does not trigger the media notice (which applies to more than 500 residents in a state) may still trigger immediate notice to HHS. The new rules interpret "immediately" to mean contemporaneously with the individual notice (that is, within 60 days). HHS says it will post instructions for notification on its website, where it also will post the names of those covered entities that report security breaches involving 500 or more people.

- *Where a breach involves less than 500 people* - The rules require a covered entity to maintain a log of security breaches and submit it to HHS on an annual basis. HHS says that it will post instructions on its website and that the log must be filed within 60 days after the end of the calendar year. HHS also notes that, for 2009, the filing only is required to include breaches occurring on or after 9/23/09, the effective date of the new rules. (As discussed above, HHS indicated it will not enforce the new rules before 180 days from publication in the Federal Register, but apparently it still intends for plans to maintain and file the log even before this date.)

Does HIPAA Supplant State Law Notice Requirements?

HHS adopts HIPAA's existing preemption rule and says that state notification laws will not be preempted unless "contrary to" the HIPAA requirement. HHS says it believes that most state laws will not conflict with the HIPAA rule and gives an example where a state law requires notification within 5 days. HHS says notice within this period also would satisfy the new HIPAA requirement, so the two laws would not conflict. Similarly, if a state law requires additional elements to be included in a notice, HHS says there would be no conflict because a covered entity could develop a notice that satisfies both laws.

Steps Plans Should Take

- Establish Notice Procedures – Covered entities will need procedures to determine when a breach has occurred, who will prepare individual notifications, and when a breach will trigger a requirement for notice to the media or immediate notice to HHS.

- Maintain Breach Log – Covered entities must establish a system to log security breaches, which the covered entity must file with HHS within 60 days after the end of the year.

- Revise Business Associate Agreements – Covered entities should negotiate with their business associates regarding the timing for a business associate to notify the covered entity of a breach by the business associate, what information should be reported, and which party will issue the required notifications.

- Enhance Training – HHS noted the need for additional training since the 60-day breach notification date will be triggered from the date a breach is discovered by anyone in the covered entity's workforce. Workforce members should understand when they have encountered a breach and how to report it.

- Update Privacy Procedures - HHS expressly amended the HIPAA privacy regulations to require that the security breach notification rule be incorporated into the covered entity's policies and procedures, training, complaint process, and sanctions.

Please feel free to call us if you have questions on the new requirements or need assistance developing or updating your HIPAA privacy procedures, training, or business associate agreements.

* * *

Contact Christy Tinnes, 202/861-6603 (cat@groom.com) to be added to the HIPAA Update list.

We will provide updates on further developments. In the meantime, if you have any questions, please contact your regular Groom attorney or any of the Health and Welfare Practice Group attorneys listed below:

Jon W. Breyfogle	jwb@groom.com	(202) 861-6641
Jenifer A. Cromwell	jac@groom.com	(202) 861-6329
Thomas F. Fitzgerald	tff@groom.com	(202) 861-6621
Cheryl Risley Hughes	crh@groom.com	(202) 861-0167
Debbie G. Leung	dgl@groom.com	(202) 861-2601
Christine L. Keller	clk@groom.com	(202) 861-9371
Tammy Killion	tsk@groom.com	(202) 861-6328
Christy A. Tinnes	cat@groom.com	(202) 861-6603
Donald G. Willis	dgw@groom.com	(202) 861-6332