WYATT TARRANT & COMBS LLP

SEPTEMBER 2009

# HEALTH CARE LAW UPDATE

## SWEEPING NEW DATA BREACH REGULATIONS IMPACT HEALTHCARE INDUSTRY, EMPLOYERS WITH SELF-INSURED HEALTH PLANS, AND VENDORS

Erin Brisbay McMahon
Partner
emcmahon@wyattfirm.com

On August 24, 2009, sweeping new data breach regulations were published in the Federal Register. These regulations go into effect on September 23, 2009. The regulations may be accessed at: http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf

The regulations apply to "Covered Entities" (CEs) under the Health Insurance Portability and Accountability Act of 1996 (HIPAA): healthcare providers, health plans (including health insurers and self-insured employee benefit plans), and healthcare clearinghouses that assist providers in billing healthcare claims. The regulations also apply to the "Business Associates" (BAs) of CEs. BAs are entities that need "Protected Health Information" (PHI) to perform a service for a healthcare provider, health plan, or healthcare clearinghouse.

Unlike most state data breach notification laws that require notifications to be sent to individuals if certain financial information (such as a social security number) is improperly disclosed, lost, or stolen, the new federal regulations, require an examination of every violation of the HIPAA Privacy Rule that a CE or BA has to determine the level of harm to individuals. The CE or BA will then need to decide whether to notify an individual of the incident and keep documentation about its decision. Further, CEs must notify the Department of Health and Human Services (HHS) of all breaches that occur at their facilities and all breaches committed by their BAs.

HHS, which issued the regulations, stated that it would not impose sanctions on any entity for failure to make the required notifications for breaches occurring between September 23, 2009 and February 20, 2010. However, all entities affected by the regulations must start logging breaches that occur on and after September 23.

### What is a Breach?

A breach is defined as the acquisition, access, use, or disclosure of PHI that (a) violates the HIPAA Privacy Rule and (b) compromises the security or privacy of the PHI. "Compromises the security or privacy of the PHI" means that the breach has posed a significant risk of financial, reputational, or other harm to the individual. To determine whether a breach has occurred, a CE or BA must investigate an incident, determine whether a violation of the Privacy Rule has occurred, and analyze whether the breach poses a significant risk of harm to the individual. In performing the risk assessment, CEs and BAs should consider

a number of factors:

- Who impermissibly used the information or to whom the information was impermissibly disclosed. If, for example PHI was impermissibly disclosed to a CE, then there is probably less of a risk of harm to the individual, since the recipient entity has an obligation to protect the privacy and security of the information it received.
- Did the CE or BA take immediate steps to mitigate an impermissible use or disclosure? If the CE or BA obtains a recipient's satisfactory assurances that the information will not be further used or disclosed or will be destroyed, and if such steps eliminate or reduce the risk of harm to the individual to less than a "significant risk," then no breach has occurred.
- Impermissibly disclosed PHI is returned prior to it being accessed for an improper purpose. For example, if a laptop is lost or stolen and then recovered and a forensic analysis of the computer shows that its information was not opened, altered, transferred, or otherwise compromised, the breach probably does not pose a significant risk to the individuals whose information was on the laptop.
- The type and amount of PHI involved in the impermissible use or disclosure. For example, if the information indicated the type of services that the individual received (such as oncology services), that the individual received services from a specialized facility (such as a substance abuse treatment program), or if the PHI includes information that increases the risk of identity theft (such as a social security number or mother's maiden name), then there is a higher likelihood that the impermissible use or disclosure compromised the security and privacy of the information.

### Exceptions to What Constitutes a Breach

There are four exceptions to what constitutes a breach under the regulations. The CE or BA must document why the incident qualifies for one of these exceptions and keep that documentation for six years from the date on which the incident occurred.

- An unintentional acquisition, access, or use of PHI by a workforce member (e.g., employee, trainee, volunteer) acting under the authority of the CE or BA and within the scope of employment or other professional relationship, if no further use or disclosure not permitted by the Privacy Rule occurs. For example, if a nurse mistakenly sends an e-mail containing PHI to a billing employee and the billing employee recognizes that he/she is not the intended recipient, deletes the e-mail, and alerts the nurse of the misdirected e-mail, there is no breach. Again, however, this must be documented in a log of incidents kept by the CE or BA.
- An inadvertent disclosure of PHI from a person authorized to access PHI at a CE or BA to another person authorized to access PHI at the same CE, BA or organized health care arrangement in which the CE participates, as long as the recipient does not further use or disclose the PHI in violation of the Privacy Rule. For example, a physician who has authority to use or disclose PHI at a hospital by virtue of participating in the organized health care arrangement between the hospital and its physicians is similarly situated to a nurse or billing employee at the hospital who also has authority to use or disclose PHI at that hospital. If the physician mistakenly sends PHI to a nurse not involved in a patient's care, that nurse should notify the physician of the inadvertent disclosure, delete the e-mail, and report the incident to the hospital. The hospital would log the incident but not report it as a breach.

- The CE has a good faith belief that the person to whom the inappropriate disclosure was made would not reasonably have been able to retain the information. For example, if a nurse mistakenly hands a patient discharge papers belonging to another patient but quickly realizes her mistake and retrieves the papers, and if the nurse can reasonably conclude that the patient could not have read or otherwise retained the information, no breach has occurred. However, the nurse must report the incident to the CE and the CE must log the incident and keep the log of the incident for six years after the date it occurred.
- If a limited data set (as that term is defined in the Privacy Rule) that has been stripped of sixteen patient identifiers is improperly used or disclosed, that does not constitute a breach if zip codes or dates or birth were also removed. Again, the CE must document that the lost information did not include any of these identifiers, and keep documentation about the incident for six years after the date on which it occurred.

Practical Tips--Develop a Data Breach Response Plan Now

- Assign a compliance person to receive incident reports of potential breaches. This person should have an understanding of the HIPAA Privacy and Security Rules.
- Assemble an internal data breach response team including the compliance person responsible for receiving incident reports, the privacy officer, the security officer, internal or external legal counsel, and a public relations person.
- Develop a data breach notification policy and train your workforce on it by September 23, 2009, the day the regulations go into effect. Your workforce needs to be able to recognize violations of the HIPAA Privacy Rule and report them to the compliance person so that your organization can document an investigation and determine whether there is a breach that requires notification.
- When performing an internal investigation, don't let time slip away. When a breach has occurred, HHS expects notifications to be sent to affected persons without unreasonable delay. If social security numbers or credit card numbers are involved, notices should be sent as soon as possible. For this reason, it is critical to appoint a compliance person to receive incident reports that does not have too much on his or her plate already.
- Decide under what circumstances law enforcement will be notified. Usually this will occur if stolen laptops or phones with unencrypted PHI stored on them are involved.
- Try to develop public relations strategies for different scenarios, recognizing that news of the breach could hit social media before it ever hits traditional media. If your company had a data breach involving several hundred patients, what would the press release look like? You definitely want to stay ahead of the story in this scenario.
- What resources are you willing to provide the individuals who are affected by the breach? Will you set up a call center? Will you provide credit monitoring? In some instances, the answer to these questions will be driven by how many people are affected.
- Draft a form letter for notifications. Notifications must contain a certain number of facts about the breach. Therefore, form letters can be developed to expedite notices to persons affected by the breach.
- Failure to report a possible breach should be subject to progressive discipline because if your organization should have known of the breach, that starts your clock for notification.

### When Individuals Must Be Notified

Notifications must be made no later than 60 days after a breach is discovered, unless law enforcement requests that a delay of notification be made. Breaches are treated as discovered by the CE as of the first date the breach is known to the CE or by exercising reasonable diligence would have been known to the CE through any workforce member or agent (including a BA) of the CE other than the individual committing the breach. If a BA is an agent of the CE, the time for the CE to notify affected persons runs from the BA's discovery, not the time the BA notified the CE. If the BA is an independent contractor, then the CE must provide notification based on the time the BA notifies the CE of the breach. Therefore, it would be prudent to put independent contractor clauses in all BA agreements.

Both CEs and BAs must implement reasonable systems for discovery of breaches. For example, a hospital would want to be able to conduct an audit that would show workforce members who have viewed the record of a high-profile patient after he or she has been discharged.

### What the Notification Must Contain

Regardless of the method of notification, the following information must be written in plain language (depending on whether the CE is subject to the federal Civil Rights Act and The Rehabilitation Act, the notice may also need to be available in other languages, Braille, large print, or audio):

- A brief description of what happened, including the date of the breach and the date of discovery of the breach;
- A description of the types of unsecured PHI that were involved in the breach (such as name, social security number, date of birth, address, account number, diagnosis, or disability code);
- The steps individuals should take to protect themselves from potential harm;
- A brief description of what the CE is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches; and
- Contact procedures for individuals to ask questions or get additional information. The contact procedures must include a toll free number, an e-mail address, a website, or a postal address.

CEs should avoid including sensitive information in the notification itself in case the notification is misdirected.

### Method of Notification

Notifications should be sent first class mail to the last known address of the individual affected or via e-mail if an individual has consented to electronic notification and the consent has not been withdrawn. If an individual that has been affected by a breach is a minor or an incompetent person, the notification should be sent to that person's personal representative. If the individual who has been affected is deceased, and if the CE knows of the death and has the address of the next of kin or personal representative, then the CE should send the notice to the next of kin or personal representative.

If the CE does not have contact information for some number of affected persons or if some notices are returned undeliverable, then the following rules apply:

- If less than 10 people are involved, then the CE may contact them via e-mail or telephone.
- If 10 or more people are involved, then there must be a conspicuous posting for 90 days on the home page of the CE's website (the CE can post a hyperlink on its home page that is

noticeable given its size, color, and graphic treatment in relation to the rest of its home page) or run a conspicuous notice in major print or broadcast media in geographic areas where the individuals affected are likely to reside. Further, if 10 or more people are affected, a toll-free telephone number must be activated for 90 days where an individual can call to learn whether his or her unsecured PHI may be included in the breach. This phone number must be included on the website or in the notice.

- If there is particular concern that misuse could be imminent, such as instances in which a social security number is involved, the CE may choose to alert individuals via telephone. However, a written notice must still be provided.

### Media Notice

If the unsecured PHI of more than 500 residents of a state or jurisdiction is, or is reasonably believed to have been accessed, acquired, or disclosed during a breach, notice must be provided to prominent media outlets in that area. This is in addition to the written notice to the individuals affected. For example, if more than 500 residents of Kentucky are affected, then media notice would be required. However, if 200 people were affected in Ohio, 200 in Kentucky and 200 in Tennessee, no media notice would be required.

### HHS Notification

Notice must be provided to the Secretary of HHS by CEs of unsecured PHI that has been involved in a breach.

- If the breach involves more than 500 individuals (no matter which state they reside in), notice must be given immediately (defined in the regulations as concurrently with the notices sent to individuals).
- If the breach involves less than 500 individuals, the CE may maintain a log and annually submit the log to the Secretary of HHS (within 60 days after December 31). In 2010, CEs will need to submit information for breaches occurring on or after September 23, 2009.
- HHS will post instructions on its website for submitting each type of notification.
- CEs and BAs will need to maintain internal logs of potential breaches and actual breaches for six years from the date they occurred.

### Safe Harbors--Encryption and Destruction

The breach notification provisions only apply to "unsecured PHI." If the PHI that a CE or BA has is secured by encryption or destruction, then there is no need to report a breach to anyone. Unsecured PHI is defined as PHI that is not secured by technology that renders it unusable, unreadable, or indecipherable to unauthorized individuals. Thus, CEs and BAs have a significant incentive to encrypt PHI or take other steps to insure that the PHI is not "unsecured."

If PHI is encrypted according to the data breach regulations, then even if it is lost or stolen, it will not be considered to have been breached. To encrypt data, a CE or a BA must use an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key. HHS stressed in the regulations that the process or key cannot have been breached and that CEs and BAs should store the process or key on a device or at a location separate from the data that has been encrypted. To meet the safe harbor for encryption for data at rest, an entity must use the standard set forth in NIST Special Publication 800-111. To meet the safe harbor for data in motion, an entity must use NIST Special Publication 800-52, 800-77, or 800-113, as appropriate. We also suggest that you review your portable media policies as the

potential for laptops and phones to be lost or stolen is perhaps the biggest risk for data breaches that CEs and BAs face.

If the media on which PHI is stored or recorded has been destroyed in one of the following ways, no reportable breach has occurred:

- Paper, film, or other hard copy media have been shredded or destroyed so that PHI cannot be read or otherwise reconstructed.
- Electronic media have been cleared, purged, or destroyed consistent with NIST Special Publication 800-88 so that the PHI cannot be retrieved.

HHS emphasized that redaction of a document does not constitute destruction of that document so as to qualify for the safe harbor.