



BENEFIT *Advisor*

In This Issue

In this tenth issue of the McGrawWentworth Benefit Advisor for 2009, we examine the recently released Breach Rules that apply to group health plans. The American Recovery and Reinvestment Act (ARRA) of 2009 includes provisions that changed the requirements of HIPAA's Privacy and Security Rules. The changes were included in the Health Information Technology for Economic and Clinical Health Act (HITECH).

One of the most significant aspects of HITECH was that the Act added a requirement that covered entities notify individuals, the Department of Health and Human Services and possibly, the media of any breaches or potential breaches of PHI. This Advisor addresses the recently released guidance on the breach requirements.

We welcome your comments and suggestions regarding this issue of our technical bulletin. For more information on this Benefit Advisor, please contact your Account Manager or visit the McGrawWentworth web site at www.mcgrawwentworth.com.

“New HIPAA Requirements”

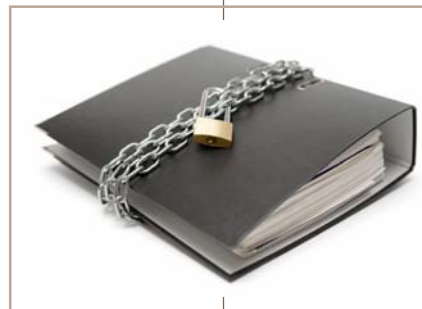
The American Recovery and Reinvestment Act (ARRA) of 2009 changed not only COBRA regulations, but also HIPAA's Privacy and Security provisions.

ARRA invested sizeable funds to encourage the health care industry to begin keeping medical records electronically. The change to electronic medical records should over time reduce health care cost and improve quality.

However, many Americans fear the move because they do not believe that health care providers can keep their electronic medical records confidential. For this reason, the Department of Health and Human Services significantly strengthened HIPAA's Privacy and Security Rule mandates. The changes are included in ARRA's Health Information Technology for Economic and Clinical Health Act (HITECH). To learn more about HITECH, please read our May 2009 *Benefit Advisor* at http://mcgrawwentworth.com/Benefit_Advisor/2009/BA_Issue_5.pdf.

Under the HITECH rules, covered entities need to notify affected individuals, DHHS and potentially the media if a breach of unsecured protected health information (PHI) occurs. The government issued interim regulations on August 24, 2009, detailing the specifics on reporting such breaches along with a request for comments. Until fi-

nal rules are issued, your organization should comply with these interim regulations.



This *Advisor* reviews the following requirements in detail:

- Secured or Unsecured PHI
- Breach Considerations
- Individual

Notifications

- Media Notifications
- DHHS Notifications
- Law Enforcement Delay
- Action Plan

HITECH originally set September 23, 2009, as the deadline for complying with the rules governing breaches. Because covered entities will need more time to thoroughly meet these new requirements, DHHS will not enforce the rules for six months.

Secured or Unsecured PHI

Protected health information (PHI) is defined in the HIPAA Privacy Rules as “individually identifiable health information that is created, received, stored or transmitted by a covered entity and relates to the past, present, or future,

physical or mental health of the individual or information relating to the provision of care or payment for that care.” Covered entities include:

- Health care providers who conduct certain transactions electronically.
- Health care information clearinghouses (organizations that take health data in one format, re-format it, and send it to other organizations). These organizations would include PPO networks and billing services for health care providers.
- Employer group health plans and health insurance carriers.

ARRA added business associates to the list of organizations considered covered entities. Business associates are organizations that need PHI to perform a function on behalf of a covered entity. Covered entities secure contracts with business associates specifying how the business associate will use the PHI and how the business associate will protect it.

The Privacy Rules address how covered entities must safeguard PHI in any form. While the rules specify many steps organizations must take to comply, the overall goals of the Privacy Rule are as follows:

- To safeguard PHI so it is used and disclosed only as HIPAA rules allow. Under no circumstances should PHI be used for any employment-related decisions.
- To issue a privacy notice explaining their policies on using and safeguarding PHI.
- To create formal policies and procedures on how PHI is used and disclosed, train workforce members on how to handle

this information and designate the person responsible for compliance.

- To secure PHI so that it is available only to those authorized to view or use it.

HIPAA Security Rules outline the steps a covered entity must take to safeguard electronic protected health information (EPHI); HITECH does not alter these basic rules. The overall goals of the Security Rules require covered entities to:

- Create reasonable and appropriate safeguards to protect the confidentiality, availability and integrity of electronic protected health information.
- Take actions to protect against threats to data security, such as viruses, worms and malicious code.
- Adopt safeguards to protect against unauthorized use or disclosure of electronically protected health information.
- Take administrative steps to ensure the workforce complies, such as training and reminders about security provisions.

The new breach requirements now define “secured PHI” and present another layer of security actions you may take to prevent breaches of this information:

- Using technology that can render PHI or EPHI unusable, unreadable or indecipherable.
- DHHS indicated that only two methods for securing data may be considered a safe harbor and any data secured in the

following manners will generally be considered “secured PHI”:

- Encryption of EPHI that would be considered consistent with requirements of the National Institute of Standards and Technology (NIST). The preamble actually divides the encryption requirements as it pertains to

“data at rest” and “data in motion”. The NIST encryption guidance for data at rest can be found in Special Publication 800-111. The NIST encryption guidance for



data in motion can be found in several Special Publications: 800-52, 800-77, 800-113. All of these Special Publications can be found at the NIST website at <http://csrc.nist.gov/publications/PubsSPs.html>. The regulations note that the encryption keys must be kept on a separate device from the data that they encrypt or decrypt.

- Destruction of EPHI or PHI which means the data is completely destroyed in one of the following ways:
 - Paper, film or other hard copy media is shredded or destroyed such that PHI cannot be read or reconstructed. The preamble specifies that redaction is specifically excluded as a means of data destruction.

- Electronic media has been cleared, purged, or destroyed consistent with the NIST Special Publication 800-88 Guidelines for Media Sanitation.
- Your IT Department should work with HR to determine if encryption is a feasible and reasonable option to secure PHI. In addition, your organization should review your procedures for the destruction of PHI to make sure it is being thoroughly destroyed.



The new notification requirements apply to **only** unsecured PHI and **only** in certain situations. If you have a potential breach of secured information, notification is not required because by definition, even with a potential breach the information is unusable, unreadable or indecipherable.

Breach Considerations

A breach is defined as “*acquisition, access, use or disclosure of PHI in an impermissible manner which compromises the security or privacy of the PHI.*” This definition is very broad and the only exception applies to “limited data sets.” Most employers did not focus on limited data sets when working through HIPAA compliance, primarily because limited data sets are used in research. A limited data set excludes 16 direct identifiers for the PHI. Breach rules do not apply to limited data sets that also exclude date of birth and zip code information.

The broad scope of the breach definition is concerning for covered entities, so in the latest round of guidance, the DHHS adopted a “harm threshold”, which simply means that the compromise in the security or privacy of PHI that poses a significant risk of financial, reputational or other harm to an individual would constitute a breach. An impermissible disclosure of PHI is an actual breach only if it meets this harm threshold. For that reason, whenever a possible breach of PHI or EPHI occurs, you must assess the risk of potential harm. What’s more, you must document this risk analysis. Consider the following questions as part of the risk assessment:

- **Who improperly used or disclosed the PHI? If PHI was improperly disclosed, to whom was it disclosed?** For example:
 - If PHI was impermissibly disclosed to another entity subject to HIPAA’s Privacy and Security Rules, the potential harm is fairly low, because the other organization is also required to protect the information.
 - If the disclosure was made to an organization not subject to HIPAA, the potential harm is considerably higher.
- **Were immediate steps taken to mitigate harm?** For example, did you:
 - Obtain satisfactory assurances that the PHI is not being used or disclosed further and will be returned or destroyed?
 - Request the unintended recipient sign a confidentiality agreement affirming the information will not be further disclosed?
- **Was impermissibly disclosed PHI returned before it was accessed?** For example:
 - A lost or stolen laptop containing PHI is found or returned soon after the incident. A forensic analysis of the laptop shows no one accessed, altered, copied or transferred the PHI; therefore, the group health plan assesses a low harm potential.
 - DHHS has assigned tight time frames for breach notifications. You can take some time to try to recover a stolen laptop, but you cannot delay notification beyond the DHHS timeframe.
- **What type of information was impermissibly disclosed?** For example:
 - The disclosed information can include a name and information that the person recently had an inpatient hospital stay. This information in and of itself does not necessarily harm a person’s finances or reputation.
 - However, if more detailed information is released, such as enough personal information to allow identity theft or the fact the inpatient stay was a drug rehabilitation clinic,

this type of information has real potential to do financial or reputational harm and should be elevated to the level of breach.

This risk assessment can help you decide what potential harm the impermissible release of PHI may cause. The rules adopt a “no harm, no foul” approach to breaches. If there is a low risk of harm, then you need to document the situation and analyze the risk, but you do not need to notify anyone else.

If the risk assessment reveals a potential for moderate or likely harm, then you must evaluate the situation one last time to see if it meets any of the three following exceptions to the definition of a breach:

1. **A workforce member unintentionally acquires, accesses or uses PHI.** Remember workforce members are employees designated in a firewall document as members of your health plan workforce. To be considered unintentionally acquired, the PHI must have been released under the authority of the covered entity or the group health plan, must have been released in good faith and within the scope of the workforce member’s authority and must not have caused any additional impermissible use or disclosures.

For example, an HR employee in the payroll department might have accidentally received an e-mail about a plan participant’s claim that

was intended for the Vice President of Human Resources. The payroll department employee immediately realizes that the e-mail was sent to the wrong person. The employee notifies the sender and deletes the e-mail.

Because the employee’s access to the PHI was unintentional and made in good faith, it does not constitute a

breach situation.

2. **An authorized person inadvertently discloses PHI to an authorized person in another area at the covered entity or business associate.** This situation occurs when the other person is not specifically authorized to access the PHI. The other person must not use or disclose the PHI any further.

For example, a workforce member dealing with claim questions reveals PHI to another workforce member dealing with enrollment but not involved in claim issues. The employee who handles enrollment should not have knowledge about a specific medical condition of any employee. You need to ensure the PHI is not further used or disclosed in any way that would violate the Privacy Rule.

3. **A covered entity or a business associate inadvertently discloses PHI in a good faith belief that the unauthorized person receiving the PHI would not be able to reasonably retain such information.** For example, an employee hands a claim form containing PHI to another employee by mistake, realizes the mistake quickly,

and recovers the PHI from the unauthorized individual.

Employers have the burden of proof to demonstrate the breach situation met one of the listed exceptions. The employer should retain all documentation demonstrating the situation met a listed exception.

Once the employer determines:

1. The PHI was unsecured.
2. The disclosure had a moderate to high potential to cause financial or personal harm.
3. The disclosure failed to meet one of the three noted exceptions.

Then the employer has a breach that they need to provide specific notification to the individuals affected, the DHHS and potentially the media.

Individual Notifications

DHHS recognizes that once a potential breach is discovered, it may take some time to investigate the situation. However, they recognize that plan participants should receive timely notice of the breach situation, especially in situations where there is a potential to cause financial or reputational harm.

Covered entities are required to send individuals affected notification of the breach, without an unreasonable delay but in no case any later than 60 days following the discovery of the breach. A breach is considered “discovered” at the point the breach is known to any person at the covered entity except the individual committing the breach or at the point the breach would have been known if the covered entity had been exercising reasonable diligence.

Continued on Page 5



If the breach is committed by a business associate or a subcontractor, it is deemed discovered once the business associate obtains knowledge of the breach. It will be important for all covered entities to specify in their business associate contracts a reasonable time frame for reporting breaches to the covered entity. The covered entity will be responsible for the notification process so the business associate's notification should be timely to ensure the covered entity has time to provide notices.

The 60 days is an outer limit. If you can reasonably notify the employee sooner, you are expected to do so. The 60 days gives you time to investigate the specifics as explained in the previous sections. It also allows time to identify which plan participants' information may have been released in error. If, after investigating, you find no breach has occurred, no notifications are necessary.

Once the covered entity identifies the individuals affected or believed to be affected by the breach, the covered entity must send an individual notification that includes the following information:

- A brief description of what happened, including the actual date of the breach and the date the breach was discovered.
- A description of the types of PHI involved, such as date of birth, social security numbers, claim information and so on. The description is meant to be general and describe the categories of information disclosed. Your organization should not include the actual specific data, such as the actual social security number.

- Steps they should take in order to protect themselves from potential harm caused by the breach.
- Description of what you are doing to investigate the breach, mitigate the harm and protect against any future breaches of PHI.

This notice must be written in plain English and can be delivered in either of these two acceptable methods:

- First class mail delivered to the last known address.
- Electronic delivery if the employee has agreed to that method.

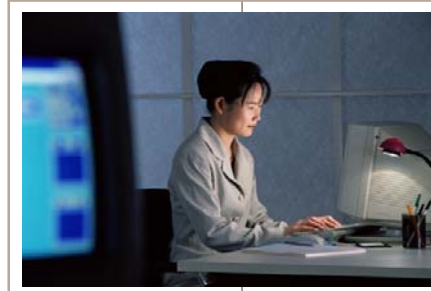
If the employee is deceased, send the notice to the next of kin or personal representative if possible. In urgent situations, the DHHS recommends immediate contact via the phone or another more immediate communication channel. In these situations, the immediate contact does not replace the actual notice requirement and covered entities are expected to follow up with the written notice.

If you do not have enough information to contact some of the people affected or the post office returns some notices as undeliverable, you can't simply ignore these people. Instead, you need to notify them in another way:

- If the group health plan identifies fewer than 10 individuals that were affected

by the breach but the employer does not have enough information to provide the notification, the employer can choose an alternative means of contacting the individuals, such as via the telephone.

- If 10 or more individuals were affected by the breach but the employer does not have enough information to provide the notification, the covered entity must conspicuously post a notice on the organization's website or provide a conspicuous notice in the local media (either a print media or broadcast media). The covered entity must establish an 800 number individuals can call with any questions about the breach and that number must be effective for at least 90 days.



This process is referred to as providing a "substitute notice." Notifying the media in this case applies only when

you do not have enough information to properly notify 10 or more affected individuals. It is not the same as the media notice discussed in the next section.

Media Notifications

In addition to notifying the people affected, in certain circumstances, you may be required to notify the media as well. The media notification applies only if the breach affects more than 500 residents of a state or jurisdiction (including the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands and Guam). Covered entities must notify a media outlet

prominent in the area where the people affected live.

Covered entities must notify the media within 60 days after discovering the breach. Again the 60 day time frame is the outer limit. Generally, the information given to the media will be the same information given to the individual.

The regulations do not define a "prominent media outlet." You have the freedom to determine the prominent media outlet, which may be a local newspaper, local news show, or even several newspapers. In most cases the media notice will simply be a press release.

According to the regulations, media notice is not necessary in the following examples:

- A breach affects 1,000 plan participants scattered across the country, but 200 are in California, 400 are in Colorado and 400 are in Florida. The media notice is not necessary because the breach did not affect 500 people in the same state or jurisdiction.
- A breach happens at a business associate and it affects the participants of more than one covered entity; for example, the breach affects a total of 800 people but they are employees of four different entities. The media notice is not necessary since the breach does not affect 500 people from one covered entity. For the breach regulations to have applied, the breach must have affected 500 people from the same covered entity in the same state or jurisdiction.

While notifying the media may seem daunting, very few breach situations will actually require this step.

DHHS Notifications

When a breach has occurred, covered entities must notify the Department of Health and Human Services (DHHS). DHHS has created a process to report breaches. The DHHS just activated the breach notification site. More details can be found at <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html>.

The DHHS reporting process differs depending on the number of people affected or believed to be affected by the breach.

- If the breach affects 500 or more people, you must notify DHHS immediately:
 - The 500 individuals are **not** required to be in the same state or jurisdiction for this threshold to apply. For example, suppose the breach affects 600 people total, 100 people in six different states. Although the media notice would not apply, the notice to DHHS would still apply because the breach affected over 500 people.
 - You must notify DHHS within 60 days.
- If the breach affects fewer than 500 employees, you must still report the breach, but you will need to report these smaller breaches only once a year:
 - Keep an annual log of breaches affecting fewer than 500 people. The log should describe the details of the incident.



- Submit the details of these smaller breaches within 60 days of the start of the calendar year.

HIPAA record keeping rules require covered entities to keep all breach-related documents for six years.

Law Enforcement Delay

The only permissible delay in any of these notice requirements is a delay requested by a law enforcement official. In this case, be sure to require a written request from

the law enforcement official stating the reason and the time period for the delay.

If you cannot obtain a written request for

the delay, document the identity of the official and the reason for the request. The maximum time frame for a delay that is not confirmed in writing is 30 days. If the law enforcement official requests a delay of more than 30 days, that official needs to provide the covered entity a written request for the delay.

Action Plan

The new breach requirements certainly seem overwhelming at first glance; however, a well developed process will help you investigate possible breaches and notify the people involved.

All group health plans should develop a procedures manual employers can use to determine whether a breach has occurred and when and

whom to notify. Make sure your process includes the following steps:

1. Determine whether the disclosed PHI falls under the definition of secure PHI. Your procedures manual should define secured and unsecured PHI. If the PHI is indeed considered secured, verify in writing PHI or EPHI did indeed meet the safe harbor requirements. No further notifications are required when the PHI is considered secured.
2. If the PHI was unsecured, your health plan will need to investigate to determine whether the breach poses a significant risk to the individual's finances or reputation or causes other harm. Create a tool to keep in your procedures manual to help document the answers to key questions the DHHS would like investigated as part of a risk assessment:
 - Who used or disclosed the PHI improperly and to whom was the information disclosed?
 - Were immediate steps taken to mitigate harm?
 - Was the impermissibly disclosed PHI returned before it was accessed?
 - What information was impermissibly disclosed?



If the risk assessment shows a low risk for harm, your organization needs to document the incident and keep

written records of the risk analysis showing a low risk level. You do not need to provide any further notifications.

3. If the risk level is high or moderate, you need to determine whether the breach falls into one of the three permissible exceptions listed below:
 - Any unintentional acquisition, access or use of PHI by workforce member.
 - Any inadvertent disclosure of PHI by a person who is authorized to access PHI at a covered entity or a business associate to another person with authorized to access PHI at the covered entity or business associate.
 - An inadvertent disclosure of PHI in a situation where a covered entity or a business associate has a good faith belief that the unauthorized person to

who PHI was disclosed would not be able to reasonably retain such information. These three situations are exceptions to the breach rules.

If any one of the situations describes your breach, you need to document the situation, but no additional notifications are necessary.

4. If the risk level is high or moderate, and the situation was not one of the three exceptions permitted by the rules, then your organization

needs to identify anyone affected by the breach.

5. Your procedures manual should specifically detail each notification requirement:
 - **Individual notice:** Because you must notify anyone affected within 60 days after you discover the breach, be sure to note the date. Each breach situation will likely be unique, making it difficult to create a notice template. However, it does make sense to create a sample notice with the specific information any notice must include:
 - Briefly describe what happened, including the actual date of the breach and the date the breach was discovered.
 - Describe the types of PHI involved, such as date of birth, social security numbers, claim information and so on.
 - List the steps people should take in order to protect themselves from potential harm related to the breach.
 - Describe what you are doing to investigate the breach, to mitigate harm and to protect against any future breaches of PHI.

Keep copies of the notices you send. If you send the notice electronically, you should have on file a record of the individual's permission to deliver information in this way. Keep track of employees

with no contact information or notices returned as undeliverable. For these people, you will need to provide some sort of substitute notice. Include in the procedures manual the acceptable substitute notices. Depending on how many people do not have current contact information, you may use an alternative method of communication or a public notice on your website or in the media.

- **Media Notice:** The media notice will apply only in a few situations. Your procedures manual should include the requirements for those rare instances. You should also include a sample press release containing the same information stated in the individual notice. Again it is important to keep a record of your media notices.
- **DHHS Notice:** Your procedures manual should include the requirements for an immediate notice to PHIs (500 or more individuals affected) and the requirements for the annual notice. Put a follow-up in your scheduling system for January 15 each year to remind you to

complete the annual notice to DHHS. More details can be found at <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html>.

6. Create a breach binder either in hard copy or electronically to maintain records of every potential breach incident and the investigation and outcomes.



It makes sense to maintain a binder for each calendar year so it coincides with reporting requirements to the DHHS. In addition, it will help your organization in maintaining records for the six-year required time frame. It is critical to retain documents proving your organization investigated all breach or potential breach situations.

7. Revisit your business associate contracts. Business associates are also directly responsible for complying with the Privacy and Security Rules. Under the breach rules covered entities are ultimately responsible for providing the required notices and conducting a risk analysis

of breach situations. You can delegate this responsibility to the business associate, but if the business associate does not provide proper notice or does not conduct a thorough risk analysis, your organization will be responsible. Your business associate contract

should include the timing for notifying you about a potential breach, the willingness to participate in an investigation and risk analysis of the situation and any assistance

the business associate will provide for the notification process.

The key right now is to create a breach procedures manual ensuring your organization investigates the breach properly, analyzes the risk thoroughly and notifies the people affected promptly. Because the DHHS recognizes as soon as technology is released it is almost out of date, it will issue annual updates on acceptable methods for securing data.

If you have any questions about this Benefit Advisor, please contact your McGraw Wentworth Account Manager. **MW**

Copyright McGraw Wentworth, Inc. Our publications are written and produced by McGraw Wentworth staff and are intended to inform our clients and friends on general information relating to employee benefit plans and related topics. They are based on general information at the time they are prepared. They should not be relied upon to provide either legal or tax advice. Before making a decision on whether or not to implement or participate in implementing any welfare, pension benefit, or other program, employers and others must consult with their benefits, tax and/or legal advisor for advice that is appropriate to their specific circumstances. This information cannot be used by any taxpayer to avoid tax penalties.

McGraw Wentworth, Inc.

3331 West Big Beaver Road, Suite 200
Troy, MI 48084
Telephone: 248-822-8000 Fax: 248-822-4131
www.mcgrawwentworth.com

250 Monroe Ave. NW, Suite 400
Grand Rapids, MI 49503
Telephone: 616-717-5647 Fax: 248-822-1278
www.mcgrawwentworth.com