McGraw Wentworth

BENEFIT Advisor

Volume Seventeen, Issue Two March 2014

"Final HIPAA Privacy and Security Regulations"

In This Issue

In this second issue of the McGraw Wentworth Benefit Advisor for 2014, we review the final HIPAA Privacy and Security rules. These rules stipulate when employer health plans can use and disclose Protected Health Information (PHI). They also establish steps employers must take to safeguard PHI in all formats.

The HIPAA Privacy and Security rules have changed substantially in the last decade. The Office of Civil Rights (OCR) is ramping up audit activity. Employers may need to revise compliance steps as a result of the final regulations.

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 McGraw Wentworth web site at www.mcgrawwentworth.com.

The federal government released final Health Insurance Portability and Accountability Act (HIPAA) rules in January 2013. The final rules covered HIPAA Privacy and Security requirements. They formally adopted many changes made over the last decade including significant changes in the breach investigation and reporting rules. Breach investigation and reporting rules were originally included in the Health Information Technology for Economic and Clinical Health Act (HITECH).

If you have kept up-to-date with HIPAA Privacy and Security rules over the years, the primary difference will be in breach rules and defining business associates. If your organization has not kept current with the changes, a complete review of your Privacy and Security compliance steps would be a good idea. This *Advisor* summarizes the steps you need to take to ensure you are complying with the following key requirements of the final HIPAA Privacy and Security rules:

- High Level Review
- Covered Entities
- Privacy Rule
- Security Rule
- Breach Investigation and Reporting Requirements
- Penalties

High Level Review

One of HIPAA's major goals was to simplify the process for administering insurance eligibility, claim submission and provider payments. To accomplish that goal, HIPAA rules have focused on creating common formats and encouraging electronic transactions for these administrative functions. These changes may make the data more vulnerable. As a result, the HIPAA Privacy and Security rules have created baseline protections for the data used in health plan transactions.

To comply with HIPAA privacy and security requirements, covered entities must take several steps. In general, they must review the Protected Health Information (PHI) that they use, disclose, store or transmit to determine whether HIPAA permits those uses and disclosures. They also need to take steps to ensure that PHI in all formats remains secure.

When the HIPAA Privacy and Security rules were initially issued, employers were confused on how the rules affected them. Over the last decade, the government has clarified many requirements.

Continued on Page 2

The HIPAA Privacy and Security rules apply only to "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" known more commonly as PHI. Genetic information is considered PHI.

The Office of Civil Rights (OCR) audits compliance with privacy, security and breach protocols. Although the OCR has focused most of its attention on health care providers, at some point, it may begin to look at employer plans.

Covered Entities

HIPAA Privacy and Security rules apply to covered entities. Covered entities are broadly defined and include:

- Health plans (including employer-sponsored health plans)
- Health care information clearinghouses (organizations, such as PPO networks or physician billing services, that process or facilitate the processing of health information)
- Health care providers that conduct certain electronic transactions

Health plans can include employer-sponsored health plans. The health plan can be self-funded or fully insured. The health plan category also includes health insurance carriers.

An employer's health plan, but not the actual employer, is considered the covered entity. To comply, employers need to establish some structure for their health plans. They will have to designate which employees are included in the health plan's "workforce." Employees such as payroll, human resources, finance and IT personnel may be responsible for administering the group health plan and may have access to PHI. These positions or departments should be included in the health plan's "workforce".

The final rules also adopted a change originally included in HITECH. This change extended HIPAA's Privacy and Security requirements directly to "business associates." Business associates are organizations that require PHI to perform a function on behalf of the group health plan. Business associates may include a third party administrator, pharmacy benefit manager or benefits consultant, among others. Insurance carriers are not considered business associates because they are considered covered entities under the Privacy and Security rules.

Covered entities must have a contract with their business associates. The contract must outline how the business associate will use and secure PHI. Covered entities should revisit their business associate contracts in light of the final regulations. Because employers must investigate breach situations promptly, the contract should explain how the business associate will notify the covered entity of any potential breaches. The Department of Health and Human Services (DHHS) has a website covering key considerations for business associate contracts. The information can be found at http://www.hhs.gov/ocr/Privacy/hipaa/understanding/coveredentities/contractprov.html.

The final rules also clarify which organizations can be considered business associates. Sometimes business associates contract with other organizations to perform a function for the business associate related to the covered entity's group health plan. There is no direct relationship between the covered entity and the other organization. In the initial regulations, these organizations were referred to as subcontractors. These organizations are now considered business associates of a business associate. This means your business associate must have a business associate contract for the entity it is using to perform a function on behalf of your plan.

Privacy Rule

When the Privacy rules were initially issued, there was a misconception that health information could not be used. In fact, the Privacy rules allow a covered entity to use PHI and they explain the steps necessary to secure it.

One of the main goals of the Privacy Rule is to keep PHI confidential. In order to achieve that goal, the employer must know how the company is using PHI and where it is stored and maintained. Remember, PHI is information related only to your health plan. Your organization may

Continued on Page 3

have health information that it maintains that is not considered PHI. Evidence of insurability for voluntary life insurance typically includes health information. It is not considered PHI because it is not related to the health plan. It is good practice to protect the confidentiality of all data you maintain. However, only PHI is subject to the Privacy and Security rules.

The Privacy Rule sets forth a number of requirements covered entities need to follow when they use or disclose PHI. It establishes certain individual rights related to PHI. It also establishes administrative steps that covered entities must take to secure PHI.

Use and Disclosure Rules

Covered entities can use PHI for TPO (treatment, payment and health care operations). These categories are so broadly defined that most functions of a group health plan are considered TPO. The Privacy Rule also permits PHI to be used for reasons other than TPO, including:

- Use and disclosures for notification or disaster relief efforts
- Use and disclosures required by law
- Use and disclosures for public health activities
- Disclosures about victims of abuse, neglect or domestic violence
- Use and disclosures for health care oversight activities
- Disclosures for judicial proceedings
- Disclosures for law enforcement purposes
- Use and disclosures about decedents
- Use and disclosures for cadaver organ, eye or tissue donation purposes
- Use and disclosures for certain limited research activities
- Use and disclosures to avert a serious threat to health or safety
- Use and disclosures for specialized government functions
- Disclosures related to work-related injuries or illnesses

Covered entities should apply the minimum necessary standard when they use PHI. This standard requires that they use only as much PHI as is necessary to accomplish the task at hand.

The Privacy Rule also mandates that covered entities create a Privacy policy. This policy should outline, at a high level, how the health plan uses PHI. It should include the enrollment process, eligibility management, claim payments, plan audit functions, and stop loss administration. When you identify the various ways in which your health plan uses PHI, you also need to determine whether they are related to TPO.

Your Privacy policy should cover all the situations where your plan will legally use PHI. To use PHI for a reason not stated in your policy or permitted under the Privacy Rule, you must obtain authorization. Developing a Privacy policy is a key action step necessary to comply with HIPAA rules. The Privacy policy must be customized to your health plan and how your organization uses PHI for plan administration.

Individual Rights

All individuals have certain rights related to their own PHI. Covered entities must recognize the following individual rights and have a process to administer them:

- Right for an individual to access PHI
- Right for an individual to request an amendment to PHI
- Right to request an accounting of disclosures of PHI
- Right to receive a notice of Privacy practices
- Requests for confidential communications
- Requests for restricted uses and disclosures of PHI

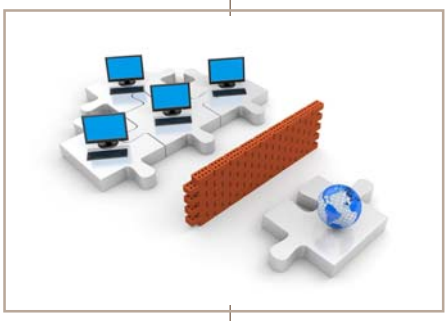
Most of the individual rights are fairly straightforward. A covered entity must allow participants to access their own PHI. The final regulations also require a covered entity to allow electronic access to PHI if it is available.

Employees can request amendments to their PHI files, but employers need only amend the information if it is reasonable.

Covered entities must account for disclosures of PHI. However, most uses and disclosures that the Privacy Rule allows are exempt from the accounting requirement, including any PHI disclosed for TPO. Some disclosures of PHI will need to be accounted for such as responses to court orders or disclosures for public health activities.

Continued on Page 4

Covered entities must allow participants to request confidential communications. For example, requests might come from spouses or children who do not want the primary insured to receive details related to their health care. Plans must approve confidential communication requests if recipients indicate that receiving their information at the current location could endanger their wellbeing.



Plans should be cautious about approving requests for restricted use. Most health plans will use PHI only for required functions, so you may be unable to properly administer your plan if you agree to restricted use. Your plan is **not** obligated to agree to any restricted use. The final rule includes an additional stipulation for restricted uses. Participants who pay in full for a service can request that PHI related to that service never be disclosed.

Most covered entities will never have to deal with participants asserting their individual rights under the Privacy Rule. However, as part of compliance, your organization must establish a process to administer these rights.

Administrative Requirements

To limit use and disclosures of PHI and maintain confidentiality, the Privacy rules require very specific administrative steps. Covered entities should document they have taken all the necessary administrative steps. The following is a high-level review of the key administrative requirements:

- **Designate a Privacy Officer:** The privacy officer is the person responsible for ensuring your organization complies with the Privacy rules.
- **Draft a Firewall Document:** The firewall document creates your health plan workforce. This document should specify who in your organization is permitted to use and disclose PHI as part of health plan administration. Organizations often use titles rather than names when they create the workforce. This eliminates the need to revise the document every time there is turnover in the health plan's workforce.
- **Draft a Privacy Policy:** Your privacy policy must specifically state how your workforce will use PHI. If your organization decided to use a sample document for a Privacy policy, it will likely not be adequate. The policy should also provide the high-level details regarding how your organization will protect the confidentiality of PHI.
- **Draft Use and Disclosure Procedures:** This document may be included in the Privacy policy or drafted independently. It is much more specific as to how PHI is used in plan administration and how it is protected. It should also include the steps you are taking to safeguard the data. For example, if someone calls to ask you a question regarding PHI, what steps will you take to verify the individual's identity?
- **Establish Safeguards:** This step is explained in more detail below. It involves reviewing where PHI is used, maintained and stored. Once you identify these areas, you must develop safeguards to keep PHI confidential both physically and electronically.
- **Appoint a Complaint Contact and Develop Complaint Procedures:** Every covered entity must establish a process for filing complaints. All complaints must be investigated.
  - Sanctions should apply to any health plan workforce member who violates Privacy procedures.
  - Your organization should take steps to mitigate any potential harm if PHI is disclosed improperly.
  - The covered entity must keep a record of all complaints and their resolution.
- **Create a Privacy Notice:** The Privacy Notice is a document sent to plan participants that summarizes the plan's privacy practices. When final regulations were released, DHHS published updated sample Privacy Notices. They can be found at http://www.hhs.gov/ocr/Privacy/hipaa/modelnotices.html. The following elements must be included in this notice:
  - Permissible uses and disclosures of PHI.
  - Individual rights regarding PHI.
  - Covered entity's legal duties related to PHI, including the responsibility to notify an affected individual of a breach.

Continued on Page 5

Privacy notices must be delivered at the following times:

- When an individual enrolls in the plan
- Within 60 days of a material change in the notice
- Every three years (only a reminder that the notice is available)

- **Create a Breach Reporting, Investigating and Tracking Process:** HITECH added the breach reporting requirements. The final rules changed the requirements significantly. This *Advisor* discusses the new requirements in a separate section.

These steps will create the administrative policies that will help limit uses and disclosures. They will also ensure PHI is safeguarded.

The Privacy Rule requires that some additional steps be taken to secure PHI:

- Implement physical safeguards.
  - Review areas where PHI is stored. Are these secure areas and is access limited to members of your health plan workforce?
  - Review all areas receiving PHI, including fax machine areas and mail rooms. Are these secure areas and is access reasonably limited to your health plan workforce?
- Evaluate electronic safeguards.
  - Review all the areas in your organization that maintain electronic PHI.
  - Ask your information technology department how your electronic information is safeguarded.
  - Verify that only your health plan workforce has access to electronic PHI.
  - Check your copy machine to determine whether it retains electronic copies of PHI.
- Obtain business associate agreements. The covered entity is responsible for ensuring it has signed business associate agreements with all the business associates of the plan.
  - Identify your business associates (third party administrators, advisors, pharmacy benefit managers, and so on).
  - Many of your business associates will provide the agreements. Your legal department should review agreements to make sure the agreement protects the plan.
- Develop a training program and a training process. Once you develop your policies on how to use and secure PHI, you must train your workforce on these policies.
  - Training must be documented for all health plan workforce members.
  - Re-training is necessary when there is a material change in privacy policies and procedures.
  - Refresher training is also a good idea to make sure your workforce understands and follows policies and procedures.

This section simply summarizes the Privacy rules high level requirements. You may want to have an attorney review your compliance plan and materials to ensure they meet the Privacy rule intent and requirements.

Security Rule

The Security Rule provides the action steps an organization must take to protect electronic PHI (EPHI). The broad goals of the Security Rule include:

- Ensuring the availability, confidentiality and integrity of electronic PHI.
- Protecting against any reasonably anticipated threats to the security of electronic PHI.
- Guarding against any reasonably anticipated impermissible uses or disclosures of electronic PHI.
- Verifying compliance of the health plan workforce members.

The Security Rule includes five categories of safeguard standards. Compliance requires documenting the necessary steps to meet the following standards.

Continued on Page 6

Administrative Safeguards

- Security management process
- Assigned security responsibility
- Workforce security
- Information access management
- Security awareness and training
- Security incident procedures
- Contingency plan
- Evaluation
- Business associate contracts

Physical Safeguards

- Facility access controls
- Workstation use
- Workstation security
- Device and media controls

Technical Safeguards

- Access controls
- Audit controls
- Integrity
- Person or entity authentication
- Transmission security

Organizational Requirements

- Business associate contracts
- Plan amendment

Documentation Requirements

- Policies and procedures
- Documentation requirements

Many of these standards specify the steps organizations can take to satisfy the requirements. Each covered entity's Security compliance plan should include a written summary of the steps it takes to meet each standard and each implementation specification.

The Department Health and Human Services (DHHS) publishes a number of resources to help with Security Rule compliance. These resources can be found at http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html.

Securing electronic PHI appropriately is imperative in today's world. A vast amount of information is stored and transmitted electronically. Your organization needs to follow these steps to make sure your electronic PHI is secure. With the addition of the breach reporting requirements, securing PHI has become even more important. If the PHI is considered "secured" based on the requirements outlined in the next section, covered entities are not required to provide breach notifications.

Although the Security rule does not require encrypting electronic PHI, all covered entities should consider it. PHI is sent almost daily from covered entities to various business associates. Sensitive data transmitted over the Internet is vulnerable if it is not protected. Encryption technology is now very affordable and strongly recommended.

In most organizations, both human resources and information technology departments handle Security compliance. Your compliance steps should ensure that only specific workforce members can access the electronic PHI stored in your system.

Breach Investigation and Reporting Requirements

HITECH added breach reporting requirements to strengthen the legislative weight of HIPAA. Before HITECH, covered entities needed to correct any breach situation and mitigate any potential harm. They were not, however, required to notify participants that there was a breach, or potential breach, of their PHI. The new breach reporting requirements add a number of steps to take if there is a breach, or suspected breach, of PHI. Timing is critical. If a notification is required it must be made within 60 days of the discovery of the breach.

The final regulations substantially changed the breach investigation process. As a result, all employers need to update their breach procedures. A breach is defined as the "acquisition, access, use or disclosure of PHI in an impermissible manner which compromises the Security or Privacy of the PHI." The investigation process determines whether PHI has been compromised.

First, identify the PHI that may have been breached. Second, determine whether the information was "secured PHI" as defined below:

- The EPHI is unusable, unreadable and indecipherable to unauthorized individuals.

Continued on Page 7

- Two methods for securing data may be considered a safe harbor, so any data secured in the following ways will be "secured PHI:"
  - EPHI encryption that is consistent with National Institute of Standards and Technology (NIST) requirements. Encryption keys must be kept on a separate device from the data which they encrypt or decrypt.
  - EHPI or PHI is completely destroyed as follows:
    - Shred or destroy paper, film or other hard copy media so that PHI cannot be read or reconstructed. Simply redacting the data is not acceptable.
    - Clear, purge or destroy electronic media following the NIST guidelines for sanitizing media.

Breaches or potential breaches involving only secure PHI are not technically breaches under the final rules. When you document the situation, include the methods you used to secure the PHI.

If the PHI was not considered secure, then you must investigate the situation. Review your Privacy policy, along with your use and disclosures procedures, to determine whether the use or disclosure was permitted under the Privacy and Security rules.

The following three situations are not breaches even if the use or disclosure was not permitted:

1. A workforce member unintentionally acquires, accesses or uses PHI.
2. Someone authorized to access PHI at a covered entity inadvertently discloses it to a business associate or someone else authorized to access PHI at a covered entity.
3. A covered entity or business associate inadvertently discloses PHI in a good faith belief that the unauthorized person to whom PHI was disclosed would not be able to reasonably retain the information.

Keep a record of the situation if it meets one of these exclusions. No further investigation is needed.

In all other cases the investigation must continue. In the third step, the covered entity must conduct a risk analysis asking the following four questions:

1. What was the nature and extent of the PHI involved in the breach?
2. Who used PHI or to whom was the PHI disclosed?
3. Was the PHI actually acquired or viewed?
4. Was the risk of the potential breach mitigated by the actions of a covered entity or business associate?

If, based on these four questions, the covered entity believes the PHI has been compromised, a breach has occurred. The final step of the breach process requires the covered entity to notify everyone affected, the DHHS and in some situations, the media.

Individual Notifications

After completing the risk analysis and determining that PHI was indeed compromised, the covered entity must notify affected plan participants of the breach within 60 days of discovering it. A breach is considered "discovered" at the point when it becomes known to anyone at the covered entity, or at the point when it would have been known if the covered entity had been reasonably diligent.

If a business associate or a subcontractor committed the breach, it is deemed discovered once the business associate knows of it. Business associate agreements should specify a reasonable length of time for the business associate to report breaches to the covered entity. The covered entity is responsible for notifying the participant, so the business associate must notify the covered entity of the breach promptly in order to give the covered entity sufficient time to provide notices.

The notice must include the following information:

- A brief description of what occurred, 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

Continued on Page 8

and claim information. The description is intended to be general when describing the categories of information disclosed.

- The steps participants should take to protect themselves from any potential harm caused by the breach.
- A description of what you are doing to mitigate the harm and to safeguard against any future breaches of PHI.

Deliver the notice by first class mail or electronically if the participant permits that delivery method.

Media Notifications

Notifying the media is necessary only in specific breach situations. If the breach affects more than 500 residents of a state or jurisdiction (including the District of Columbia, the Commonwealth of Puerto Rico, the U.S. Virgin Islands and Guam), covered entities must notify the media, preferably a prominent media outlet in the area where the affected people reside.

Covered entities must notify the media within 60 days after the discovering the breach. Very few breach situations will require this step.

DHHS Notifications

Covered entities must notify the Department of Health and Human Services (DHHS) of **all** breaches.

The DHHS reporting process differs, depending on the number of people the breach may affect:

- If the breach affects 500 or more people, you must notify the DHHS immediately (within 60 days of the beach's discovery at the very latest).

Type of Violation	Potential Penalty
If the offenders did not know and by exercising reasonable diligence would not have known	$100 for each violation (capped at $25,000) for all violations (in a calendar year) of an identical requirement
If the violation was reasonable and not caused by deliberate neglect	$100 for each violation (capped at $100,000) for all violations (in a calendar year) of an identical requirement - fine waived if corrected within 30 days
If violation was caused by deliberate neglect, but was corrected	$10,000 for each violation (capped at $250,000) for all violations (in a calendar year) of an identical requirement
If violation was caused by deliberate neglect, but was not corrected	$50,000 for each violation (capped at $1,500,000) for all violations (in a calendar year) of an identical requirement

- If the breach affects fewer than 500 employees, you must still report the breach, but in an annual report:
  - Keep a log of breaches affecting fewer than 500 people in each calendar year. The log should describe each incident.
  - Submit the details of these smaller breaches within 60 days of the start of the next calendar year.

Submit all breach notifications electronically to the DHHS at http://www.hhs.gov/ocr/Privacy/hipaa/administrative/breachnotificationrule/brinstruction.html.

Covered entities must keep all breach-related documents for a minimum of six years.

Penalties

Covered entities failing to comply with HIPAA rules may have to pay a fine and may also be sued in civil court. The penalties included in the initial Privacy and Security rules were relatively light. Many felt the rules were ineffective because of the lack of accountability and the minimal penalties. HITECH substantially changed the penalty picture by dramatically increasing the penalties permitted. It also allowed state attorneys general to sue a covered entity on behalf of state residents.

Covered entities that fail to comply with the HIPAA Privacy and Security rules may be subject to the following:

- **Civil Money Penalties** - These fines can be substantial. They start at $100 for each violation up to $50,000 for each violation. They are capped from $25,000 a year to $1,500,000 a year. Penalty amounts are based on intent and how the covered entities correct the situation. Civil monetary penalties are outlined in the chart above.

Continued on Page 9

- **Civil Action** – A state attorney general may file a civil action on behalf of state residents for HIPAA violations.
- **Criminal Penalties** – These penalties may apply if a person knowingly violates HIPAA rules by using or disclosing individually identifiable health information. Enhanced penalties can apply if a violator acted for personal gain or with malicious intent.

The final rules require the Secretary of Health and Human Services to formally investigate all violations due to willful neglect.

The Office of Civil Rights (OCR) audits compliance with Privacy, Security and breach protocols. Your organization should be ready in case of an audit. The penalties associated with HIPAA non-compliance can be substantial.

Concluding Thoughts

The HIPAA Privacy and Security Rules are very complex. This *Advisor* provides only a high-level summary of the compliance steps. Initially, the penalties were insignificant and the federal government was not monitoring compliance. As a result, many covered entities took few steps to comply with the Rules.

However, HITECH has dramatically changed the penalties along with many aspects related to HIPAA compliance. The final rules added a few changes last year. It is now imperative your organization take steps to comply with the Privacy and Security rules.

If you are not confident that your compliance activities would fare well upon review, refer to the OCR site describing audit activities, found at http://www.hhs.gov/ocr/Privacy/hipaa/enforcement/audit/protocol.html. A review of this site should help you assess whether your compliance activities are adequate.

If you have any questions, please contact your McGraw Wentworth Account Manager. MW

McGraw Wentworth

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

http://www.twitter.com/McGrawWentworth
http://www.linkedin.com/company/McGraw-Wentworth
http://www.facebook.com/McGrawWentworth