



BENEFIT *Advisor*

In This Issue

In this fifth issue of the McGrawWentworth Benefit Advisor for 2009, we review the recently passed changes to HIPAA's Privacy and Security Rules. The changes to these rules will require employers to revisit their privacy and security compliance steps. Employers may need to make several amendments to their policies and procedures.

It will be important to review your current compliance steps thoroughly as the new rules also substantially increase the penalties for non-compliance.

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.

“Latest Guidance on HIPAA and Security Rules”

The American Recovery and Reinvestment Act of 2009 (ARRA) does not just pertain to COBRA, it also makes major investments in health information technology. ARRA's Health Information Technology for Economic and Clinical Health Act (HITECH Act) funds the move to electronic medical records. Many believe that electronic medical records will significantly decrease the cost and increase the quality of health care in the United States.

Many health care providers question this move to electronic health records. They are very concerned with not only the business expense of changing their record management systems but also the security of health information. The security issue is significant and the government understands the need to develop security protocols to keep this data confidential.

Lawmakers tackled medical information security under HIPAA's Privacy and Security Rules. Because the consensus was the existing HIPAA rules do not do enough to protect medical information, they decided to include amendments to the HIPAA Privacy and Security Rules in ARRA. These new amendments require covered entities to take stronger action to secure protected health information.

In this *Benefit Advisor*, we:

- Overview the basics for HIPAA Privacy and Security Rules
- Discuss the following HITECH changes:
 - Business Associate Requirements
 - Breach of Data Requirements
 - General Updates to Privacy and Security Rules
 - Personal Health Record Additions
 - Stricter Enforcement and Stronger Penalties for Violations
- Offer Action Steps to Comply with HIPAA Changes



The new HITECH Act strongly secures the confidentiality of protected health information. Employers do have some time to update their privacy and security policies and procedures. Most of the changes do not become effective until February 17, 2010.

Overview of the Basics for HIPAA Privacy and Security Rules

The HIPAA Privacy Rules became effective for most group health plans on April 14, 2004. The Security Rules became effective on April 21, 2006.

Initially, the Privacy and Security Rules applied only to the following entities:

- 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.

Privacy Rules safeguard specific certain health information. Protected health information (PHI) is "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." The Privacy Rules require group health plans to use PHI only for plan administration and other permitted activities. In addition, companies need to consider how the health plan uses PHI. Compliance steps varied depending on whether the plan is fully insured or self-funded.

Most organizations offer medical flexible spending accounts. The law treats these accounts the same as self-funded medical plans. Thus these employers need to take the steps necessary for self-funded plans to comply with Privacy Rules. The health plan should have:

- Appointed a privacy officer.
- Designated a complaint contact, a process for filing complaints, and a procedure to investigate and respond to complaints.
- Executed contracts with the plan's business associates.
- Developed a process to handle the following rights of individuals:
 - Right to see and copy PHI
 - Right to amend PHI
 - Right to be informed of PHI disclosures
 - Right to confidential communications
 - Right to restrict the use of PHI
- Established procedures to protect PHI that explain how the plan will use and disclose PHI as a part of plan administration.
- Created a firewall document naming the people or departments allowed access to PHI to perform plan functions and to administer the health plan.
- Amended plan documents to explain how the plan will comply with the Privacy Rule and how the plan will use and disclose PHI.



- Distributed a privacy notice stating all of the plan's intended PHI disclosures and uses.
- Signed a plan sponsor certification. This simple statement to the group health plan

verifies the organization has amended the plan document and will use PHI only for plan administrative functions. If your plan is insured, it is

likely your insurance carrier provides this form. If your plan is self-funded, your TPA probably provides this form.

- Implemented physical safeguards:
 - Review all the areas where PHI is actually stored. Are these locations safeguarded and is access limited only to your "workforce members"?
 - Review all areas where PHI is received, including fax machine areas and mail rooms. Are these areas secured and is access reasonably limited to workforce members?
- Addressed electronic safeguards:
 - Review all the areas in your organization that keep PHI on an electronic system.
 - Ask your IT department how your electronic information is safeguarded.

- Verify only your workforce has access to electronic PHI.
- Developed a training program and adopt a training process. Training must be documented for all workforce members.

While your organization may have taken appropriate steps to comply with HIPAA Privacy Rules, you may now need to amend some of your HIPAA policies to comply with the HITECH Act.

The Security Rules apply to protected health information stored or transmitted electronically. Under the Security Rules employers need to meet the eighteen standards listed below to protect that information. The standards are divided into three separate sections:

Administration Safeguard Standards

1. Security management process
2. Security responsibility
3. Workforce security
4. Information access management
5. Security awareness and training
6. Security incident procedures
7. Contingency plan
8. Evaluation
9. Business associate contracts and other arrangements

Physical Safeguard Standards

10. Facility access controls
11. Workstation use
12. Workstation security
13. Device and media controls

Technical Safeguard Standards

14. Access controls
15. Audit controls
16. Integrity
17. Person or entity verification
18. Transmission security

Covered entities needed to meet each of these standards in order to fully comply with the Security Rule. If your organization met these standards, it satisfied the overall goals of the Security Rule. The overall goals of the Rules required 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.



Rules. These organizations may wish to revisit their processes for complying with the Security Rules given the HITECH Act changes.

The overall goal of the Privacy and Security Rules is to protect the health information a covered entity has in its possession and to make sure the information is not improperly disclosed or improperly used. For example, organizations should never use health information for employment related decisions.

Business Associate Requirements

These regulations recognized that health plans sometimes hire business associates to administer the group health plan. Business associates may include your third party administrator, your PPO network, your pharmacy benefit manager and so on. The business associate contract must provide satisfactory assurances that the business associate will protect PHI and EPHI. The responsibility of the business associate has increased significantly under the HITECH Act.

The initial Privacy and Security Rules simply required business associates to provide satisfactory assurances that they are protecting PHI and EPHI. The government had no legal right to penalize business associates if they did not comply. In addition, covered entities were not required

Complying with the Security Rule was quite challenging for group health plans. It required Human Resources and Information Technology areas to work together to meet the requirements. For that reason many organizations took minimal steps to comply with the Security

to monitor the administrative practices of the business associates. However, if the covered entity knew that the business associate violated the rules, the covered entity was required to take action.

The HITECH Act significantly changes the business associate's responsibilities. Under the HITECH Act, the HIPAA Privacy and Security Rules will apply directly to business associates. This would include potential penalties for violating the Privacy and Security Rules.

This change may not significantly affect covered entities themselves. However, they will need to update their business associate agreements to reflect the business associate's additional responsibilities. Business associates will need to revisit their procedures. The government is expected to release more information over the next year to help business associates comply with the new HITECH provisions.

Breach of Data Requirements

The initial Privacy and Security Rules did regulate improper disclosures of PHI and EPHI. Covered entities had to mitigate any harm the breach caused, investigate the situation and possibly change their procedures to avoid any future breaches. They were not required to notify individuals of such a breach. Critics have long felt that these measures were not strong enough.

The new provisions under the HITECH Act significantly changes how breaches and misuses of PHI/EPHI will be handled. The Act provides very stringent actions a covered entity or a business associate must take if there is a breach related to unsecured PHI. Unsecured PHI is defined by the HITECH Act as PHI that

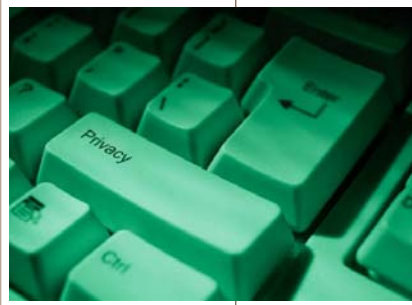
is not secured through the use of technology or a methodology set forth by the Secretary of the Department of Health and Human Services (DHHS). A breach is defined as the unauthorized acquisition, access, use or disclosure of PHI that compromises the security or privacy of this information. This definition is very specific and would exclude unauthorized disclosures that are inadvertent or unintentional. More guidance is expected over the next year to define what the DHHS will determine to be secured technologies or methodologies for protecting PHI and EPHI.

If the breach is made of unsecured PHI or EPHI, or if the covered entity reasonably believes a breach has occurred, the covered entity must notify the individual impacted by the breach within 60 days of the discovery of the breach of PHI or EPHI. The notification to the individual does not have to be done if it would impede a criminal investigation or harm national security. If a business associate experiences a breach of PHI or EPHI, the business associate is required to notify the covered entity of the breach in security.

Not only do covered entities need to notify the individuals affected, they also need to notify the Secretary of the Department of Health and Human Services (DHHS) of a breach of unsecured PHI or EPHI. The good news is that if the breach affects fewer than 500 people, the covered entity can keep a log of breach incidents and notify the Secretary of the DHHS once a year. If the breach affects more than 500 people, the covered entity must notify the Secretary of DHHS and the

local media immediately. The DHHS will then post a list of the covered entities involved in these breaches.

More specific information on handling breaches will soon be published. However, all covered entities will need to take certain steps to comply with these changes. First, they will need to amend their HIPAA privacy and security policies and procedures to define a breach of unsecured PHI. Second, they will need to amend the details in their policies and procedures on handling these breaches. Finally, they will need to watch for additional guidance on handling breaches affecting more than 500 people.



These new breach requirements will force covered entities to disclose

breach incidents to the people affected. If the breach affects a significant number of people, the reporting to the DHHS and the local media will put breaches in the public spotlight. This potential for negative publicity may compel employers to revisit their privacy and security policies and perhaps take stronger steps to secure PHI and EPHI more carefully.

General Updates to Privacy and Security Rules

The HIPAA Privacy Rules contain a number of individual rights relating to PHI, such as the right to see and copy PHI records, the right to amend PHI, the right to request restrictions when using PHI and so on.

ARRA has expanded these individual rights in a number of ways, including:

- Individuals can ask to receive their PHI electronically if the covered entity maintains electronic health records.
- The right to request restrictions on the use of PHI has been expanded. Covered entities cannot disclose PHI to health plans when the individual has fully paid for the services out of pocket and does not intend to ask the health plan to pay for those services.
- The HITECH Act expands the situations when a covered entity must account for disclosing PHI. Initially, covered entities had to maintain accounting of certain disclosures for six years. (An example of an accountable reason for disclosing information might be if PHI was requested as part of a court order.) The HITECH Act expands the situations when a covered entity must account for a disclosure. The covered entity must account for any PHI disclosures made by the covered entity or a business



associate associated with treatment, payment and health care operations during the previous three years and only if the disclosures were made through an electronic health record. Covered entities will have more time to comply with this requirement. The Act stipulates that the government must issue more guidance on the information to be included in this accounting. For accountings related to electronic health records held by a covered entity as of January 1, 2009, this accounting requirement will apply to disclosures made on or after January 1, 2014. For electronic health records held by a covered entity after January 1, 2009, the accounting rule will apply to disclosures on or after January 2011.

One of the more interesting aspects of the ARRA rules applies to the Security Rules. The provisions of the original Security Rules were initially very non-specific. The lack of specificity was intentional. One reason for the lack of specifics was the numerous strategies covered entities could adopt to comply with the rules. Another reason noted was the changes in technology occur so quickly, the rules could not be technologically specific because they would be quickly outdated. The Secretary of the Department of Health and Human Services will issue annual guidance to discuss the most appropriate technical safeguards that covered entities can adopt to protect EPHI. This annual guidance will prompt covered entities to review

their security protocols annually and make updates when necessary.

Personal Health Record Additions

While HIPAA rules apply only to covered entities, the HITECH Act applies to business associates as well. It also extends the HIPAA privacy and security breach notification provisions to vendors of personal health records (PHRs) and any organizations associated with the PHR vendors, for example, organizations that sell products and services through the PHR website. The regulations also create a new term – unsecured PHR identifiable health information. The new rules are not limited to protecting PHI or EPHI. Personal health record vendors are compelled to protect identifiable health information that is maintained in the health record.

Primarily, these vendors must now meet the disclosure of breach requirements. These organizations must notify both the people the breach of unsecured PHR identifiable health information affects and the Federal Trade Commission (FTC). The FTC will notify the Secretary of the Department of Health and Human Services of a breach.

Stricter Enforcement and Stronger Penalties for Violations

The original HIPAA Privacy and Security Rules include fines and criminal penalties depending on the intent of the potential violation. The HITECH Act significantly increases the penalties for violating these rules. The changes include the following:

- The HITECH Act establishes four new tiers of civil monetary penalties. Initially, these fines were \$100 for each violation capped at \$25,000 for violations of the same requirement within a calendar year. The act increased the fines significantly and these increased penalties are effective immediately. (See table to the right.)
- The Act also expanded the power of the Office of Civil Rights (OCR) to investigate potential HIPAA violations. The OCR can refer a case to the Justice Department for criminal investigation. If the Justice Department fails to prosecute, the OCR can assess a fine.
- The HITECH Act revisions require a formal investigation and fines for violations caused by willful neglect. The Secretary of the Department of Health and Human Services must issue regulations within 18 months after the bill passes to explain how this investigation process will be handled.
- The Act authorizes any state attorney general to sue anyone violating HIPAA Rules in federal district courts. Previously, these lawsuits were not permitted. However, only the

Type of Violation	Potential Penalty
If offenders did not know, and by exercising reasonable diligence would not have known that they violated the law.	\$100 for each violation capped at \$25,000 for all violations of an identical requirement within the calendar year. ARRA waives the fine if the violation is corrected within 30 days.
If the violation was reasonable and not caused by deliberate neglect, the fine is higher.	\$1,000 for each violation capped at \$100,000 for all violations of an identical requirement within the calendar year. ARRA waives the fine if the violation is corrected within 30 days.
If the violation was caused by deliberate neglect, but was corrected, the fine increases.	\$10,000 for each violation capped at \$250,000 for all violations of an identical requirement within the calendar year.
If the violation was caused by deliberate neglect, and was not corrected, the fine is even higher.	\$50,000 for each violation capped at \$1,500,000 for all violations of an identical requirement within the calendar year.

state attorney general can sue, and the Act limits damages to \$100 for each violation capped at \$25,000.

- Finally the Government Accounting Office (GAO) must develop a process for allowing harmed individuals to receive a share of the fines assessed for violations. The Secretary of Health and Human Services has three years to pass legislation based on the GAO recommendations.



The HITECH Act has significantly increased the penalties for deliberately violating or not following HIPAA Privacy and Security Rules. Employers should make sure they are adequately protecting health information. They now face not only significantly increased fines, but also potential bad publicity and possible lawsuits.

Action Steps to Comply with HIPAA Changes

While employers have time to make the changes the HITECH Act requires, your organization should begin to think through the areas that you will need to review. For some of the changes, you will need additional details to fully comply.

Complying with these new provisions will be a challenge. These rules apply to many organizations that use health information to provide and pay for health care. You need to *balance your organization's compliance actions with the relative amount of PHI/EPHI your organization uses or maintains.*

To develop an action plan take the following key steps:

Step 1: Look at all the HIPAA Privacy and Security materials your organization has developed. Both of the rules stress documenting compliance steps. You need to find these materials for two reasons. First, the HITECH Act significantly increases the penalties for not following the rules. Because of the added liability, your organization should review the action steps you took to comply with the Privacy and Security Rules in the past and decide whether you need to revise any of your compliance steps. Second, the HITECH Act will require you to modify a number of your compliance plans to meet the new requirements.

Step 2: Identify all your current business associates. You probably identified business associates in the past but you may have different business associates now. Remember, a business associate is an organization that uses PHI or EPHI to perform a function on behalf of your group health plan. Business associates may include your third party administrator, your pharmacy benefit manager, your benefits consultant and so on. Once you identify these associates, ask them to update their business associate agreements to reflect their additional responsibility under the HITECH Act. While it is the group health plan's responsibility to execute business associate contracts, in practice most business associates create contracts for group health plans to sign. On December 1 follow up with business associates that have not updated the wording in their contracts.

Step 3: Review your EPHI and PHI breach policies and procedures. The HITECH Act has created new definitions of breach and unsecured PHI

or EPHI. Your organization will need to add these new definitions. Expect more government guidance defining these concepts.

In addition, because you are a covered entity, you will need to disclose potential breaches to anyone affected, the Department of Health and Human Services, and potentially the media. Besides adding this detail to your policies, you should create a procedure for handling potential breach situations to make sure you notify all the appropriate parties.

Step 4: Update your policies and procedures. Review the following areas:

- *Requests for access to an individual's own PHI.* Make changes to allow your organization to send PHI or EPHI records electronically if the information is in an electronic health record.
- *The right to request restrictions on the use of PHI.* If a plan participant pays in full for a service and does not intend to ask the health plan to pay, then the participant has the right to ask covered entities not to disclose this health information. For the most part this requirement will apply to health care providers.
- *Business associates using electronic health records.* If your business associates uses electronic health records, you may want to include follow up on the changes in the disclosure rules that apply to electronic medical records. The government will need to

issue additional guidance, so it is too early to modify your current procedures.

Step 5: Create an annual reminder to review your Security Rule compliance. The government will issue guidance every year to address appropriate compliance actions.

The HITECH Act made many changes to the HIPAA Privacy and Security Rules. Your organization will need more government guidance to determine the steps necessary to comply with these changes. Because penalties for violating these rules can be significant, you'll need to review your compliance steps carefully. You

must adequately protect PHI and EPHI. If your initial compliance steps do not fully protect PHI, you should modify your policies and procedures to strengthen your position.

McGraw Wentworth will keep you posted on any further developments on the HITECH Act. Please contact your McGraw Wentworth Account Manager with any questions. **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