

Legislative Brief

The Health Insurance Portability and Accountability Act of 1996



The Health Insurance Portability and Accountability Act of 1996 (HIPAA) contains a number of provisions that affect group health plans, including rules related to portability, insurance market requirements and administrative simplification. This issue of the Scott Benefit Services Legislative Brief will provide you with an overview of the major provisions of HIPAA that affect your organization's employee benefits.

PORTABILITY PROVISIONS

The group health insurance portability provisions of HIPAA provide important protections for individuals who have pre-existing medical conditions and move from one job to another. Prior to HIPAA, these individuals might have been denied coverage under the new employer's health plan or were required to serve a pre-existing condition waiting period.

Pre-Existing Condition Limitations

HIPAA regulates pre-existing condition limitations in the following ways:

- Defines a pre-existing condition as a condition for which medical advice, diagnosis, care, or treatment was recommended or received within the previous 6-month period ending on the individual's enrollment date. For individuals who apply at initial eligibility, the enrollment date is the date that coverage is effective or the date of hire, whichever is earlier. For all other individuals, the enrollment date is the day coverage is effective.
- States that group health plans may no longer exclude a condition because a reasonably prudent person would have sought treatment.
- Prohibits limiting coverage for a pre-existing condition beyond 12 months for individuals that apply when initially eligible or during a special enrollment period. A pre-existing condition waiting period of no more than 18 months may be applied to late enrollees.
- Prohibits the application of a pre-existing condition limitation to newborns and adopted children if coverage is requested within 30 days of the birth or adoption.
- Does not allow pregnancy to be treated as a pre-existing condition.
- Requires that the pre-existing condition waiting period be reduced by the number of days the individual had prior creditable coverage if the prior coverage did not terminate more than 63 days prior to the enrollment date. (Note: Any waiting period does not constitute a break in coverage.)
- Requires a plan to give written notice of a pre-existing condition exclusion's existence and terms (including any applicable waiting period) and of the individual's right to demonstrate creditable coverage. This notice must be part of any written application materials distributed by the plan.

Certificates of Creditable Coverage

An individual may reduce a pre-existing condition limitation by demonstrating that he or she previously had creditable health coverage. HIPAA requires a group health plan or health insurer to issue a certificate of creditable coverage to an individual who loses regular health coverage or COBRA coverage under the plan. An individual may also request a certificate while covered by the plan or within two years after losing coverage.

The certificate must include the following information:

- The date the certificate was issued.
- General identifying information regarding the group health plan and the participant or beneficiary.
- The date any waiting period began.

Legislative Brief

The Health Insurance Portability and Accountability Act of 1996

- The dates that coverage began and ended. However, if the individual had at least 18 months of uninterrupted coverage under the plan, the certificate may simply state that fact.
- An educational statement explaining HIPAA rights.

The deadline for providing the certificate depends on the reason the individual is losing coverage. For a loss of coverage due to an event that is a COBRA qualifying event, the certificate must be provided by the deadline for providing the COBRA election notice. For other losses, the certificate must be provided as soon as the plan can provide it, if it is acting in a reasonable and prompt fashion.

Special Enrollment Rights

HIPAA also requires that insurers and health insurance plans recognize special enrollment periods. If an individual applies for coverage during a special enrollment period, he or she may not be considered a late enrollee. HIPAA requires that:

- Group health plans and insurers provide eligible employees and their eligible dependents with an opportunity to enroll when they a) had other coverage at the time of enrollment, b) waived coverage at the time of enrollment and c) lose the other coverage. The applicant must apply within **30 days** of the loss of other coverage. The effective date of coverage is the first of the month following the date the application is received. The "loss of coverage" can be due to an exhaustion of COBRA, reduction in hours, divorce, or termination of employer premium contributions.
- Group health plans and insurers allow eligible employees and their dependents to enroll in the plan in the event of a marriage, birth, adoption, or placement for adoption. Again, the eligible employee or eligible dependent must apply within **30 days** following the event. The effective date of coverage for marriage is the first day of the month following the request for enrollment. Otherwise, the effective date is retroactive to the date of the birth, adoption, or placement for adoption. Note: The eligible employee can add himself, his spouse and/or newly-acquired dependents during the special enrollment period.
- Effective April 1, 2009, group health plans and insurers provide eligible employees and their dependents with the opportunity to enroll in the plan if they lose coverage under a Medicaid plan or State Children's Health Insurance Program (CHIP) or become eligible for a premium assistance subsidy under Medicaid or CHIP. Eligible individuals must be given **60 days** after the loss of coverage or determination of eligibility for assistance to request coverage under the plan. It appears that the effective date of coverage would be the first of the month following the date of the request, although regulations have not yet been issued to confirm the effective date.

Nondiscrimination Rules

HIPAA prohibits discrimination by group health plans and insurers based on health status related factors. Insurers or health plans may not determine eligibility of any individual to enroll based upon health status related factors. Neither plans nor insurers may require an individual to pay a premium or contribution that is greater than that for a similarly situated individual based upon a health status related factor.

Health status related factors include:

- Health status,
- Medical condition (physical or mental),
- Claims experience,
- Receipt of health care,
- Medical history,
- Genetic information,
- Evidence of insurability (including participation in dangerous activities like skiing, motorcycling and horseback riding), and
- Disability.

Legislative Brief

The Health Insurance Portability and Accountability Act of 1996

Group health plans may still impose limits on benefits, as long as the limits do not discriminate based on a health factor and treat similarly situated individuals alike. For example, a plan may exclude all coverage for a specific condition or include a lifetime cap on certain benefits, provided that the limits are not directed at individual sick employees or dependents. Plans may also discriminate in favor of participants and beneficiaries who have adverse health conditions. For example, a group health plan that usually provides coverage for dependents until age 23 can choose to provide dependent coverage for disabled dependents beyond age 23.

Nondiscrimination rules also apply to wellness programs. Specifically, the rules distinguish between standard-based programs and participation-only programs. Standard-based programs provide rewards based on satisfaction of a health standard. To comply with HIPAA, these programs must:

- Provide a reward that is no more than 20% of the cost of coverage;
- Be designed to promote health or prevent disease;
- Give participants an opportunity to qualify for the reward at least once per year;
- Provide a reward that is available to all similarly-situated individuals (i.e., a reasonable alternative standard must be available for those for whom it is unreasonably difficult, because of a medical condition, or medically inadvisable to meet the standard); and
- Disclose that alternative standards or waivers are available.
- Participation-only plans reward individuals for participating in the program and do not require satisfaction of a health standard. Participation-only programs must be available to all similarly-situated individuals and do not have to meet additional nondiscrimination requirements.

INSURANCE MARKET RULES

Group Health Insurance Provisions

HIPAA includes provisions that require health insurance issuers to make health care coverage available to a greater number of individuals. These provisions are summarized below.

All products marketed to small employers (2-50 employees) must be made available to all small employers, regardless of the health status of its employees, and all individuals who apply for coverage when they are first eligible must be accepted. However, HIPAA does not limit the amount an insurer may charge an employer for coverage.

HIPAA requires that an insurer renew an employer's group health plan, unless:

1. The group commits fraud or intentional misrepresentation of material fact used to issue coverage.
2. The group fails to pay premiums when due or within the allowable grace period.
3. The insurer discontinues offering a particular type of group health plan or ceases to offer group health plans in the state. In each case, the insurer is required to provide advance notice to the employer. In some cases, the insurer is required to offer another product if appropriate.
4. The employer no longer has a covered employee who resides, lives, or works in the insurer's service area.
5. The employer violates mandatory contribution or group participation requirements.

When the group health plan is offered to association members, termination of an employer's membership in the association will also allow the insurer to cancel the employer's group health plan.

Individual Health Insurance Provisions

HIPAA ensures that certain individuals are guaranteed access to individual health insurance coverage through the individual health insurance provisions.

Eligible Individuals

Health insurers offering individual health insurance policies must offer coverage to any individual that meets the following criteria:

- The individual was most recently covered under a group health plan, governmental plan or church plan for a period of at least 18 months;
- The coverage ended no more than 63 days prior to the date of application;

Legislative Brief

The Health Insurance Portability and Accountability Act of 1996

- The coverage did not terminate because of fraud or nonpayment of premiums;
- The individual is not eligible for Medicare, Medicaid or a group health plan and is not covered by any other insurance; and
- The individual is ineligible for COBRA or if offered COBRA continuation coverage (or continuation coverage under a similar state law) has both elected and exhausted their continuation coverage.

Required Coverage

A policy issued to an individual meeting these criteria may not contain pre-existing conditions and must be guaranteed renewable. As with group policies, the insurer must also provide a certificate of coverage if the policyholder cancels. An insurer may comply with HIPAA by offering individuals the following:

- All of its individual health insurance products offered in the market;
- Two policies determined to be the insurer's most popular individual policies measured by premium volume; or
- Two policies — a high deductible and a low deductible plan, with average benefits.

Acceptable State Alternative

If a state has an acceptable alternate mechanism for assuring access to individual health coverage, insurers in that state will not have to comply with the individual health insurance provisions in their entirety. Health risk pools or mandatory conversion policies are two examples of acceptable state alternatives. If an acceptable state alternative is available, insurers are not required to guarantee issue their individual policies. Instead, they are only required to offer policies that are guaranteed renewable and must issue certificates of coverage if the individual terminates the policy.

ADMINISTRATIVE SIMPLIFICATION

HIPAA's Administrative Simplification provisions include rules regarding Electronic Data Interchange (EDI), Privacy and Security. These rules apply to "Covered Entities," which are defined by HIPAA as health plans, health care clearinghouses and health care providers that conduct certain electronic transactions.

Electronic Data Interchange (EDI)

The EDI rules provide standards for payment-related electronic transactions (covered transactions) conducted by Covered Entities. These rules are designed to streamline the electronic communications between Covered Entities. The rules set out format and content requirements, uniform codes and specific format and content for each transaction. Transactions that qualify for these standards include:

- Health claims;
- Benefit payments;
- Coordination of benefits; and
- Health plan enrollment.

Transactions that use paper only or are conducted via the telephone do not qualify as covered transactions.

In addition, health plans that are Covered Entities must comply with the following special rules:

- Must conduct a transaction as a standard transaction (i.e., in accordance with EDI standards) if another entity requests.
- May not delay or reject a transaction because it is a standard transaction.
- May not reject a standard transaction because it contains data elements not needed or used by the health plan.
- May not require providers to make changes or additions to standard transactions.

Privacy Rule

The Privacy Rule provides standards for access, use and disclosure of personally identifiable information, or protected health information (PHI). In general, the Privacy Rule provides that Covered Entities may use and disclose PHI for treatment, payment and health care operations. Other disclosures of PHI require authorization from the individual.

Legislative Brief

The Health Insurance Portability and Accountability Act of 1996

However, PHI may be disclosed without authorization in instances involving a public policy purpose, such as for judicial or administrative proceedings, or to protect public health and safety.

Many of these disclosures are subject to the minimum necessary standard, which requires that the PHI used or disclosed be the minimum amount necessary to achieve the purpose of the disclosure. The Privacy Rule also imposes requirements for disclosing PHI to a group health plan sponsor and to a Covered Entity's service providers or "business associates."

It also grants individuals rights regarding access to, use and disclosure of PHI and the right to receive notice of privacy practices. A covered entity must provide a notice of privacy practices to individuals whose PHI it maintains. The notice must explain the uses and disclosures that may be made, the individual's rights regarding PHI and the Covered Entity's legal duties.

The Privacy Rule also requires Covered Entities to comply with the following administrative requirements:

- Appoint a Privacy Official;
- Conduct workforce training;
- Establish safeguards for protecting PHI;
- Create a complaint process;
- Establish a disciplinary process;
- Mitigate improper use or disclosure of PHI;
- Refrain from intimidation of or retaliation against individuals for exercising HIPAA rights;
- Do not require waivers of HIPAA rights; and
- Implement privacy policies and procedures.

Security Rule

The Security Rule provides standards for protecting electronic PHI (ePHI) maintained by a Covered Entity. It requires Covered Entities to implement safeguards to:

- Ensure confidentiality, integrity and availability of ePHI;
- Protect against reasonably anticipated threats to security and impermissible uses or disclosures of ePHI; and
- Ensure compliance with the standards by the Covered Entity's workforce.

The required safeguards include administrative, physical and technical safeguards. To ensure that it is meeting the requirements, a Covered Entity must perform a risk analysis to determine how to comply with the implementation specifications outlined in the Security Rule.

Please contact your Scott Benefit Services representative with any questions or to receive further information on other areas regulated by HIPAA.

EAM 6/09

This Scott Benefit Services Legislative Update is not intended to be exhaustive nor should any discussion or opinions be construed as legal advice. Readers should contact legal counsel for legal advice.

Content copyright © 2004- 2009 Zywave, Inc. Images copyright © 2000-2004 Getty Images, Inc. All rights reserved.

Legislative Brief

HIPAA Privacy Regulations *What are Plan Sponsors Required to Do?*



While employers are not directly regulated by the HIPAA Privacy Rules, the rules indirectly affect employers that sponsor group health plans. The compliance requirements imposed on the plan sponsor will vary, depending upon whether or not it has access to personally identifiable health information. This issue of the Scott Benefit Services Legislative Brief is intended to provide plan sponsors with an overview of what is required of them by the HIPAA Privacy Rules.

What are the HIPAA Privacy Rules?

As required by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the U.S. Department of Health and Human Services (HHS) released final federal regulations that govern the use and disclosure of personally identifiable health information in December 2000 (HIPAA Privacy Rules). Final changes to the regulations were published on August 14, 2002. In most cases, the deadline for compliance with the HIPAA Privacy Rules was April 14, 2003.

What entities are regulated by the HIPAA Privacy Rules?

The HIPAA Privacy Rules directly regulate the following Covered Entities:

- Health plans,
- Health care clearinghouses, and
- Health care providers that conduct certain transactions electronically.

The HIPAA Privacy Rules indirectly regulate plan sponsors and other third parties by requiring that a Covered Entity require an otherwise non-regulated entity to agree to comply with the restrictions contained within the HIPAA Privacy Rules.

What do the HIPAA Privacy Rules accomplish?

The HIPAA Privacy Rules place restrictions on how personally identifiable health information may be used and disclosed by certain organizations. While some states have laws that protect patients' privacy, the federal Privacy Rules establish a minimum level of privacy protections that must be afforded to all information covered by the Privacy Rules. In summary, the Privacy Rules:

- Require that individuals be told how their medical records will be used and disclosed,
- Set limits on how individuals' medical records may be used and disclosed, and
- Impose fines where the requirements contained within the regulations are not followed.

In short, the regulations allow protected health information to be used or disclosed by a Covered Entity for the purposes of treatment, payment, and health care operations, subject to the minimum necessary standard. Unless an exception applies, an individual's prior written authorization must be received before protected health information may be used in any other manner.

What information is governed by the HIPAA Privacy Rules?

The HIPAA Privacy Rules govern Protected Health Information (PHI), which is defined as information that is:

- Oral, written, or electronic,

Legislative Brief

HIPAA Privacy Regulations

What are Plan Sponsors Required to Do?

- Individually identifiable,
- Created or received by a Covered Entity, and
- Relates to past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

What are plan sponsors required to do?

The compliance requirements indirectly imposed upon a plan sponsor by the HIPAA Privacy Rules vary based on whether or not the plan sponsor has access to PHI.

Plan Sponsors Offering a Fully-Insured Group Health Plan — No Access to PHI

A plan sponsor that offers a fully-insured group health plan will be minimally impacted by the HIPAA Privacy Rules if its access to health information is limited to the following plan sponsor functions:

- Assisting employees with claim disputes as permitted by the employees' written authorization,
- Receiving Summary Health Information (SHI)¹ for purposes of obtaining premium bids or modifying, amending or terminating the plan, and
- Conducting enrollment and disenrollment activities.

While insurance carriers are required to comply with the majority of requirements contained within the HIPAA Privacy Rules on behalf of the group health plan, plan sponsors within this category may not:

- Require an individual to waive the rights afforded to him or her by the HIPAA Privacy Rules as a condition on the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits;
- Intimidate, threaten, coerce, discriminate against, or take other retaliatory action against an individual for exercising his or her rights provided by the HIPAA Privacy Rules; or
- Use PHI received in connection with an employee benefit plan when making employment related decisions.²

Plan Sponsors Offering a Fully-Insured or Self-Funded Group Health Plan — With Access to PHI³

Where a plan sponsor has access to PHI in order to perform plan administration functions⁴, the plan sponsor must do all of the following:

- Amend the plan documents to include a description of permitted uses and disclosures of PHI by the plan sponsor;
- Certify to the group health plan that the plan documents have been amended; and
- Comply with all of the administrative requirements contained within the HIPAA Privacy Rules.

What are the administrative requirements of the HIPAA Privacy Rules?

In general, the HIPAA Privacy Rules require plan sponsors with access to PHI, together with the group health plan, to comply with all of the following administrative requirements contained within the HIPAA Privacy Rules.

- Limit its use and disclosure of PHI to activities related to treatment, payment, and health care operations (unless specific patient authorization permits otherwise), including the creation of internal firewalls.
- Designate a privacy official.
- Train members of its workforce on its policies and procedures with respect to PHI.

¹ SHI summarizes claims history, claims experience, or type of claims experienced by individuals from whom a plan sponsor has provided health benefits under a group health plan. The HIPAA Privacy Rules require that certain identifiers such as name, social security number, and date of birth be excluded from SHI.

² The regulations provide an exception to the plan amendment requirement for plan sponsors within this category, however, some benefit experts disagree.

³ Self-funded, self-administered plans with fewer than 50 participants are not required to comply.

⁴ Plan administration functions include claims processing, quality improvement, and fraud detection activities.

Legislative Brief

HIPAA Privacy Regulations

What are Plan Sponsors Required to Do?

- Create policies and procedures designed to ensure compliance with the HIPAA Privacy Rules, including providing plan participants with a right to:
 1. Access and copy records containing their PHI,
 2. Amend records which contain their PHI,
 3. An accounting of disclosures made containing their PHI during the last 6 years⁵, and
 4. Request reasonable restrictions on the use and disclosure of PHI, including that communications containing PHI be sent to an alternate location.
- Provide a notice of privacy practices to all new plan participants at enrollment.⁶
- Provide a process for individuals to make complaints concerning its policies and procedures related to use and disclosure of PHI.
- Refrain from taking retaliatory action against an individual that makes a complaint with the plan sponsor, group health plan, or U.S. Department of Health and Human Services alleging a violation of the HIPAA Privacy Rules.
- Require that any business associate that is provided access to PHI agrees to limit its use and disclosure of PHI as set forth in the HIPAA Privacy Rules.
- Establish and apply appropriate sanctions against business associates and members of its workforce that fail to comply with its privacy policies and procedures.
- Report to the group health plan any violations of its privacy policy and procedures.
- Mitigate, to the extent possible, the harmful effect of any violation of its privacy policies.
- Not require individuals to waive their privacy rights as a condition of enrollment in the plan, eligibility for benefits, treatment, or payment.
- Refrain from using PHI received in connection with an employee benefit plan when making employment related decisions.
- If feasible, return or destroy all PHI when no longer needed.

Does a plan sponsor need to obtain a signed authorization in order to assist a plan participant with a claim?

Yes. In order for a plan sponsor or other third party to discuss a pending claim on behalf of the plan participant with an insurance carrier or third party administrator, the HIPAA Privacy Rules require the insurance carrier or third party administrator be provided with the plan participant's written authorization.

What happens if our organization doesn't comply with the HIPAA Privacy Rules?

Failure to comply with the HIPAA Privacy Rules may result in assessment of the following penalties:

- \$100 per violation, up to \$25,000 per year, per standard, for disclosures made in error;
- \$50,000 and/or one year in prison for knowingly obtaining or disclosing PHI;
- \$100,000 and/or up to five years in prison for obtaining information under false pretenses; and

⁵The accounting is not required to include those made for treatment, payment, or health care operations or pursuant to authorization.

⁶Thereafter, all plan participants must be notified every three years that a Privacy Notice is available and how they may obtain a copy. Plan sponsors of fully-insured plans with access to PHI must provide a HIPAA Notice of Privacy Practices upon request.

Legislative Brief

HIPAA Privacy Regulations

What are Plan Sponsors Required to Do?

- \$250,000 and up to ten years in prison for obtaining PHI with an intent to sell, transfer, or use it for commercial advantage, personal gain, or malicious harm.

How will Scott Benefit Services assist its clients in complying with the HIPAA Privacy Rules?

Scott Insurance will assist our clients with their HIPAA Privacy compliance efforts by:

- Providing them with a HIPAA Privacy Legislative Guide located on our Web site designed especially for our clients — MyWave™⁷;
- Continuing to keep our clients informed of the latest legal developments impacting employee benefit plans, including any future guidance from the Department of Health and Human Services related to the HIPAA Privacy Rules;
- Reviewing the services provided by third party administrators in response to the HIPAA Privacy Rules⁸; and
- Evaluating the need for and assisting with the creation of formal business associate relationships, including Scott Insurance, third party administrators, and pharmacy benefit management organizations.

How will Scott Benefit Services comply with the HIPAA Privacy Rules?

Like plan sponsors with access to PHI, insurance brokers are also indirectly regulated by the HIPAA Privacy Rules. In cases where Scott Insurance needs access to PHI in order to a) assist the plan sponsor with plan administration functions, b) obtain bids from insurance carriers, or c) recommend plan design modifications, we will ask that the plan sponsor enter into a business associate contract with us. In short, the business associate contract requires the insurance broker to limit its use and disclosure of PHI to the permissible uses defined by the plan sponsor.

Scott Insurance takes the obligations imposed upon it by the HIPAA Privacy Rules seriously. More importantly, we continue to follow policies and procedures designed to ensure that *all* confidential information entrusted to us by our clients is held in strictest confidence.

We look forward to continuing to be of service to you. Please contact your Scott Insurance representative with any questions.

9/02; EAM 1/09

This Scott Benefit Services Legislative Brief is not intended to be exhaustive nor should any discussion or opinions be construed as legal advice. Readers should contact their legal counsel for legal advice.

Content copyright © 2000-2008 Zywave, Inc. Images copyright © 2000-2004 Getty Images, Inc. All rights reserved.

⁷ The HIPAA Privacy Legislative Guide contains answers to commonly asked questions, legislative news, and sample forms.

⁸ The services offered by third party administrators in response to the HIPAA Privacy Rules vary. For example, some third party administrators will create and distribute a notice of privacy practices for their clients, while others will not.

Legislative Brief

HIPAA Regulations: Privacy, Security and Electronic Data Interchange



The Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) is a broad statute that contains many provisions that affect health plans. Some of the significant rules contained within HIPAA relate to ensuring the privacy and security of personally identifiable information (the Privacy and Security Regulations) and setting uniform standards for the transmission of electronic health care claims data (the Electronic Data Interchange Regulations).

This issue of the Scott Benefit Services Legislative Brief will provide an overview of each regulation.

Privacy Regulations

The HIPAA Privacy Regulations (or “Privacy Rule”) govern the use and disclosure of personally identifiable health information. The key items contained within the Privacy Rule are listed below.

- **Information Protected.** The Privacy Rule governs Protected Health Information, or PHI, which is personally identifiable health information in any form (oral, paper, and electronic).
- **Covered Entities.** The organizations governed by the Privacy Rule are known as Covered Entities, which include health plans, health care clearinghouses, and health care providers that conduct certain financial and administrative transactions electronically.
- **Patient Rights.** Patients must be given detailed written information explaining their privacy rights and how their information will be used (a Notice of Privacy Practices). Patients have a right to view their own health records and request corrections. Patients also have a right to obtain documentation of any disclosures made of their health care records.
- **Permitted Uses and Disclosures.** The Privacy Rule provides that PHI may not be used or disclosed other than as permitted by the Privacy Rule. The main permitted uses are for treatment of the individual, payment for the individual’s health care and health care operations of the Covered Entity. PHI may also be disclosed to plan sponsors for purposes of plan administrative activities. In some cases, disclosures may be made to an individual’s family and/or friends and for specific public policy purposes.
- **Business Associates.** Covered Entities may disclose PHI to certain vendors or service providers, known as Business Associates, if a proper contract protecting the PHI is in place.
- **Authorization for Other Uses.** Specific authorization must be obtained prior to any disclosure that is not expressly permitted by the Privacy Rule. Employers that sponsor health plans may not gain access to health information for employment-related purposes without the patient’s consent.
- **Minimum Necessary Standard.** When making a disclosure to another health care provider for purposes of treatment, providers have been given full discretion to determine what records shall be released. When a disclosure is made for purposes of payment, Covered Entities may send only the minimum amount of information needed.

Legislative Brief

HIPAA Regulations: Privacy, Security and Electronic Data Interchange

- **Administrative Requirements.** Covered Entities must comply with certain administrative requirements, such as appointing a Privacy Official, implementing safeguards to protect PHI and training members of the workforce.
- **State Privacy Laws.** Where a state has passed a law that conflicts with these regulations, the law that provides the greater privacy protections will apply.

Security Regulations

The HIPAA Security Regulations (or “Security Rule”) impose requirements on Covered Entities with respect to the protection of electronic PHI (“ePHI”).

- **Safeguarding ePHI.** The main purpose of the Security Rule is to ensure the confidentiality, availability and integrity of ePHI. Covered Entities must implement certain safeguards designed to do so. Covered Entities must protect against reasonably anticipated threats to ePHI and uses or disclosures of ePHI that are not permitted under the Privacy Rule. Covered Entities must also protect ePHI by ensuring that their workforces comply with the security requirements.
- **Safeguard Standards.** Covered Entities must implement reasonable and appropriate safeguard standards to protect ePHI. The safeguards are intended to be flexible depending on the type, size and sophistication of the Covered Entity. There are specific standards for administrative, technical, physical, organizational and documentation safeguards.

Enforcement of the Privacy and Security Regulations

- **Civil Enforcement and Penalties.** The Department of Health and Human Services (“HHS”) is responsible for enforcing the Privacy and Security Rules. The regulations set forth specific civil penalties ranging from \$100 per violation up to \$50,000 per violation, depending on the circumstances. Maximum civil penalties for violations of identical standards range from \$25,000 to \$1.5 million.
- **Criminal Enforcement and Penalties.** HHS may also refer cases to the Department of Justice for criminal prosecution. The criminal penalties vary depending on the circumstances of the violation:
 - ✓ \$50,000 and/or one year in prison for knowingly obtaining or disclosing protected information.
 - ✓ \$100,000 and/or up to five years in prison for obtaining information under false pretenses.
 - ✓ \$250,000 and/or up to ten years in prison for obtaining PHI with the intent to sell, transfer, or use it for commercial advantage, personal gain, or malicious harm.
- **Private Right of Action.** Neither the Privacy nor Security Rule grants individuals the private right to sue for violations. However, by February 17, 2012, HHS must establish a methodology for allowing a portion of the civil penalties paid for a violation to be paid to affected individuals.

Electronic Data Interchange Regulations

The Electronic Data Interchange (“EDI”) regulations set forth standardized electronic transaction guidelines for transmission of health care data.

- **Covered Entities.** The organizations governed by this regulation include health plans, health care clearinghouses, and health care providers that transmit any health information in electronic form. Self-administered group health plans with less than 50 plan participants are exempt. (Note: When

Legislative Brief

HIPAA Regulations: Privacy, Security and Electronic Data Interchange

employers are acting as a health plan or health care provider, they are required to comply with these standards.)

- **Covered Electronic Transactions.** The following transactions are governed by these regulations: health care claims or equivalent encounter information, health care payment and remittance advice, coordination of benefits, health care claim status, enrollment and disenrollment in a health plan, eligibility for a health plan, health plan premium payments, and referral certification and authorization.
- **Standardized Electronic Transaction Guidelines.** The regulations require that all Covered Entities a) use the same "code sets" and b) transmit the data in the same format. A code set is any set of codes used for encoding data elements, such as medical diagnosis codes or medical procedure codes.
- **Purpose.** The regulations are intended to streamline electronic health care transactions by insuring that insurance carriers, third party administrators, and health insurance providers keep and exchange information in a uniform format. While the initial implementation costs are significant, it is expected that use of uniform standards will produce cost savings.

Please contact your Scott Benefit Services representative with any questions or to receive further information on other areas regulated by HIPAA.

This Scott Benefit Services Legislative Brief is not intended to be exhaustive nor should any discussion or opinions be construed as legal advice. Readers should contact legal counsel for legal advice.

Content copyright © 2000-2009 Zywave, Inc. Images copyright © 2000-2004 Getty Images, Inc. All rights reserved.

Rev. EAM 5/09



The HIPAA Privacy Rules: Three Types of Information

	Protected Health Information (PHI)	Summary Health Information (SHI)	De-Identified Information
Definition	Personally Identifiable + Health Information + Created or received by a Covered Entity + Relates to past, present or future conditions, treatment or Payment for health care	May be individually identifiable health information + Summarizes claims history, claims expenses, or types of claims experienced by individuals for whom a plan sponsor has provided health benefits under a group health plan + 18 identifiers ⁱ deleted, but may include 5 digit zip code	Health information + Does not identify an individual + No reasonable basis to believe information can be used to identify and individual + Can use Statistical Method ⁱⁱ or Safe Harbor Method ⁱⁱⁱ
Example	Medical records in the possession of the physician	DMW Reports ^{iv}	High cost claimant report that does not identify individual
Purpose	May use PHI for treatment, payment, or health care operations, or other uses permitted by HIPAA. Must apply minimum necessary standard.	Employer may use SHI for (1) obtaining premium bids for providing health insurance coverage under the group health plan or (2) modifying, amending, or terminating the group health plan.	De-identified information is NOT regulated by the Privacy Rules.

i

- (1) Name
- (2) All geographic subdivisions smaller than state
- (3) All elements of dates (except year) related directly to individual (birth date, admission date, discharge date, date of death) and ages over 89 unless aggregated into single category of 90 and older
- (4) Telephone numbers
- (5) Fax numbers

- (6) Electronic mail addresses
- (7) Social security numbers
- (8) Medical record numbers
- (9) Health plan beneficiary numbers
- (10) Account numbers
- (11) Certificate/license numbers
- (12) Vehicle identifiers and serial numbers, including license plate numbers

- (13) Device identifiers and serial numbers
- (14) Web universal resource locators (URLs)
- (15) Internet protocol (IP) address numbers
- (16) Biometric identifiers, including finger and voice prints
- (17) Full face photographic images and any comparable images
- (18) Any other unique identifying number, characteristic or code

ⁱⁱ A person with appropriate knowledge and experience applying generally applicable statistical and scientific principles and methods for rendering information not individually identifiable makes a determination that the risk is very small that the information could be used, either by itself or in combination with other available information, by anticipated recipients to identify the subject of the information. The Covered Entity must also document the analysis and results that justify the determination.

ⁱⁱⁱ PHI has 18 identifiers removed and Covered Entity has no actual knowledge that the information could be used alone or in conjunction with other information to identify an individual who is a subject of the information.

^{iv} SHI may not constitute de-identified information because there may be a reasonable basis to believe that the information is identifiable to the plan sponsor, especially for plans with few participants. Preamble to December 2000 Regulations, 65 Fed. Reg. 82461; 82647.

Legislative Brief

HIPAA Administrative Simplification: *Guidance and Compliance Dates*



In August 1996, President Clinton signed into law the Health Insurance Portability and Accountability Act of 1996 (HIPAA). HIPAA is a broad federal law with provisions related to pre-existing conditions and guaranteeing issuance of insurance coverage (Portability Rules), and prohibiting discrimination by a health plan based upon an individual's health status (Nondiscrimination Rules).

HIPAA also includes administrative simplification provisions. Specifically, these provisions address a) uniform standards for electronic health care transactions (Electronic Data Interchange (EDI) Rules) and b) privacy and security of personally identifiable health information (Privacy and Security Rules) that apply to health care providers, health plans and healthcare clearinghouses (Covered Entities).

This issue of the Scott Benefit Services Legislative Brief outlines the guidance that has been issued by regulatory agencies with respect to the EDI, Privacy and Security Rules, as well as the initial compliance dates associated with these rules.

Legislative Guidance

EDI Rules

- On August 17, 2000, the U.S. Department of Health and Human Services (HHS) released final regulations designed to standardize electronic transactions conducted within the health care industry. The regulations require Covered Entities that conduct certain transactions electronically, such as health care claims and payments and health plan enrollment, to use standardized formats, content and uniform code sets that are specified in the regulations.
- In December 2001, President Bush signed into law the Administrative Simplification Compliance Act of 2001, which allowed Covered Entities to request an additional year to comply with the EDI standards.
- On February 20, 2003, HHS published modifications to the final regulations, which made changes to certain code sets and transactions.
- On January 16, 2009, HHS published final regulations to update the EDI standards and code sets. The EDI standard provisions are effective **January 1, 2012**. However, until then, Covered Entities may use either the older or updated standards. The effective date for the code set provisions is **October 1, 2013**.
- In July 2003, the Centers for Medicare and Medicaid Services (CMS) issued guidance on enforcement of the EDI Rules. The guidance recognized that Covered Entities may encounter compliance hurdles when dealing with noncompliant Covered Entities and stated that CMS would not impose penalties on otherwise compliant Covered Entities if they deployed contingencies to promote the smooth flow of payments and made a reasonable and diligent effort to comply with the rules.

Privacy Rule

- On December 28, 2000, HHS released final regulations governing the privacy of medical records (the Privacy Rule). The Privacy Rule set out guidelines for the use and disclosure of health information by Covered Entities and established rights for individuals with respect to their own information.
- In August 2002, final modifications to the Privacy rule were published by HHS.

Legislative Brief

HIPAA Administrative Simplification: *Guidance and Compliance Dates*

Security Rule

- The HIPAA statute required Covered Entities that conduct electronic transactions to maintain reasonable and appropriate safeguards to protect the integrity, confidentiality and security of health information and to ensure compliance by their officers and employees.
- On February 20, 2003, HHS published final regulations regarding the security of health information (the Security Rule). The Security Rule established standards and implementation specifications for Covered Entities that transmit or maintain electronic health information to ensure that the confidentiality, integrity and availability of the health information are maintained.

When were health plans initially required to comply with these rules?

EDI Rules

Health plans were required to comply with the EDI Rules no later than October 16, 2002, but were permitted to file for a one-year extension. Small health plans had to comply by October 16, 2003.

Privacy Rule

Health plans were required to comply with the Privacy Rule no later than April 14, 2003. Small health plans had an additional year to comply.

Security Rule

Health plans were required to comply with the Security Rule no later than April 20, 2005. Small health plans had an additional year to comply.

What is a small health plan?

HHS defines a small health plan as a health plan with annual receipts of \$5 million or less. HHS later clarified that, for purposes of determining whether a health plan is a small health plan, they consider pure premiums to be equivalent to annual receipts. In September 2002, CMS released additional clarification on how group health plans may calculate annual receipts. CMS's most recent guidance explains that for purposes of determining whether a health plan has annual receipts of \$5 million or less:

- Fully-insured group health plans should use the amount of total premiums which they paid for health insurance benefits during the plan's last full fiscal year.
- Self-funded group health plans should use the total amount paid for health care claims by the employer, plan sponsor, or benefit fund, as applicable to their circumstances, on behalf of the plan during the plan's last full fiscal year.
- Plans that provide health benefits through a mix of fully-insured and self-funded arrangements should combine total premiums and health care claims paid to determine their annual receipts.

This Scott Benefit Services Legislative Brief is not intended to be exhaustive nor should any discussion or opinions be construed as legal advice. Readers should contact legal counsel for legal advice.

Content copyright © 2002, 2009 Zywave, Inc. Images copyright © 2000-2004 Getty Images, Inc. All rights reserved.

Legislative Brief

HIPAA Administrative Simplification: *Guidance and Compliance Dates*

Compliance Date Chart

Covered Entity	HIPAA Regulations – Effective Dates		
	EDI Rules	Privacy Rule	Security Rule
Small Health Plans	October 16, 2003	April 14, 2004	April 20, 2006
Health Plans	October 16, 2002 A one year extension was permitted for plans that filed prior to 10/15/02.	April 14, 2003	April 20, 2005

Please contact your Scott Benefit Services representative with any questions regarding HIPAA Administrative Simplification or any other HIPAA-related issue.

10/02, EAS 6/09

Legislative Brief

HIPAA: Important Dates and Deadlines



There are a number of HIPAA regulatory compliance deadlines of which health plans should be aware. This issue of the Scott Benefit Services Legislative Brief summarizes some topical compliance dates.

HIPAA Portability Rules – Special Enrollment Changes

HIPAA requires group health plans to provide special enrollment rights to certain individuals who lose eligibility for other health coverage or who acquire a new spouse or dependent. The **Children's Health Insurance Program Reauthorization Act of 2009** extended these special enrollment rights to employees and dependents who lose eligibility under a Medicaid plan or State Children's Health Insurance Program (CHIP) and employees and dependents who become eligible for a premium assistance subsidy under Medicaid or CHIP. Eligible individuals must be given 60 days after the loss of coverage or determination of eligibility for assistance to request coverage under the group health plan.

If necessary, group health plan documents must be amended to provide the new special enrollment rights. Appropriate notices of the amendment, such as a Summary of Material Modifications, should be provided to participants in accordance with the plan's existing procedures for providing such notices. Existing special enrollment notices provided to new enrollees should also be revised to contain information regarding the new provisions.

The effective date for these new special enrollment rights was **April 1, 2009**. If they have not yet done so, group health plans should review their plan documents and notices for compliance.

HIPAA Privacy Rule – Notice of Privacy Practices

The HIPAA Privacy Rule requires health plans to provide a **Notice of Privacy Practices** to all enrollees, or to remind them of its availability and how to obtain a copy, every three years. Health plans may satisfy this requirement by sending a Notice of Privacy Practices or reminder to all participants or by publishing the information in a newsletter or other plan publication. The notice should be updated to incorporate any material changes in a health plan's privacy policies or procedures.

Health plans that previously sent a notice by April 14, 2006 had until April 14, 2009 to send a new notice or reminder. They should send the next notice or reminder by **April 14, 2012**. Small health plans, which were required to send a notice by April 14, 2007, have until **April 14, 2010** to send the next notice or reminder.

Health plans should also be aware that the Notice of Privacy Practices must be provided in the following circumstances:

- To new enrollees at the time of enrollment;

Legislative Brief

HIPAA: Important Dates and Deadlines

- Within 60 days of a material change to the notice; and
- Any time upon a participant's request.

HIPAA Privacy and Security Rules – Application to Business Associates

Under current law, Business Associates are not directly regulated by HIPAA. Instead, they are governed by the terms of the Business Associate Agreement that a Covered Entity, such as a health plan, must obtain before providing Protected Health Information (PHI) to the Business Associate. The American Recovery and Reinvestment Act of 2009 ("ARRA") has expanded the application of the privacy provisions reflected in the agreements and the security requirements to Business Associates. This change is effective **February 17, 2010** and will require changes to existing Business Associate Agreements.

Please contact your Scott Benefit Services representative with any questions.

This Scott Benefit Services Legislative Brief is not intended to be exhaustive nor should any discussion or opinions be construed as legal advice. Readers should contact legal counsel for legal advice.

Content copyright © 2000-2009 Zywave, Inc. Images copyright © 2000-2004 Getty Images, Inc. All rights reserved.

EAM 5/09

Legislative Brief

Changes to HIPAA Rules: American Recovery and Reinvestment Act of 2009



On February 17, 2009, President Obama signed into law the American Recovery and Reinvestment Act of 2009 ("ARRA"). In addition to provisions designed to stimulate the economy, ARRA contains the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act" or the "Act"). The HITECH Act contains health information technology provisions and also makes significant changes to the privacy and security requirements of the Health Insurance Portability and Accountability Act of 1996 (the "HIPAA Privacy and Security Rules"). The general effective date of the HITECH Act is **February 17, 2010**, but many provisions have varying effective dates and must be reviewed carefully.

This issue of the Scott Benefit Services Legislative Brief provides you with an overview of the changes to the HIPAA Privacy and Security Rules imposed by the HITECH Act.

Business Associates

The HIPAA Privacy and Security Rules currently apply to Covered Entities: health plans, health care providers and health care clearinghouses. Under current law, a Covered Entity's Business Associates must agree, through a Business Associate Agreement, to comply with certain requirements of the HIPAA Privacy and Security Rules, but are not directly regulated by the regulations. The HITECH Act makes a number of these requirements directly applicable to Business Associates. In addition, penalties for violations of the Privacy and Security Rules that formerly applied only to Covered Entities will now apply to Business Associates as well.

Business Associates will now be required to comply directly with many provisions of the HIPAA Privacy Rules that currently apply to Covered Entities. The obligations that were previously required to be included in the Business Associate Agreement, such as using Protected Health Information ("PHI") only for permitted purposes and using appropriate safeguards, are now directly applicable to Business Associates. In addition, Business Associates that become aware of breaches of the Privacy Rule by a Covered Entity are required to take steps to cure the breach. If they are unsuccessful, they must terminate the agreement or notify the Secretary of Health and Human Services ("HHS"). This responsibility must be included in the Business Associate Agreement.

Business Associates must also comply with the HIPAA Security Rules. The additional obligations must be incorporated into the Business Associate Agreement between the Covered Entity and Business Associate. The Act also provides that, each year, HHS must issue guidance on the most effective and appropriate technical safeguards for use in compliance with the HIPAA Security Rule.

The HITECH Act also expands the definition of Business Associate to include organizations that provide data transmissions of PHI to a Covered Entity (or its Business Associate) and require access on a routine basis to such PHI, as well as vendors that contract with Covered Entities to offer a Personal Health Record to patients. These Business Associates must enter into Business Associate Agreements with the Covered Entities.

The new requirements for Business Associates are effective on **February 17, 2010**.

Security Breach Notification

Covered Entities do not currently have a specific obligation to report breaches of privacy or security of PHI. The HITECH Act will require Covered Entities to notify individuals whose "unsecured PHI" has been breached. If the breach involves PHI held by a Business Associate, the Business Associate must notify the Covered Entity.

Legislative Brief

Changes to HIPAA Rules: American Recovery and Reinvestment Act of 2009

The notification must be made without unreasonable delay and no later than 60 days after the discovery of the breach. Generally, the notification must be provided by first class mail but can also be provided by e-mail, if the individual has specified a preference to receive notices electronically. The Covered Entity must also provide notice to “prominent media outlets” if the breach affects more than 500 individuals in a state or jurisdiction. Covered Entities must notify HHS of all breaches. Notice must be provided immediately for breaches involving more than 500 individuals and annually for all other breaches. HHS will post breaches involving more than 500 individuals on its website (www.hhs.gov).

The Act requires the notice to include the following information:

- A description of the breach, including the date of the breach and date of discovery;
- The type of PHI involved (such as full name, Social Security number, date of birth, home address or account number);
- Steps individuals should take to protect themselves from potential harm resulting from the breach;
- Steps the Covered Entity is taking to investigate the breach, mitigate losses and protect against future breaches; and
- Contact procedures for individuals to ask questions or learn additional information, including a toll-free telephone number, e-mail address, website or postal address.

The Act does not specify when PHI is considered to be “secure” but directs HHS to issue guidance regarding which technologies are considered secure within 60 days of the Act’s enactment. In the event timely guidance is not issued, “unsecured PHI” will mean PHI that is not secured by a technology standard that renders PHI unusable, unreadable or indecipherable to unauthorized individuals. HHS is also required to issue interim final regulations governing the notification requirement within 180 days of enactment. The notification requirement will apply to breaches discovered on or after the date that is **30 days after the regulations are issued**.

The Act also imposes a temporary breach notification requirement on vendors of personal health records (“PHR”) and other non-HIPAA Covered Entities. PHR vendors must notify any individual who is a citizen or resident of the United States whose unsecured PHR identifiable health information was acquired by an unauthorized person as a result of a breach of security. PHR vendors must also notify the Federal Trade Commission (“FTC”), which will in turn notify HHS. Any third party service provider that provides services to a PHR vendor and discovers a breach, must notify the vendor. Violations of this requirement will be treated as unfair and deceptive acts or practices in violation of the Federal Trade Commission Act. The FTC is required to issue interim final regulations regarding this requirement within 6 months of enactment and the requirement will be effective **30 days after the regulations are issued**.

Individual Rights

Accounting for Disclosures

The HIPAA Privacy Rule requires a Covered Entity to provide an individual with an accounting of disclosures of PHI upon request, but permits routine disclosures for treatment, payment or health care operations to be excluded from the accounting. The new law extends HIPAA’s requirement to provide that, if a Covered Entity maintains an “electronic health record” for an individual, the Covered Entity must account for disclosures through the electronic

Legislative Brief

Changes to HIPAA Rules: American Recovery and Reinvestment Act of 2009

health record for treatment, payment or health care operations as well. This additional disclosure accounting is limited to a period of three years prior to the request.

An electronic health record is defined as an electronic record of health-related information on an individual that is created, gathered, managed or consulted by authorized health care clinicians and staff.

The effective date for this provision depends on when the electronic health record is held by the Covered Entity and appears to give current users of electronic health records additional time to update their systems. For electronic health records held by a Covered Entity as of January 1, 2009, the disclosure accounting requirement would apply to disclosures on or after **January 1, 2014**. For electronic health records held after January 1, 2009, the requirements apply on or after **January 1, 2011**, or the date the electronic health record is acquired, whichever is later. However, these dates may be delayed to 2016 and 2013 respectively.

Access to Electronic Health Records

In addition to being able to access PHI held by a Covered Entity as required by the HIPAA Privacy Rule, an individual is permitted under the HITECH Act to access PHI in an electronic health record in electronic form. The Covered Entity may charge the individual for the cost of labor for providing access. An individual may also direct the Covered Entity to transmit the electronic health record directly to another person or entity. This provision is effective on **February 17, 2010**.

Right to Restrict Disclosures

Under current law, an individual may request that a Covered Entity not disclose the individual's PHI, even if the disclosure would be for treatment, payment or health care operations. However, the Covered Entity is not required to agree to the restrictions. The HITECH Act will require Covered Entities to agree to an individual's request to restrict disclosures to a health plan for payment or health care operations if the PHI pertains to services or treatment that have been paid out of pocket and in full. This provision is effective on **February 17, 2010**.

Restrictions on Disclosure

The HITECH Act contains several new restrictions on the disclosure of PHI.

Prohibition on Sale of Protected Health Information

Under the Act, Covered Entities and Business Associates may not receive remuneration for the disclosure of PHI without the individual's authorization. There are limited exceptions for disclosures for public health, treatment or research purposes. Payment for research purposes is limited to the cost of preparing and transmitting the data. HHS is required to issue regulations implementing these new restrictions within 18 months. The new rule will become effective **six months after the regulations are issued**.

Marketing Restrictions

Certain marketing communications that were permissible under the HIPAA Privacy and Security Rules are no longer permitted under the HITECH Act. Pursuant to the new rule, Covered Entities and Business Associates may not use PHI to inform an individual about the Covered Entity's products or services without the individual's authorization if the Covered Entity receives compensation from another party for making the communication. This new rule does not apply in cases where the communication involves a drug the individual is already taking and where any compensation

Legislative Brief

Changes to HIPAA Rules: American Recovery and Reinvestment Act of 2009

for that communication is reasonable in amount or where the communication is made by a Business Associate on behalf of a Covered Entity and is consistent with the terms of the business associate agreement.

Minimum Necessary Standard

In general, Covered Entities are required to use or disclose the “minimum necessary” amount of PHI. Currently, there is little guidance as to what constitutes the minimum amount necessary and Covered Entities were required to make this determination on their own. The HITECH Act requires HHS to issue regulations **within 18 months of enactment** regarding the minimum necessary requirement. Until then, Covered Entities must use or disclose only a limited data set, if it is sufficient for the intended purpose. A limited data set excludes certain identifying information but is not fully de-identified.

Penalties and Enforcement

Civil Penalties

HHS may currently conduct compliance reviews to determine whether a Covered Entity is in compliance with the HIPAA Privacy and Security Rules. The Act also requires HHS to perform periodic audits of Covered Entities to ensure their compliance.

Currently, HHS may assess civil penalties of \$100 per violation of the Privacy and Security Rules, up to \$25,000 for violations of each requirement during a calendar year. The HITECH Act increases the amounts of the civil penalties that may be assessed and distinguishes between the types of violations. These penalties may not apply if the violation is corrected within 30 days of the date the person knew, or should have known, of the violation. HHS is also required to assess penalties for violations involving willful neglect and to formally investigate complaints of such violations.

For violations where the individual does not know of the violation, the minimum penalty remains \$100 per violation, up to \$25,000 per calendar year for identical violations. If the violation is due to reasonable cause, the minimum penalty is \$1,000 per violation, up to \$100,000 per calendar year. For corrected violations that are caused by willful neglect, the minimum penalty is \$10,000 per violation, up to \$250,000 per calendar year. The maximum civil penalty for any type of violation and the minimum penalty for violations caused by willful neglect that are not corrected is \$50,000 per violation, up to \$1.5 million per calendar year for identical violations.

The updated civil penalty amounts apply to violations occurring after **February 17, 2009**. Other enforcement provisions apply to penalties that are imposed **24 months after the date of enactment**. HHS is required to issue regulations governing the enforcement provisions within 18 months of enactment.

The Act requires the General Accounting Office to review methodologies for allowing a portion of civil penalties to be paid to affected individuals. HHS must establish a methodology by **February 17, 2012**.

State Attorneys General are authorized by the Act to bring civil actions against Covered Entities to enjoin further violations and obtain damages on behalf of residents of their states, if HHS has not already taken action. The amount of damages is up to \$100 per violation, with a maximum of \$25,000 per calendar year for identical violations. This provision is effective for violations occurring any time after **February 17, 2009**.

Legislative Brief

Changes to HIPAA Rules: American Recovery and Reinvestment Act of 2009

Criminal Penalties

The new law does not change the criminal penalties that may be assessed for violations of the Privacy and Security Rules. Those penalties remain \$50,000 and one year in prison for knowing violations, \$100,000 and five years in prison for violations committed under false pretenses and \$250,000 and 10 years in prison for offenses committed for commercial or personal gain.

Under the Act, criminal actions may be brought against anyone who wrongly discloses PHI, not just Covered Entities or their employees. Also, the Act gives HHS (in addition to the Department of Justice) the authority to bring criminal actions against these individuals.

Please contact your Scott Benefit Services representative with any questions.

This Scott Benefit Services Legislative Brief is not intended to be exhaustive nor should any discussion or opinions be construed as legal advice. Readers should contact legal counsel for legal advice.

Content copyright © 2009 Zywave, Inc. Images copyright © 2000-2004 Getty Images, Inc. All rights reserved.

EM 2/09

KNOW YOUR EMPLOYEE BENEFITS



Benefit and insurance issues important to you—brought to you by the insurance specialists at Scott Benefit Services.

Your Right to Privacy

HIPAA Basics

In April 2003, the final regulations that place restrictions on how personally identifiable health information may be used and disclosed by certain organizations became effective.

These regulations (the Privacy Rules) implement the privacy requirements contained within the Administrative Simplification subtitle of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

While some states have laws that protect health information, the HIPAA Privacy Rules establish a uniform, minimum level of privacy protections for all health information.

In summary, the HIPAA Privacy Rules:

- Set limits on how health information may be used and disclosed;
- Require that individuals be told how their health information will be used and disclosed;
- Provide individuals with a right to access, amend or copy their medical records;
- Give individuals a right to receive an accounting of disclosures, to request
- special restrictions, and to receive confidential communications; and

- Impose fines where the requirements contained within the regulations are not met.

Restrictions on Use & Disclosure

The rules allow health care providers, health plans, and health care clearinghouses (Covered Entities) to use and disclose your personally identifiable health information for purposes of treatment, payment, or health care operations.

For example, your health care provider may submit your health information to a health insurance company in order to seek payment for the treatment provided to you. Your primary care physician can share your health information with a specialist that he or she recommends you consult. In these cases, your written permission to disclose your health information is not required.

In general, any use or disclosure not considered treatment, payment, or a health care operation requires your written authorization, unless an exception applies. For example, your physician may not share your health information with your employer or a life insurance carrier without your written permission.

However, disclosure of health information is permitted for certain purposes specifically listed in the HIPAA Privacy Rules, such as national security, law enforcement and public health issues. If you authorize release of your health information to a third party, the information released may no longer be protected by HIPAA.

Notice of Privacy Practices

You are entitled to receive an explanation of how your personally identifiable health information will be used and disclosed.

For example, a physician or hospital is required to provide you with a Notice of Privacy Practices at your first visit. You will be required to sign an acknowledgement indicating that you received the Notice of Privacy Practices.

If you have health insurance coverage, the insurance company or health plan will also provide you with a Notice of Privacy Practices immediately after you are enrolled in the plan. It is important that you read the Notice of Privacy Practices in order to understand your rights and know who to contact if you feel your privacy rights have been violated.

Scott Benefit Services

1301 Old Graves Mill Road • Lynchburg, VA • 24502

Phone 434-832-2100 • Fax 434-832-2190 • Web site <http://www.scottins.com>

KNOW YOUR EMPLOYEE BENEFITS

Right to Access, Amend, or Copy

You have a right to view and copy your medical records. You may be charged a fee for the cost of reproduction. If you believe that information within your medical records is incorrect or if important information is missing, you have a right to request that your medical records be amended.

Right to an Accounting of Disclosure

You also have a right to a list of uses and disclosures made of your medical records where the use or disclosure was not for purposes of treatment, payment, health care operations, or pursuant to your written authorization.

Right to Request Restrictions

You may request in writing that a health care provider or health plan not use or disclose information for treatment, payment, or other administrative purposes unless specifically authorized by you, when required by law, or in emergency circumstances. Health care providers and health plans must consider your request, but are not legally obligated to agree to those restrictions.

Confidential Communications

You have a right to receive confidential communications containing your health information. Health care providers and health plans are required to accommodate your reasonable requests. For example, you may ask that a physician contact you at your place of employment or send communications regarding treatment to an alternate address.

Violations of Privacy Rights

If you believe that your privacy rights have been violated, you may contact the Privacy Officer for the organization that you feel

has violated your right to privacy. The name of the Privacy Officer should be included in the Notice of Privacy Practices provided to you by that organization.

If the Privacy Officer does not adequately resolve your concerns, you may contact the Department of Health and Human Services — Office of Civil Rights (OCR). OCR is responsible for enforcing the HIPAA Privacy Rules. Its Web site contains instructions on how to file a complaint <http://www.hhs.gov/ocr/privacyhowtofile.htm>, and a complaint form <http://www.hhs.gov/ocr/howtofile/privacy.pdf>.

Penalties for Noncompliance

The HIPAA Privacy Rules do not provide individuals with a private right to sue, although methodologies for allowing a portion of civil penalties to be paid to affected individuals must be established by February 17, 2012.

Currently, health care providers, health plans, and health care clearinghouses that do not comply with the HIPAA Privacy Rules may be subject to civil money penalties ranging from \$100 to \$50,000 per violation, with maximum penalties ranging from \$25,000 per year to \$1.5 million per year.

Criminal violations of the HIPAA Privacy Rules may also be referred to the Department of Justice for enforcement. Criminal penalties for such violations include:

- \$50,000 and/or up to one year in prison for knowingly obtaining or disclosing protected health information not permitted by law;
- \$100,000 and/or up to five years in prison for obtaining or disclosing protected health information under false pretences; and

- \$250,000 and/or up to ten years in prison for obtaining protected health information with an intent to sell, transfer, or use it for commercial advantage, personal gain, or malicious harm.

State Attorneys General (AG) may also bring suit against Covered Entities to enjoin further violations and obtain damages on behalf of residents of their states, if HHS has not already taken action. The AG may seek damages of up to \$100 per violation, with a maximum of \$25,000 per year for identical violations.

HIPAA Privacy Resources

- Office of Civil Rights (HHS) <http://www.hhs.gov/ocr/>
- Health Privacy Project <http://www.healthprivacy.org>

This brochure is for informational purposes only and is not intended to replace the advice of an insurance professional or legal counsel. Please seek professional advice before making decisions about your personal finances or legal rights.

This brochure is intended to provide an objective, reader-friendly summary of the rights afforded to individuals by the HIPAA Privacy Rules. This information may be used to supplement the Notice of Privacy Practices required by HIPAA. In no event should this article be used in place of any legal notice required by HIPAA.

Know Your Employee Benefits is written and produced for Scott Benefit Services. © Zywave, Inc.