



## PRIVACY AND CONFIDENTIALITY

A claims administrator or insurance company must respect the individual's right to privacy when obtaining information necessary to process claims. Although most organizations processing claims have developed procedures addressing the individual's right to privacy, not until recently have federal regulations been issued protecting the privacy of patient health information.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) required Congress to pass comprehensive health privacy legislation by 8/21/99. In absence of the passage of federal legislation addressing patient privacy protections, HIPAA required the Department of Health and Human Services (HHS) to issue final privacy regulations within 42 months or by 2/21/00. As Congress did not enact privacy regulations, on 10/29/99, HHS issued proposed regulations. The proposed regulations were to become effective 2/21/02.

On 12/29/00, final regulations developed by HHS were published. These regulations were to become effective 2/26/01 and affected entities had two years to comply (2/26/03). Small health plans (small health plans are defined as those with less than 50 employees and less than \$5 million in revenue) did not have to come into compliance until 2/26/04. However, HHS failed to deliver the regulation to the General Accounting Office within the time required by the Congressional Review Act. As a result, the regulation had to be resent and the effective date was pushed back to 4/14/01. As required by HIPAA, covered entities had until 4/14/03 to comply with the final rule. Small health plans had until 4/14/04 to comply.

On 7/6/01, HHS issued its first set of guidance to answer commonly asked questions and to provide clarification about the final rule's provisions. Proposed changes to the final rule were published in the 3/27/02 Federal Register. On 8/9/02 HHS issued the final privacy regulation which was published in the 8/14/02 Federal Register.

The "Standards for Privacy of Individually Identifiable Health Information - Final Rules," (Privacy Rule) in its current format, are summarized in this topic.

### **Definitions**

**Business Associates** - By law, the Privacy Rule only applies to health plans, health care clearinghouses and certain health care providers. However, most of these entities do not perform all of its health care activities by themselves. These entities require assistance from a variety of other associates and businesses. A business associate helps a covered entity with a function or activity which involves the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice



**Trilogy Claims Administrative Handbook**  
**Section 4 - Benefits Legislation**  
**Privacy And Confidentiality (4.15)**

management and repricing, legal, actuarial, accounting, consulting, data aggregation management, administrative, accreditation or financial services.

Covered Entities - As required by HIPAA, “covered entities” include health plans, health care clearinghouses and health care providers who conduct certain financial and administrative transactions electronically.

Health Care Clearinghouses - Public or private entity that processes or facilitates the processing of nonstandard data elements of health information into standard elements.

Health Care Operations - Defined by the rule as quality assessment and improvement, training and evaluation including accreditation and similar activities, underwriting and premium rating relating to insurance and reinsurance, conducting and arranging for medical review, legal services and auditing including fraud and abuse detection, business planning and management and customer service.

Health Plan - A health plan is defined as an individual or group plan, self-funded or insured, private or public, with 50 or more members, administered by an entity other than the employer that establishes and maintains the plan. The definition includes church plans, health insurers and HMOs.

Individually Identifiable Information - Health related information created or received by a covered entity relating to an individual’s past, present or future health or health condition which identifies the individual or involves a reasonable basis to identify an individual.

Personal Health Information (PHI)- covered by the Privacy Rule includes all medical records and individually identifiable health information used or disclosed by a covered entity in any form, whether electronically, written or orally.

### **Responsibilities of Covered Entities**

Covered entities are bound by the regulation even if they contract with others, called “business associates,” to perform some essential functions. The law does not give HHS the authority to regulate private business such as life insurance companies, employers or public agencies which deliver social security or welfare benefits.

Covered entities are required to:

- adopt and implement written procedures;
- train employees in privacy policies and procedures;
- designate an officer to ensure procedures are followed; and
- provide a notice of privacy procedures and policies to affected individuals.



If a covered entity retains a TPA to perform plan administrative functions, the entity can also contract out to the TPA the responsibility to develop and follow HIPAA compliant privacy procedures.

To allow covered entities to give PHI to business associates, the Privacy Rule requires covered entities, typically by contract, to obtain assurances that the business associate will only use the information for the purposes for which they were engaged by the covered entity. PHI may be disclosed to a business associate only to help providers and plans carry out their health care functions - not for independent use by the associate.

A covered entity is not liable for the privacy violations of a business associate and is not required to actively monitor and oversee the means by which a business associate abides by the requirements of the contract. If the covered entity becomes aware of a pattern or practice of the business associate which constitutes a material breach of the business associate's obligation under the contract, the covered entity must take reasonable steps to end the violation. If such steps are not successful, the covered entity must terminate the contract, if feasible. If termination of the contract is not feasible, the covered entity must report the problem to HHS.

HHS posts the answers to frequently asked questions related to "Business Associates" on the Internet:

<http://www.hhs.gov/hipaafaq/providers/business/index.html>

### **Payment**

As required by the Privacy Rule, a covered entity may use and disclose PHI for payment purposes.

Payment is a defined term which encompasses the various activities of health care providers to obtain payment or to be reimbursed for their services, and for health care plans to obtain premiums, fulfill their coverage obligations and provide benefits under the plan.

Common payment activities include but are not limited to:

- determining eligibility under the plan and adjudicating claims;
- risk adjustments;
- billing and collection activities;
- reviewing health care services for medical necessity, coverage, justification of charges;
- utilization review activities; and
- disclosures to consumer reporting agencies (limited to information about an



**Trilogy Claims Administrative Handbook**  
**Section 4 - Benefits Legislation**  
**Privacy And Confidentiality (4.15)**

individual's payment history and to identify the individual).

### **Consent**

The Privacy Rule originally required that most health care providers obtain written consent before using or disclosing a patient's personal health information (PHI) to carry out treatment, payment or health care operations (TPO). However, this requirement was eliminated in 2002 due to concerns about its potential impact on the delivery of care. In lieu of the consent requirement, the notification requirement for providers was expanded.

### **Authorization**

An authorization is a more customized document than a consent which gives covered entities permission to use specified PHI for specified purposes other than TPO.

An authorization should be detailed and specific but must be written in "plain" language. An authorization must include the following:

- the specific information to be disclosed;
- the name of the person authorized to make the authorization;
- the name of the person or organization to whom the covered entity is authorized to make the disclosure;
- an expiration date;
- a statement to the individual regarding the right to revoke an authorization; and
- a statement advising the individual that the PHI being disclosed may no longer be protected under the regulation.

The authorization must be signed and dated by the individual or the individual's representative. If it is signed by the individual's representative, there must be documentation provided regarding the representative's authority to act for the individual.

An authorization is required for disclosure of PHI maintained in psychotherapy notes for treatment by persons other than the originator of the notes, for payment or for health care operations.

HHS posts the answers to frequently asked questions related to "Authorization Use & Disclosure" on the Internet:

<http://www.hhs.gov/hipaafaq/use/index.html>



**Cross Reference:**

**Section 4.16, Authorization to Release Information**

**Minimum Necessary**

The Privacy Rule requires covered entities to take reasonable steps to limit the use and disclosure of PHI to the minimum necessary to accomplish the intended purpose. Group health plans must develop policies and procedures for applying the minimum necessary standard.

The minimum necessary provisions do not apply to:

- Disclosures by health care providers for treatment purposes;
- Disclosures to individuals who are the subject of the information;
- Uses or disclosures pursuant to an authorization;
- Uses or disclosures for compliance with HIPAA;
- Disclosures to HHS of information required for enforcement purposes; and
- Uses and disclosures required by other laws.

The Privacy Rule permits the covered entity to rely on the judgement of the party requesting the information as to the minimum amount required. This type of reliance is permitted when requests are made by:

- A public official or agency;
- Another covered entity;
- A professional who is a workforce member or business associate of the covered entity holding the information; and
- A researcher with appropriate documentation from an Institutional Review Board.

The Privacy Rule allows covered entities flexibility in determining what PHI is necessary for a particular purpose. There is not a strict standard but rather a reasonableness standard consistent with guidelines currently used by providers to limit the unnecessary sharing of information.

HHS posts the answers to frequently asked questions related to “Limited Use & Disclosure” on the Internet:

<http://www.hhs.gov/hipaafaq/limited/index.html>



### **Patient Rights**

Patients have rights which include the following:

- Providers and health plans are required to provide patients with a notice providing clear written explanation of how they use, keep and disclose their health information.
- Patients must be able to review and get copies of their records, and request amendments. A history of any non-routine disclosures of medical information must be made accessible to patients.
- Patients must provide authorization for non-routine disclosures and most non-health care purposes.
- Providers and health plans cannot generally condition treatment on a patient's agreement to disclose health information for non-routine purposes.
- Patients may request use and disclosure of PHI be restricted.
- Patients have the right to complain to the covered provider, the health plan and the HHS about privacy violations or the privacy policies and procedures of a covered entity.

### **Proposed and Final Modifications**

On 3/27/02, HHS issued proposed modifications to the Privacy Rule to correct any unintended negative effects of the rule on health care quality or access to health care. These proposed changes were published in the 3/27/02 Federal Register.

On 8/9/02, the final modifications to HIPAA's privacy rules were issued by HHS. The final rules were published in the 8/14/02 Federal Register and largely left intact the proposed changes.

The new HHS proposed and final rules left intact the compliance date of 4/14/03. However, the requirement that covered entities have contracts with business associates to ensure they follow the privacy rules was extended for an additional year, until 4/14/04.

The highlights of the proposed and final changes are summarized below. Changes to the proposed regulations addressed in the 8/9/02 final modifications are indicated in italics.

**Consent and Notice** - The proposed regulations would promote access to care by removing the consent requirements that would potentially interfere with the efficient delivery of health



care, while strengthening requirements for providers to notify patients of their privacy rights and practices. Concerns had been raised that the consent requirements in the current rule interfered with pharmacists filling prescriptions, referrals to specialists and hospitals, providing treatment over the telephone and emergency situations. Under the proposed rules patients would be asked to acknowledge receipt of the notice of privacy rights and practices. This change would give the patient an opportunity to consider a provider's privacy policies before making health care decisions, while eliminating barriers that could delay or block the patient's access to care. This proposed change to consent only applies to uses and disclosures for TPO purposes. Patient authorizations would still be required for uses and disclosures for non-TPO purposes.

In the final rule, HHS makes optional the obtaining of consent to use and disclose PHI for treatment, payment, or health care operations on the part of all covered entities, including providers with direct treatment relationships. Under the rule, covered health care providers would be required to make a good faith effort to obtain an individual's acknowledgment of receipt of the provider's notice of privacy practices. The rules require certain elements be included in the notice. Health plans would not be required to obtain this acknowledgment. The rule requires covered entities to provide patients with notice of privacy rights and the privacy practices of the covered entity.

**Minimum Necessary and Oral Communications** - This provision requires covered entities to make reasonable efforts to limit the use and disclosure of and request for protected health information to the minimum necessary to accomplish the intended purpose. The proposed rules would retain both the oral communication and minimum necessary requirements, but it would make clear that a doctor could discuss a patient's treatment with other doctors and professionals involved in the patient's care without fear of violating the rule if they are overheard.

The final rule clarified that the minimum necessary standard was not intended to impede disclosures necessary to comply with laws relating to workers compensation programs. The final rule exempted from the minimum necessary standards any uses or disclosures for which the covered entity had already received an authorization.

**Business Associates** - The current rule required covered entities to have contracts with their business associates to ensure the business associates protect the privacy of the information. The proposed changes included model business associate contract provisions, to make it easier and less costly for covered entities to implement the requirements. The changes also would give covered entities (except for small health plans) up to an additional year to change existing contracts, easing the burden of renegotiating the contracts all at once.

The final rule retained the business associate contract provision but gave covered entities



**Trilogy Claims Administrative Handbook**  
**Section 4 - Benefits Legislation**  
**Privacy And Confidentiality (4.15)**

(except for small health plans) up to an additional year beyond the April 14, 2003 compliance date to change existing written vendor and service requirements. HHS also provided sample business associate contract provisions.

A model Business Associate Contract is available on the Internet:

<http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html> (go to Covered Entities/Sample Business Associate Contract)

**Marketing** - Based on consumer concerns that the marketing provisions in the current rule did not protect individual privacy, the proposed changes would explicitly require covered entities to first obtain the individual's specific authorization before sending them any marketing materials. At the same time, the proposed rules would permit doctors and other covered entities to communicate freely with patients regarding treatment options and other health related information, including disease management programs.

The final rule clarified that it is not considered marketing for a covered entity to communicate with its own patients about health related products and services. The marketing definition excludes communications for the individual's treatment and for case management, care coordination or the recommendation of alternative therapies.

**Parents and Minors** - The initial rule may have unintentionally limited a parent's access to their child's medical records. The proposed and final rules clarify that state law governs disclosures to parents. In cases where state law is silent or unclear, the revisions would preserve state law and professional practice by permitting a health care provider to use discretion to provide or deny a parent access to such records as long as that decision is consistent with state or other law.

The final rule clarified that the intent of the rule is to defer to state or other applicable law and to remain neutral to the extent possible. The final rule makes clear that nothing in the regulation prohibits disclosure of health information to a parent if, and to the extent that, state or other law permits or requires such disclosure. If a state or other law prohibits the disclosure of protected health information about a minor to a parent, so does the privacy rule.

In a 2005 legal case, the New Hampshire Supreme Court ruled that HIPAA rules do not guarantee parents access to their children's PHI if a state court determines they are not seeking it on the child's behalf. The case, In re Berg, 2005 confirmed HIPAA deference to state law. This case involved divorce and custody issues and access to psychotherapy medical records. State privacy protections apply to both parents (custodial and non-custodial) and may protect a minor's privacy relating to conditions such as pregnancy, abortion, HIV and substance abuse.



Claims administrators need to implement procedures to ensure compliance with state privacy protection laws. For example, an explanation of benefits form (EOB) may need to be revised to ensure that certain procedures are not detailed on the EOB when a state law protects the minor's medical information.

HHS posts the answers to frequently asked questions related to "Personal Representatives and Minors" on the Internet:

<http://www.hhs.gov/hipaafaq/personal/index.html>

**Uses and Disclosures for Research Purposes** - The proposed changes would eliminate the need for researchers to use multiple consent forms - one for informed consent to the research and one or more related to information privacy rights. Instead researchers could use a single combined form to accomplish both purposes. HHS also sought comments on establishing a limited data set that does not include directly identifiable information but in which certain identifiers remain.

The final rule permits the creation and dissemination of a limited data set (that does not include directly identifiable information) for research, public health, and health care operations. However, the entity and the recipient must enter into a data use agreement, in which the recipient would agree to:

- limit the use of the data set to the purposes for which it was given,
- ensure the security of the data,
- keep the identity of the information confidential, and
- avoid using the information to contact any individual.

Additional information on the interaction of the Privacy Rule and HIPAA is available on the Internet:

<http://privacyruleandresearch.nih.gov/>

**Uses and Disclosures for Which Authorizations Are Required** - The proposed changes would allow the use of a single type of authorization form to get a patient's permission for a specific use or disclosure that otherwise would not be permitted under the Privacy Rule. Patient's would still need to grant permission in advance for each type of use or disclosure, but the proposed rule would eliminate the need for covered entities to use different types of forms to obtain that advance permission.

The final rule adopted the proposed modifications. That is, authorizations for use or disclosure of psychotherapy notes may be combined only with another authorization for the use or disclosure of psychotherapy notes. Other authorizations may be combined, unless a



**Trilogy Claims Administrative Handbook**  
**Section 4 - Benefits Legislation**  
**Privacy And Confidentiality (4.15)**

covered entity has conditioned the provision of treatment, payment, enrollment in a health plan or eligibility for benefits on one of the authorizations. A covered entity generally may not combine an authorization with any other type of document, such as a notice of privacy practices or a written voluntary consent.

Other Provisions:

**Sale of Business** - The proposed and final rule clarify that the Privacy Rule permits disclosures in certain circumstances for the sale of a covered entity's business.

**Group Health Plans** - The proposed and final rule clarify that a group health plan or health insurance issuer can disclose enrollment or dis-enrollment information to a plan sponsor without amending plan documents.

**Accounting of Disclosures of Protected Health Information** - The proposed and final rule would not require the covered entity to account for disclosures for which the individual provided written authorization.

**Disclosures for TPO of Another Entity** - The proposed and final rule clarify that covered entities can disclose protected health information for the TPO of another health care provider or another covered entity.

**Uses and Disclosures Regarding FDA Regulated Products and Activities** - The proposed and final rule assure that the rule permits covered entities to continue to disclose information to non-government entities subject to FDA jurisdiction about the quality, safety and effectiveness of FDA regulated products and activities.

**Hybrid Entity** - The proposed and final rule permits any entity that performs covered and non-covered functions to elect to use the hybrid entity provisions. The proposed and final rule clarified that protected health information does not include employment records.

**Stop Loss Insurance** - The rules recognize that stop loss insurance is included under the definition of health care operations and does not require individual authorization for PHI to be exchanged between covered entities and stop loss insurers.

**Impact on Business Associates**

Although the final privacy regulation's definition of covered entities does not include third party administrators (TPAs), TPAs as well as insurers are considered business associates and will have access to protected information as defined by the final privacy regulations. The following actions can be taken by employers and claim administrators to ensure compliance with the final privacy regulations:



- Draft and distribute an organizational privacy statement;
- Review current policies for compliance;
- Develop procedures addressing requests for medical information;
- Develop guidelines for maintaining the confidentiality of medical data;
- Draft template consents to release information for routine and non-routine purposes;
- Define the “minimum amount of information necessary” to fulfill the purpose of the disclosure;
- Ensure all external vendors are in compliance;
- Review and rewrite contracts to include privacy provisions;
- Develop an internal audit and training program to ensure compliance; and
- Designate an individual responsible for administering privacy policy and addressing any complaints regarding violation of federal privacy regulations.

If there are any questions relating to privacy and confidentiality issues, or the release of medical records outside the claim department, advice should be obtained from Legal Counsel.

Training materials are available on the HHS Web site:

<http://www.hhs.gov/ocr> (go to Health Information Privacy/HIPAA Privacy Rule/Training Materials)

### **Claims Assistance**

HHS clarified circumstances relating to when a health care plan can disclose PHI to a person who calls the plan on a beneficiary’s behalf.

HIPAA privacy rules permit a health care plan to disclose to a family member, relative or close personal friend of the individual beneficiary, PHI directly relevant to that person’s involvement with the individual’s care or payment for care. A health care plan also may make these disclosures to persons who are not family members, relatives or close personal friends of the individual, provided that the plan has reasonable assurance that the person has been identified by the beneficiary as being involved in his or her care or payment.



**Trilogy Claims Administrative Handbook**  
**Section 4 - Benefits Legislation**  
**Privacy And Confidentiality (4.15)**

Plans may disclose PHI only if it can reasonably infer that the beneficiary does not object to the disclosure. When the beneficiary is not present or is incapacitated, a plan can disclose PHI if in the exercise of professional judgement, the plan believes the disclosure is in the best interests of the individual. Examples of allowable disclosures given by HHS include:

- A health plan may disclose relevant PHI to a beneficiary's daughter who has called to assist her hospitalized, elderly mother in resolving a claim or other payment issue.
- A health plan may disclose relevant PHI to a human resources representative who has called the plan with the beneficiary also on the line, or who could turn the phone over to the beneficiary, who could then confirm for the plan that the representative calling is assisting the beneficiary.
- A health plan may disclose relevant PHI to a congressional office or staffer that has faxed to the plan a letter or e-mail it received from the beneficiary requesting intervention with respect to a health care claim, which assures the plan that the beneficiary has requested the congressional office's assistance.

A claims administrator should develop prepared scripts for Examiners or Customer Service Representatives to use when responding to oral inquiries.

### **Compliance in Disaster Situations**

HHS has published a Web-based interactive decision tool designed to assist emergency preparedness and recovery planners in determining how to access and use health information consistent with the HIPAA Privacy Rule. The tool will guide emergency preparedness and recovery planners through a series of questions regarding how the HIPAA Privacy Rule applies to a particular disclosure. The intended audiences include covered entities as well as emergency preparedness and recovery planners at the local, state and federal levels. To navigate this decision tool a series of questions must be answered to receive an answer as to whether the specific disclosure is allowed. This decision tool is available on the Internet at:

<http://www.hhs.gov/ocr/privacy> (go to Health Information Privacy/HIPAA Privacy Rule/Special Topics/Emergency Preparedness)

### **Interplay of HIPAA Privacy and Drug Treatment Confidentiality Rules**

A group health plan may indirectly be affected by additional confidentiality requirements that apply to alcohol and drug abuse treatment programs. HHS issued guidance in June 2004 addressing the interaction between the HIPAA Privacy Rule and drug treatment



confidentiality rules. HIPAA patterned its Privacy Rule on privacy rules previously issued by HHS' Substance Abuse and Mental Health Services Administration (SAMHSA). However, the SAMHSA rules are stricter in some respects and treatment programs generally must be in compliance with both rules. For example, the SAMHSA rules protect certain individual information at the time a person applies for a treatment program, even before treatment has begun. A group health plan with a utilization review program must treat this information as PHI even though it is not related to treatment, diagnosis or health care. Also, a treatment program generally must obtain an applicant's written consent to disclose any information, including information relating to the disclosure regarding application to a treatment program. SAMHSA consent requirements, unlike the HIPAA authorization requirements, do not include the exception for treatment, payment and health care operations. SAMHSA consent must include the purpose of the disclosure, as well as how much and what kind of information will be disclosed. The consent must also include an expiration date.

A group health plan needs to implement privacy procedures to ensure that PHI received from a substance abuse program is used and disclosed only as permitted by the consent form. Any requests for disclosure for non-TPO purposes should be referred to Legal Counsel.

This guidance, as well as additional information, is available on SAMHSA's Web site at:

[www.hipaa.samhsa.gov](http://www.hipaa.samhsa.gov)

### **Discovery, Subpoenas and Court Orders**

A health plan may receive a request for PHI in conjunction with a lawsuit or administrative hearing. The request may be made through a court order, subpoena, as part of the discovery process or by other means.

The Privacy Rule permits covered entities to use and disclose PHI without a written authorization in the following circumstances:

- for legal representation purposes, and
- in judicial and administrative proceedings, subject to specific procedural rules

The covered entity should always first request a legal review of state court discovery rules to determine if more stringent rules should be applied.

### **Court Order**

Disclosure due to a court order falls under the Privacy Rule exception for disclosures "required by law". If the request for PHI is accompanied by a court order or a subpoena



**Trilogy Claims Administrative Handbook**  
**Section 4 - Benefits Legislation**  
**Privacy And Confidentiality (4.15)**

from a court or administrative tribunal, the covered entity can disclose the PHI. However, only the PHI specified in the order should be disclosed.

Request From a Party Other Than a Court

If the request is not accompanied by a court order (e.g., subpoena, discovery request or other lawful process) the covered entity can release PHI if either one of the following requirements are satisfied:

- Satisfactory assurance in the form of a written statement accompanied by supporting documentation is received from the party seeking the PHI that includes:
  - the party has made a good faith effort to provide written notice to the individual;
  - the notice to the individual included sufficient information about the litigation to allow the individual to raise an objection; and
  - the time allowed for an objection has passed, or if an objection was raised, it has been resolved.
- If the request received is in the form a qualified protective order, and the parties have agreed to a prohibition from using or disclosing the PHI for any other purpose other than the proceeding for which the information was requested, as well as destruction or return of the PHI to the covered entity at the end of litigation. In this case, only the minimum necessary information to satisfy the purpose of the disclosure should be provided.

A health plan may respond to a request for PHI without a court order in the following ways:

- If the covered entity determines the requirements for disclosure have been satisfied to release PHI, the information can be released.
- If a request is received without the above described required documentation, the covered entity should advise the requestor that the information will not be released until it receives the required documentation.
- Alternatively, the covered entity can take the steps itself to make reasonable efforts to provide the notice or obtain the qualified protected order. However, the covered entity is not required to take these steps and can raise an objection to the subpoena in the court or tribunal where the litigation is pending.
- The covered entity can disclose or withhold PHI under another provision of the Privacy Rule.



Supporting documentation should be kept for a period of six years to comply with the Privacy Rule.

A health plan can disclose PHI without prior authorization, to its outside Legal Counsel without first obtaining the individual's authorization if there is a signed business associate agreement in place.

HHS posts the answers to frequently asked questions related to "Permitted Use & Disclosure" on the Internet:

<http://www.hhs.gov/hipaafaq/permitted/index.html>

### **Final Security Rules for Protected Health Information in Electronic Form**

Security rules were originally proposed in 1998 to require administrative, physical and technical safeguards for PHI in electronic form. HHS issued final security rules published in the Federal Register on 2/20/03 which include modifications designed to coordinate with the HIPAA privacy rules. The privacy rules apply to electronic, oral and paper PHI while the security rules apply only to electronic transactions. The security rules cover only information that is subject to the privacy rules and apply to internal electronic communications as well as external electronic transactions.

The final rules address standards for general rules, administrative, physical and technical safeguards, organizational requirements, policies and procedures, and documentation requirements. Covered entities must comply with the rules by 4/21/05, except for small health plans, which had until 4/21/06. Although security rule compliance did not begin until April 2005 at the earliest, electronic PHI still must be protected under the privacy rules beginning 4/14/03.

Electronic transmissions include any exchange of information in electronic media, even when the information is physically moved from one location to another on a magnetic tape, disk or CD. Also included are telephone voice response, faxback systems, HTML transactions, the Internet, extranets, leased lines, dial-up lines and private networks.

### **Cross Reference:**

**Section 4.11, HIPAA Standards for Electronic Data Interchange**

The final privacy rule provides a federal "floor" of protection. More stringent state laws, (such as those covering mental health, HIV, etc.) continue to apply.

HHS posts the answers to frequently asked questions related to "State Laws" on the



**Trilogy Claims Administrative Handbook**  
**Section 4 - Benefits Legislation**  
**Privacy And Confidentiality (4.15)**

Internet:

<http://www.hhs.gov/hipaafaq/state/index.html>

HHS published guidance for the electronic exchange of health information. The Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information can be accessed on the Internet at:

<http://healthit.hhs.gov/portal/server.pt>

### **Enforcement**

Covered entities that violate the privacy rules are subject to civil penalties of \$100 per incident, up to \$25,000 per person, per year, per standard. Covered entities which knowingly and improperly obtain or disclose information are subject to criminal penalties of up to \$50,000 and one year in prison, \$100,000 and five years in prison for obtaining protected information under “false pretenses” and up to \$250,000 and ten years in prison for obtaining or disclosing protected information with the intent to sell, transfer or use it for commercial advantage, personal gain or malicious harm.

HHS finalized its civil enforcement rules relating to HIPAA privacy and security on 2/16/06. The final rules clarify HHS’ procedures for determining violations and calculating civil monetary penalties (CMPs). The \$25,000 cap is not a limit on all CMPs, but applies to all violations of the same requirement. If more than one privacy requirement is violated, the total CMPs can be greater than \$25,000.

Generally, the rules do not apply to workers’ compensation programs. However, the “minimum amount of information necessary” standard for disclosure of protected information may affect the flow of information from providers to workers’ compensation program administrators.

The regulation will be enforced by HHS’ Office for Civil Rights. Anyone can file a complaint. The right to file a complaint is not limited to the individual whose PHI was disclosed. Additional information on how HHS enforces health information privacy rights and standards is available on the Internet at:

<http://www.hhs.gov/ocr/privacy> (go to Health Information Privacy/HIPAA Privacy Rule/Enforcement Activities)



### **The American Recovery and Reinvestment Act (ARRA) of 2009/HITECH Act**

The economic stimulus package signed into law on 2/17/09 included new HIPAA privacy and security requirements. ARRA tightened some existing HIPAA provisions and imposed entirely new requirements. The most significant changes were a new breach notification requirement, the application of the security and certain privacy requirements directly to business associates and new enforcement penalties. These new regulations were addressed in provisions of the Health Information Technology for Economic and Clinical Act (HITECH Act), passed as part of ARRA. Covered entities and business associates must comply with most of the new privacy requirements by 2/17/10. Covered entities will need to update their policies and procedures and retrain employees.

HHS issued interim final rules on the HITECH Act that were published in the 10/30/09 Federal Register and the rules became effective on 11/30/09. The interim final rules amended the HIPPA enforcement regulations, as they related to the imposition of civil money penalty amounts to incorporate the HITECH Act's categories of violations. Also in August 2009, guidance was provided related to implementation of the breach notification regulations and on encryption and destruction for PHI.

A link to the HITECH Act Enforcement Interim Final Rule is available at:

[www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule](http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule)

Key privacy and security provisions included with the passage of ARRA are summarized below:

- A group health plan or other covered entity must notify each individual whose unsecured PHI it reasonably believes was compromised by an unauthorized use or disclosure. If the breach to PHI occurs under a business associate's control, the business associate must also notify the covered entity. This can involve written notification by mail or, if specified by preference by the individual, e-mail. If the covered entity or business associate lacks current contact information, it may be required to post notice of the breach on its Web site or in newspapers or other broadcast media. Breach notifications must be made without unreasonable delay and within 60 calendar days after the breach is discovered.
- If the breach affects more than 500 people, the covered entity must also report the incident to HHS and the media. This notification requirement applies only to "unsecured" information, which is defined as PHI not secured by an accredited "technology standard". HHS has provided guidance on the breach notification rule including instructions for covered entities to submit breach notifications. The guidance can be accessed at:



**Trilogy Claims Administrative Handbook**  
**Section 4 - Benefits Legislation**  
**Privacy And Confidentiality (4.15)**

<http://www.hhs.gov/ocr/privacy/hipaa/administrative> (link to the breach notification rule)

- HHS has provided guidance related to technologies and methodologies to render unsecured PHI unusable, unreadable or indecipherable to unauthorized individuals. A link to approved encryption processes for data and guidance on destroying PHI is available at:

<http://www.hhs.gov/ocr/privacy/hipaa/administrative> (link to the breach notification rule/unsecured PHI and guidance)

- TPAs and other business associates are now considered to be HIPAA covered entities. Beginning in February, 2010 HIPAA security requirements and civil and criminal penalties will also apply to business associates. A business associate will need to appoint a security official, develop written policies and procedures and train its workforce on how to protect electronic PHI. Business associates will also need to follow HIPAA's security rules relating to physical safeguards (e.g., locking computers with electronic PHI) and technical safeguards (e.g., encrypting e-mails). TPAs and other business associates need to ensure that the security safeguards encompass "home-based access" and that employees who have access to electronic PHI from their home computers are in compliance.
- Civil monetary penalties were significantly increased with a new tiered scale that is tied to the severity of the violation. These new penalty provisions are effective immediately. In addition, state attorney generals can now bring a HIPAA enforcement action against a covered entity or business associate that violates the rules. HHS is required to establish a regulation within the next three years, providing that individuals affected by a HIPAA violation will be able to receive a percentage of any civil monetary penalty or settlement connected with respect to the offense.
- Marketing restrictions were tightened with the prohibition on the sale of PHI without an authorization and restrictions on the instances where a covered entity can use PHI for a communication paid for by a third party.
- Patients now have the opportunity to opt out of PHI disclosures for payment or health care operations by paying for the service out-of-pocket.
- Rather than relying on the minimum necessary standard for other than treatment based PHI, the use of a limited data set is encouraged. HHS is required to issue guidance on what the term "minimum necessary" encompasses with 18 months of the passage of ARRA.



- ARRA creates a new term, “electronic health record” which is an electronic record of health related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff. Under ARRA, if the disclosure of an electronic health record is for treatment, payment or healthcare operations, the covered entity and business associate must maintain an accounting of the disclosure.
- ARRA does not change any state law preemption and covered entities and business associates will continue to have to comply with federal privacy and security standards as well as more restrictive state law requirements.

### **Additional Information**

Additional information regarding federal medical privacy regulations can be obtained by accessing the HHS Web site at:

<http://www.hhs.gov/ocr/hipaa/finalreg.html>

The CMS Web site includes information on HIPAA at:

[http://www.cms.hhs.gov/HIPAAgenInfo/01\\_Overview.asp](http://www.cms.hhs.gov/HIPAAgenInfo/01_Overview.asp)

The Health Privacy Project is dedicated to raising public awareness of the importance of ensuring health privacy in order to improve health care access and quality, both on an individual and a community level.

<http://www.healthprivacy.org/>

The Employer’s Guide to HIPAA Privacy Requirements can be purchased from Thompson Publishing Group, Inc.

[www.thompson.com](http://www.thompson.com)