HIPAA

HIPAA and Group Health Plans

CareFirst BlueCross BlueShield

This booklet is provided as an informational service only and is not intended to replace or serve as legal counsel. To ensure that you and/or your company are taking the necessary steps to comply with HIPAA regulations, you should consult your attorney.

Overview of HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 was designed to streamline all areas of the health care industry and to provide additional rights and protections to participants in health plans.

The law includes five sections that incorporate a variety of provisions from creditable coverage and tax-related issues to health care fraud and privacy. This booklet is concerned with the implementation requirements of HIPAA relating to Transactions & Code Sets, Security and Privacy.

A wide range of health care organizations are affected by HIPAA, and are referred to under the law as "covered entities". These include:

- health plans;
- health care clearinghouses; and
- health care providers who transmit certain health information in electronic form.

HIPAA regulations have a number of implications for employer plan sponsors, agents and brokers, even though they are not "covered entities".

An Introduction to HIPAA for Transaction & Code Sets, Security and Privacy

Sometimes called Administrative Simplification, these regulations involve two primary areas –

(1.) the standardization of health care-related transactions, and
(2.) the implementation of controls to protect an individual's health information.

(1.) *Standardization of Health care Transactions* regulations include:

- An Electronic Transactions and Code Sets Rule; and
- Several Unique Identifiers Rules.

Covered entities must be compliant with the Electronic Transactions Requirements by October 2002 (October 2003 if the covered entity has requested a 1-year extension from the government) and with the Unique Identifiers Rules 26 months after the final rule is published.

(2.) *Controls to Protect Health Information* regulations include:

- A Privacy Rule; and
- A Security Rule.

Covered entities must be compliant with the Privacy Rule by April 2003 and with the Security Rule 26 months after the final rule is published.

In order to fully understand HIPAA, it is important to understand some key definitions. Following are a few with which we recommend you become familiar in order to ensure you appropriately comply with the law.

Health Information – Health information is oral or recorded in any form or medium created or received by a health plan, provider, clearinghouse, employer, etc. that relates to:

- an individual's past, present, or future physical or mental health or condition;
- the provision of health care to an individual; or
- the past, present, or future payment for the provision of health care to an individual.

Protected Health Information (PHI) – Health information becomes PHI when it is matched with another piece of information that identifies the individual or from which the individual could reasonably be identified. For ex. name, SSN, address, DOB, certificate number, etc.

Summary Health Information – Summary health information is stripped of all information that could identify or reasonably identify an individual, and summarizes the claims history, claims expenses, or type of claims experienced by individuals for whom an employer provides health benefits under a group health plan.

Health Plan – An "individual or group plan that provides, or pays the costs of, medical care." A health plan includes group health plans, health insurance issuers, managed care plans, essentially all government health plans, Medicare, Medicare supplemental plans and Medicaid.

Because HIPAA includes a group health plan as a covered entity, most employee welfare benefit plans provided by an employer, whether insured or self-insured, are covered by the regulation. As a result, employers will be subjected to some obligations under HIPAA.

Group Health Plan – The component of the employer that includes individuals who require access to other employees' PHI to perform their day-to-day job functions of administering health benefits for those employees. These individuals usually work within the human resources/employee benefits area of the employer.

If any PHI is to be received by the group health plan, these individuals must be clearly identified by name or position by the employer and they must carefully protect the confidentiality of individuals in the health plan. Additionally, the group health plan will be required to comply with all applicable group health plan requirements under HIPAA.

Plan Sponsor – A legal entity that offers the group health plan to its employees or members (as defined by the ERISA statute). A plan sponsor may be a director, senior executive, or all other employees who do not require access to enrollees' PHI to perform their day-to-day job functions. These individuals should have no access to the employees' PHI other than their own personal information.

The HIPAA regulations regard the Group Health Plan and the Plan Sponsor as ***two separate entities***.

Penalties for Noncompliance

HIPAA includes both civil and criminal penalties for noncompliance.

Maximum $25,000 fine annually
For simple noncompliance with HIPAA requirements. No penalty will be assessed if it is determined that there was a reasonable effort made to learn and implement the requirements and correction of the noncompliance takes place within 30 days.

Maximum $50,000 fine and one year prison term
For knowingly obtaining Protected Health Information (PHI) and wrongfully disclosing it.

Maximum $100,000 fine and five year prison term
For obtaining and disclosing PHI through false pretenses.

Maximum $250,000 fine and ten year prison term
For obtaining and disclosing PHI for commercial advantage, personal gain or malicious harm.

HIPAA violations that carry civil (monetary) penalties will be investigated and enforced by HHS' Office for Civil Rights. Criminal investigations (violations punishable by prison terms) will be handled by the Office of Inspector General.

There is no private right of action given to individuals under the HIPAA legislation, but in the future, individuals who bring suit for a violation of state-law rights of privacy may point to these HIPAA requirements as setting a standard that a provider, employer or health plan should have observed in protecting the individual's health information.

Transactions Requirements

A standard set of code terminology and electronic transaction formats will **allow all health care providers, health plans (for ex. CareFirst BlueCross BlueShield or your group health plan), employers and individuals** to exchange appropriate information faster and more accurately than the current practice of using a variety of formats.

These standard transaction formats and code sets are designed to allow for convenient electronic exchange of basic health care transactions such as submitting and checking the status of claims, enrollment and disenrollment information, remittance notices, premium payments, eligibility inquiries and responses and coordination of benefit activities.

Information shared between health plans for the coordination of benefits and the processing of claims for individuals with more than one health insurer must also follow the transaction standards.

The standard transactions addressed in the current Transactions and Code Sets Rule and their associated identifying numbers are:

- Claim Submission (837)
- Claim Payment (835)
- Claim Status Inquiry (276)
- Claim Status Response (277)
- Eligibility Benefit Inquiry (270)
- Eligibility Response (271)
- Referrals and Authorizations (278)
- Payroll Deducted and Other Group Premium Payment (820)
- Benefit Enrollment and Maintenance (834)

As part of this Rule, unique identifiers will be implemented for all entities involved in administering health care, such as providers, employers and health plans to further ensure faster and more accurate administration.

National provider and health plan identifiers will be overseen by the Centers for Medicare and Medicaid Services (CMS, formerly HCFA). Employer identifiers will be the IRS-assigned Employer Identification Number (EIN) already in use today.

Note: If the employer wants the group health plan to act as a conduit, the submission would have to comply with the transaction requirements.

Impact on Employers

This Rule concerns primarily insurance companies, HMOs, health care providers and any organization that may act as a conduit of PHI (for ex. clearinghouses, billing firms, TPAs, etc.). Although employers may submit the content of some of the standard transactions (e.g., enrollment and disenrollment (834), or premium payment (820)), to one of the entities listed above, the *format* of those submissions does not have to comply with the requirements of this HIPAA Rule.

The Security Rule

The Security Rule directly addresses the means used by a covered entity to safeguard PHI against unauthorized uses or disclosures. There are three primary types of security requirements of this Rule, including:

Administrative Procedures – For example, the establishment of clear policies and procedures to ensure understanding of who has and does not have authorized access to PHI.

Physical Safeguards – For example, the establishment of restricted, locked areas where PHI is stored.

Technical Safeguards – For example, the establishment of private computer files and/or firewalls making unauthorized access to PHI on a computer difficult.

By doing all three, covered entities will be able to better protect the integrity and confidentiality of PHI.

Impact on Employers

The Security Rule is currently in draft form pending finalization, but group health plans (i.e. the department or staff of the employer that handles day-to-day administration of the health plan) should begin planning now to comply with the Rule's requirements.

When planning for compliance, please note that the Security Rule requirements are intended to be "technology neutral" and "scalable". This means that no specific type of hardware or software is required, so long as the objectives of HIPAA are accomplished, and smaller group health plans that may not have the staff or dollar resources as larger group health plans are not required to use the same solutions to meet the Security Rule requirements.

The Privacy Rule

The Privacy Rule sets a national minimum standard for the protection of individuals' PHI regardless of the form of that information. State laws still apply if they give the enrollee more privacy protection.

It is the Privacy Rule that will have the most impact on employers and the health benefits plans that they sponsor.

The Privacy Rule sets out requirements for:

- contracts with "business associates"
- uses of "consents" and "authorizations"
- uses and disclosures of PHI
- a "notice of privacy practices"
- member rights with regard to:
  - access to PHI,
  - amendment to PHI
  - restrictions on use of PHI, and
  - accounting for uses and disclosures of PHI
- privacy policies and procedures, including handling complaints, appointing a privacy officer, record retention, and providing staff training.

The Privacy Rule uses the structure created by ERISA, which sets up two distinct components within an entity offering health insurance benefits to employees to set its requirements. These components are the plan sponsor (i.e. the employer) and the group health plan (i.e. those who administer the plan).

The Privacy Rule creates a regulatory barrier to restrict the flow of PHI between a group health plan and the plan sponsor. *The primary goal of this separation is to prevent employers from using their employees' PHI when making employment-related decisions.*

Impact on Employers

Again, group health plans are considered covered entities under the Privacy Rule and as such, must comply with the requirements of the regulation in the same way as health insurers and providers.

A group health plan is not subject to the HIPAA requirements if, and only if, it meets two criteria:

1. The plan provides benefits solely through an insurance contract with an insurer or HMO (i.e., is fully insured); AND

2. the plan does not create or receive PHI. *(The plan may receive summary health information or information on whether an individual is enrolled or disenrolled from an insurer or HMO).*

Fully-Insured Group Health Plans that Do Not Receive PHI

A group health plan that fits this category has limited obligations under the Privacy Rule. The plan must:

1. Refrain from interfering with employees exercising their rights under the Privacy Rule (e.g., requesting access to or a copy of their health information, filing a privacy complaint); and

2. Refrain from requiring any person to waive rights under the Privacy Rule as a condition of receiving payment, enrolling in a health plan or being eligible for benefits.

Fully-Insured Group Health Plans that Receive PHI or Self-Insured and Cost-Plus Plans

Group health plans that fall into this category must fully comply with the Privacy Rule in the same way that a health insurer or provider would have to comply.

In addition to the two obligations imposed on fully insured group health plans that do not receive PHI (listed above), fully insured group health plans that receive PHI and self-insured and cost-plus group health plans must:

1. Designate a privacy official who is responsible for the development and implementation of the group health plan's policies and procedures;

2. Designate a contact person (or office) who is responsible for receiving complaints filed under the Privacy Rule;

3. Establish policies and procedures concerning PHI that comply with the Privacy Rule;

4. Train all members of the workforce on the group health plan's PHI policies and procedures;

5. Establish appropriate administrative, technical, and physical safeguards to protect the privacy of PHI from intentional or unintentional use or disclosure that violates the Privacy Rule;

6. Provide a process for individuals to make complaints concerning the group health plan's policies and procedures, or its compliance with its policies and procedures or the Privacy Rule;

7. Establish and apply appropriate disciplinary measures against members of its workforce for violations of the group health plan's policies and procedures, or the Privacy Rule;

8. Act promptly to correct a violation or otherwise lessen the harmful effects resulting from a violation of its policies and procedures about which it has knowledge;

9. Provide Notice of Privacy Practices to members of group health plan; and

10. Send agreements to business associates to ensure HIPAA compliance dealing with PHI.

Plan Sponsors

A plan sponsor's obligations will vary depending on whether it receives PHI, summary health information or no health information at all.

If the plan sponsor needs no health information at all (neither PHI or summary health information):
The plan sponsor has no compliance obligations under HIPAA.

If the plan sponsor needs no PHI, but only summary health information or information on whether an individual is enrolled or disenrolled from an insurer or HMO:
The impact of the Privacy Rule will be minimal. Summary health information may be released to a plan sponsor if the plan sponsor agrees to only use the information to:

1. obtain premium bids for providing health insurance coverage to the group health plan; or

2. modify, amend or terminate the group health plan.

If a plan sponsor requires PHI to manage its health benefits program:
The compliance requirements increase dramatically in this situation. Before the plan sponsor may receive PHI from either the group health plan or the insurer, it must "certify" to the group health plan that its plan documents have been amended to incorporate the following provisions, and that it agrees to abide by them.

The plan sponsor must:

1. Only disclose PHI as permitted by the plan documents or as required by law;

2. Not use or disclose the PHI for employment-related actions or decisions, or in connection with any other benefit or employee benefit plan of the sponsor;

3. Ensure "adequate separation" of records and employees is established and maintained between the group health plan and the plan sponsor;

4. Ensure that the plan sponsor's agents and subcontractors (e.g., benefits consultants) agree to abide by the same restrictions and conditions as the plan sponsor in regard to the use of PHI received from the group health plan;

5. Report any improper use or disclosure of PHI to the group health plan;

6. Allow individuals to inspect and obtain copies of PHI about themselves;

7. Allow individuals to request to amend PHI about themselves;

8. Provide individuals with an accounting of disclosures of PHI made within the six years prior to the request for such accounting; and

9. Return or destroy PHI provided by the group health plan that is still maintained by the plan sponsor when no longer needed for the purpose that the disclosure was made. If not feasible, then limit the use and disclosure to those purposes; and

10. Make its internal practices, books and records relating to the use and disclosure of PHI available to the Department of Health and Human Services (HHS) for purposes of auditing the group health plan's compliance with the Privacy Rule.

It may be relatively easy to certify that the plan sponsor will not use employee PHI for employment decisions. However, in some situations, when the employees managing the group health plan are the same persons responsible for other employment-related matters, potentially posing a challenge to the requirement of maintaining "adequate separation" of employee records, these requirements create significant complexity for employers as plan sponsors.

An employer, in its role as plan sponsor, must carefully consider the implications of these requirements to determine whether it wishes to receive PHI.

Note: We intend to send PHI directly to the group health plan and not to the plan sponsor. If the plan sponsor requires us to send PHI, we will request a copy of the certification that the plan documents have been amended.

Your Relationship with CareFirst BlueCross BlueShield Under HIPAA

CareFirst has spent significant time examining how the HIPAA regulations affect our business relationship with plan sponsors and fully insured and self-insured group health plans. We believe the policies we will implement to ensure compliance will allow both CareFirst BlueCross BlueShield and you to continue to administer coverage in a manner that minimizes disruption to the service you and your employees enjoy from CareFirst.

Plan Sponsors

As a corporate policy, we will *not* provide PHI to a plan sponsor. The plan sponsor can still receive summary health information or information on whether an individual is enrolled or disenrolled from an insurer or HMO. PHI will be shared only with the group health plan and the employees identified as administering the plan.

Fully Insured Group Health Plans

As a corporate policy, we will provide PHI to a *fully insured* group health plan only according to the following:

1. We will inform the group health plan representative that we will take his/her question or issue, but will return the call directly to the member; or

2. If the member is in the presence of the group health plan representative while he/she is attempting to contact us, we will accept a verbal authorization from the member, note that in our records, then discuss the issue with the member and health plan representative; or

3. If the first and second options listed above are not possible, we will ask the group health plan representative to fax us an authorization completed by the member that will allow us to speak with him/her about a particular issue. Once this has been received, we will assist the group health plan representative in the appropriate manner.

By following this protocol, a *fully insured* group health plan WILL NOT be required to meet the 10 Privacy Rule requirements listed on bottom of page seven. Remember, the group health plan or plan sponsor can still receive summary health information or information on whether an individual is enrolled or disenrolled from an insurer or HMO.

Self-Insured or Cost-Plus Group Health Plans

A *self-insured or cost-plus* group health plan must complete the 10 Privacy Rule requirements listed on page seven. To ensure that these group health plans continue to receive the PHI they are currently receiving from CareFirst BlueCross BlueShield to administer the group health plan, we will take the following actions:

1. We will enter into a Business Associate Agreement that specifies the functions CareFirst BlueCross BlueShield will perform for the plan, after which the group health plan can exchange PHI with us to allow us to assist in administering the health plan;

2. A disclaimer will be placed on all reports and other communications to the group health plan that may contain PHI stating that the PHI is being furnished to the group health plan only and not the plan sponsor; and

3. Before responding to one who has contacted us for a member, we will verify the identity of the person, and ascertain that he/she is representing the group health plan and not the plan sponsor.

Making the Decision – *What Employers Should Be Doing Now*

Before deciding the path your company will take to become compliant, you, as plan sponsor and for your group health plan, must first understand and analyze the HIPAA Privacy Rule as it applies to your health benefits plans. By answering the following questions, you can begin to plan your strategy.

- Is the plan insured or self-insured?
- Is there a single plan or multiple plans?
- Does the employer rely on an insurer to handle day-to-day operations of the plan? Or does the employer use a traditional third-party administrator?
- How involved is the employer in the operation of the plan?
- What kinds of information does the employer receive about the health plan?
- Are there other kinds of benefit plans (e.g., disability, workers' compensation) that the employer is trying to integrate with the health plan?
- What should the employer do about these questions if it is not covered by the ERISA statute (for example, a health plan for state or local government employees)?

Next, assess whether your company's plan sponsor or group health plan requires PHI by answering the following:

Plan Sponsor

- Does the employer as plan sponsor wish to be involved in the overall management of the group health plan?
- If so, can the plan sponsor accomplish its business goals by performing the plan administration functions without receiving any PHI?

If the plan sponsor feels that it must receive or use PHI to achieve its goals, then the plan sponsor will need to comply with the HIPAA privacy requirements outlined in this booklet in order to receive PHI either from the group health plan directly or from an insurer or other entity involved in administering the plan.

Group Health Plan

- Is the plan fully insured or self-insured/cost-plus?
- If fully insured, does the group health plan need to receive PHI to administer the health plan?*
- If self-insured or cost-plus, how will the plan meet all of the HIPAA administrative requirements?
- If self-insured or cost-plus, are the compliance obligations so extensive that the employer wishes to revisit the financing structure of its health plan operations?

**Remember, if the plan is fully insured and no PHI is received by the group health plan, then the plan may be able to avoid many of the compliance obligations imposed by HIPAA. If the plan receives PHI, it will need to comply with the full range of requirements imposed by HIPAA.*

We are actively involved in a nationwide effort with our sister Blue Cross Blue Shield Plans to achieve a higher level of service and security for health plan participants.

Our HIPAA Privacy Office is responsible for ensuring our compliance with HIPAA, responding to privacy-related complaints, and addressing the Security, Privacy and Transactions and Code Sets requirements. More information about HIPAA and our compliance efforts, is available on our Web site, *www.carefirst.com*.