HIPAA Blue Book:
HIPAA and Group Health Plans

COMPLIMENTS OF

v04.11(2)

HIPAA and Group Health Plans

Section I: Overview of HIPAA

The **H**ealth **I**nsurance **P**ortability and **A**ccountability **A**ct of 1996 (HIPAA) 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 (including health insurers, HMOs, managed care plans, and group health plans sponsored by employers, health and welfare funds and associations);
- Health care clearinghouses; and
- Health care providers who transmit certain health information in electronic form.

In February 2009, Congress passed the **H**ealth **I**nformation **T**echnology for **E**conomic and **C**linical **H**ealth Act (HITECH), which is part of the American Recovery and Reinvestment Act (ARRA). Among other things, HITECH expanded the reach of HIPAA by strengthening HIPAA's privacy and security protections, including a mandated breach notification process, increasing civil/criminal penalties and enforcement, and directly subjecting business associates to the security and privacy protections of HIPAA, including enforcement and penalties.

Impact on Employers

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

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

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

- The standardization of health care-related transactions; and
- The implementation of controls to protect an individual's health information.

A. *Standardization of Healthcare Transactions* regulations include:

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

B. *Controls to Protect Health Information* regulations include:

- A Privacy Rule; and
- A Security Rule.

Section III: Key Definitions

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

Individually Identifiable Health Information – Any information whether oral or recorded, received or created, in any form or medium by a health plan, provider, clearinghouse, or employer 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) – Individually identifiable 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. Examples include: name, Social Security number, telephone number, address, date of birth, health plan ID, medical history, health records, and claim information.

Summary Health Information – Information that may be PHI, which summarizes the claims history, claims expense, or type of claims experienced by an individual for whom an employer has provided health benefits under a group health plan and from which most identifiers have been removed. Summary health information must be aggregated to a 5-digit zip code.

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, most 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 fully insured or self-insured, are covered by the regulation. As a result, employers can be subject to HIPAA's obligations at varying degrees.

Group Health Plan – An employee welfare benefit plan (as defined in section 3(1) of the Employee Retirement Income and Security Act of 1974 (ERISA), 29 U.S.C. 1002(1)), including fully insured and self-insured plans to the extent the plan pays for the costs of medical care to employees or their dependents directly or through insurance, reimbursement, or otherwise that:

(1) Has 50 or more participants (as defined in section 3(7) of ERISA, 29 U.S. C. 1002 (7)); **or**

(2) Is administered by an entity other than the employer that established and maintains the plan.

All group health plans are covered entities. A group health plan is 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 a 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.

NOTE: The HIPAA regulations regard the group health plan and the plan sponsor as ***two (2) separate entities.***

Business Associate – An external third party, individual, or entity that provides services or assistance to a covered entity which requires the business associate to access, create, or maintain PHI on behalf of the covered entity. Under HITECH, business associates are directly regulated by HIPAA's security and privacy provisions, including enforcement and penalties.

Minimum Necessary – Covered entities generally are required to use, disclose, and request only the minimum necessary PHI to accomplish the purpose of the request. This concept is called minimum necessary under the Privacy Rule.

Section IV: Penalties for Noncompliance

HIPAA includes both civil (monetary) and criminal (violations punishable by prison terms) penalties for noncompliance. The U.S. Department of Health and Human Services (HHS) Office of Civil Rights (OCR) is the entity responsible for investigating and enforcing HIPAA and may impose penalties as described in the chart below. Criminal investigations (violations punishable by prison terms) are be handled by the Office of Inspector General (OIG). Additionally, under HITECH, a state's attorney general can pursue HIPAA violations in Federal Court – another potential HIPAA enforcement agency.

Type of Violation	Minimum Civil Penalty	Maximum Civil Penalty
Individual did not know (and by exercising reasonable diligence would not have known) that he/she violated HIPAA	$100 per violation	Up to annual $25,000
Violation due to reasonable cause and not due to willful neglect	$1,000 per violation	Up to annual $50,000
Violation due to willful neglect but violation is corrected within the required time period	$10,000 per violation	Up to annual $250,000
Violation is due to willful neglect and is not corrected	$50,000 per violation	Up to annual $1.5M

Section V: Transactions Requirements

A standard set of code terminology and electronic transaction formats allows all health care providers, health plans (e.g., BCBSMT), 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 Deduction and Other Group Premium Payment (820)
- Benefit Enrollment and Maintenance (834)

As part of the Transaction and Code Set Rule, unique identifiers have been 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 are overseen by the Centers for Medicare and Medicaid Services (CMS). Employer identifiers are the IRS-assigned Employer Identification Number (EIN) already in use today.

Impact on Employers

The Transaction and Code Set Rule concerns group health plans, as well as insurance companies, HMOs, health care providers, and any organization that may act as a conduit of PHI (e.g., clearinghouses, billing firms, or third party administrators (TPAs), etc.). The submission of the standard transactions (e.g., enrollment and disenrollment (834) or premium payment (820)), by group health plans must satisfy the requirements of the Transaction and Code Set Rule. If the employer wants the group health plan to act as a conduit, the submission would have to comply with the transaction requirements.

Section VI: 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 and the assignment of responsibility for security.
- **Physical Safeguards** – For example, the establishment of restricted, locked areas where PHI is stored, policies and procedures to protect computer (IT) systems and device/media controls.
- **Technical Safeguards** – For example, the establishment of private computer files and/or firewalls making unauthorized access to PHI on a computer difficult, access controls (e.g., unique ID and passwords, laptop encryption, and encrypted remote storage devices) and transmission security (e.g., email encryption).

By complying with these standards, covered entities and business associates will be able to better protect the availability, integrity, and confidentiality of electronic PHI (ePHI).

Impact on Employers

Covered entities, including group health plans, and business associates must be in compliance with the Security Rule requirements. In complying with the rule, the requirements are intended to be "technology neutral" and "scalable." This means that no specific type of hardware or software is required, as long as the objectives of HIPAA are accomplished. Small 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 objectives of the rule.

Section VII: 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.

The Privacy Rule has the most impact on employers and group health benefit plans that they sponsor. The 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.

The Privacy Rule sets out requirements for:

- Using consents and authorizations;
- Using and disclosing PHI;
- Acting promptly to mitigate or otherwise lessen the harmful effects resulting from a violation, and in the event of a breach of unsecured PHI (as defined under HIPAA), timely notify appropriate parties;
- Establishing privacy policies and procedures, including handling complaints, appointing a privacy officer, record retention, and providing staff training;
- Contracting with business associates;
- Providing a notice of privacy practices (NOPP); and
- Member rights with regard to:
  - Access to PHI
  - Amendment to PHI
  - Confidential communications
  - Restricting use of PHI
  - Accounting of disclosures of PHI

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 (e.g., BCBSMT) and providers. Employers may not use employees PHI when making employment-related decisions.

Section VIII: Specific Requirements for Group Customers

Of all the components of Administrative Simplification, the Privacy Rule has the most impact on group customers. The following section outlines the impact of this rule.

While the HIPAA Privacy Rule imposes obligations on the entire health care industry, the Privacy Rule does not affect the benefit design of the programs offered by our customers, the services provided under these programs, the provider networks available to their members, or the day-to-day operations of providing health care benefits.

Group health plans and their plan sponsors must follow special rules in connection with the Privacy Rule. The rule does not directly regulate plan sponsors; however, it does regulate the group health plans sponsored by the plan sponsors. All group health plans are covered entities under the Privacy Rule and as such, must comply with the applicable requirements of the rule in the same way as health insurance carriers, like BCBSMT, and covered providers. However, the extent of compliance for employers on behalf of the group health plans or as plans sponsors depends on whether the group health plan is fully insured or self-insured and the type of information (e.g., PHI, summary health information, and/or enrollment/disenrollment information) received by the group health plan and/or plan sponsor.

A. Fully Insured Group Health Plan that Does Not Receive PHI

A group health plan is subject to **limited** HIPAA obligations if, and only if, it meets two (2) criteria:

- The group health plan provides benefits solely through an insurance contract with an insurer or HMO (i.e., is fully insured); AND
- The group health plan does not create, maintain, or receive PHI. (The group health plan may receive summary health information or enrollment/disenrollment information from the insurer or HMO.)

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

1. Refrain from intimidating, threatening, coercing, discriminating against, or taking any action against an individual who exercises his or her rights under the Privacy Rule, including the filing of a complaint;
2. Refrain from requiring any person to waive rights under the Privacy Rule as a condition for receiving payment, enrolling in a health plan, or being eligible for benefits;
3. Retain certain documentation; and
4. Enter into business associate agreements when required by the Privacy Rule.

The fully insured group health plan that does not receive PHI can do the following:

1. Perform enrollment functions; and
2. Receive summary health information for any treatment, payment, or health care operation purposes.

B. Fully-Insured Group Health Plan that Receives PHI or Self-Insured Plans

A group health plan that falls into this category must fully comply with the Privacy Rule in the same way that a health insurer like BCBSMT 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 in Section A above), a fully insured group health plan that receives PHI and self-insured group health plans (regardless of whether or not it receives PHI) must:

1. Designate a privacy official who is responsible for the development and implementation of the group health plan's policies and procedures;
2. Establish policies and procedures concerning PHI that comply with the Privacy Rule;
3. Train all members of the workforce on the group health plan's privacy policies and procedures;
4. Designate a contact person (or office) that is responsible for receiving complaints filed under the Privacy Rule and 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. Such complaints and the disposition must be documented;
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 and limit incidental uses of disclosures made pursuant to a permitted or required use or disclosure;
6. 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;
7. Act promptly to notify appropriate parties of a breach involving unsecured PHI (as defined under HIPAA);
8. 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;
9. Provide notice of privacy practices to all individuals in the group health plan;
10. Provide the individual the right to access or amend PHI contained in a designated record set;
11. Provide the individual the right to request confidential communications, restriction on the use and disclosure of PHI, and an accounting of disclosure(s) of PHI made within the six (6) years prior to the request for such accounting (excluding those for treatment, payment or health care operations);
12. Send agreements to business associates to ensure compliance with HIPAA when dealing with PHI, including notification of any unauthorized access, use of disclosure, or breach involving PHI; and
13. Retain compliance documentation for six (6) years.

C. Plan Sponsors (Employers)

A plan sponsor's obligations will vary depending on whether it receives:

- No health information;
- Summary health information and enrollment/disenrollment information only; or
- PHI.

(i) Plan Sponsor Receives or Needs No Health Information: The plan sponsor has no compliance obligations under HIPAA.

(ii) Plan Sponsor Receives Summary Health Information and Enrollment/Disenrollment Information Only (Needs No PHI): The impact of the Privacy Rule is 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.

(iii) Plan Sponsor Receives PHI to Manage a Health Benefit 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. Promptly report to the group health plan any improper access, use, or disclosure of PHI or breach of unsecured PHI (as defined under HIPAA);
6. Allow individuals the right to inspect and obtain copies of PHI contained in a designated record set;
7. Allow individuals the right to request an amendment to PHI contained in a designated record set;
8. Provide individuals with an accounting of disclosures of PHI made within the six (6) years prior to the request for such accounting (excluding those for treatment, payment or health care operations);
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 HHS for purposes of auditing the group health plan's compliance with the Privacy Rule.

Impact on Employers

It may be relatively easy to certify that the plan sponsor will not use employee PHI for employment decisions. However, when the employees managing the group health plan are the same persons responsible for other employment-related matters, this can potentially pose a challenge to the requirement of maintaining "adequate separation" of employee records. The requirements for plan sponsors can create significant complexity for employers acting as plan sponsors. An employer, in its role as plan sponsor, must carefully consider the implications of these requirements to determine whether to receive PHI.

Section IV: Plan Sponsor Responsibility for Fully Insured and Self-Insured Groups

The following chart summarizes what type of information, depending on the funding status of a group health plan and whether or not it receives PHI, can be shared with the plan sponsor and the associated privacy and security requirements:

How the Plan Provides Benefits	PHI Shared with Plan Sponsor	Privacy and Security Requirements for Plan and Plan Sponsor	PHI/ePHI that may be Disclosed by Plan to the Plan Sponsor
Fully Insured (plan does not create or receive PHI – or "hands off")	Plan sponsor receives: • De-identified information (18 specific identifiers removed) • Enrollment/Disenrollment • Summary health information (SHI) for – Obtaining bids; or – Modifying, amending, or terminating the Plan • PHI pursuant to a signed authorization	• No privacy requirements apply to plan or plan sponsor except for a policy prohibiting retaliation and a policy that does not require an employee to waive privacy or security rights • Security requirements if any PHI is maintained or transmitted in electronic form (ePHI)	• SHI for limited purposes • Enrollment/disenrollment • De-identified data (not PHI)
Fully Insured - receiving PHI (also known as "hands on")	Plan sponsor receives: • De-identified information (18 specific identifiers removed) • Enrollment/Disenrollment • SHI for – Obtaining bids; or – Modifying, amending, or terminating the Plan • PHI for plan administration functions • PHI pursuant to a signed authorization	• Privacy requirements, but limited NOPP requirements • Insurer's NOPP must say that PHI is disclosed to plan sponsor and what PHI is shared • Sponsor is responsible for plan's compliance • Plan document and firewall requirements apply to plan and plan sponsor • Must certify to insurer of plan amendment • Security requirements if any PHI is maintained or transmitted in electronic form (ePHI)	• Information as described in the plan document • SHI for limited purposes • Enrollment/disenrollment • De-identified data (not PHI)

Self-Insured (self-administered or TPA)	Plan sponsor receives: • Enrollment/Disenrollment • SHI for – Obtaining bids; or – Modifying, amending, or terminating the Plan • PHI for plan administration functions	• Privacy requirements • NOPP • Sponsor is responsible for plan's compliance • Plan document and firewall requirements apply to plan and plan sponsor • Security requirements if any PHI is maintained or transmitted in electronic form	• Information as described in the plan document • SHI for limited purposes • Enrollment/disenrollment • De-identified data (not PHI)
Plan Administration Functions are limited to activities included in the definition of payment or health care operations. It does not include enrollment/disenrollment or the functions related to receipt of SHI. It does include quality assurance, claims processing, auditing, and monitoring.			

Section X: Group Health Plans and Their Business Associates

When group health plans have taken the necessary steps to become HIPAA compliant based on their fully insured or self-insured status, as well as the amount of PHI/ePHI they elect to receive or create, they must also take steps to ensure their business associates are HIPAA compliant. Under HITECH, business associates, like covered entities (e.g., BCBSMT), are directly subject to HIPAA's privacy and security provisions, including enforcement and penalties. A business associate is an external third party that the covered entity contracts with to perform a covered function on its behalf involving the use or disclosure of PHI. For example, an insurer that provides third party administration (TPA) for a self-insured plan is the business associate of the self-insured plan.

Group health plans that share PHI/ePHI with their business associates must enter into a contract or other arrangement that satisfies HIPAA's specific mandated provisions governing how business associates protect the PHI that they create, receive, use, or disclose. Therefore, the business associate contracts must specify that the business associate:

- Agrees not to use or disclose PHI other than as permitted or required by HIPAA and its contract with the group health plan;
- Agrees to develop, implement, maintain and use appropriate administrative, technical, and physical safeguards that reasonably prevent the use or disclosure of PHI and ePHI;
- Agrees to mitigate, to the extent practicable, any harmful effect that is known to business associate, of a use or disclosure of PHI by business associate in violation of the requirements of this Agreement;
- Must ensure that any agent, including a vendor or subcontractor, to whom business associate provides PHI agrees to the same restrictions and conditions that apply to the business associate with respect to such information, including implementation of reasonable and appropriate safeguards to ensure the confidentiality, integrity, and availability of the PHI/ePHI;
- Must provide enrollees with the right upon request to access and amend PHI contained in a designated record set;
- Must provide enrollees with the right to request an accounting of disclosure(s) made within the six (6) years prior to the request for such accounting (excluding those for treatment, payment or health care operations);

- Agrees to make its internal practices, books, and records, including policies and procedures, and any PHI, relating to the use and disclosure of PHI, available to HHS for purposes of determining compliance with applicable law;
- Agrees to document and maintain a record of disclosures of PHI in order to respond to an enrollee's request for an accounting of disclosures of PHI and maintain such accounting for at least six (6) years following the date of the disclosure;
- Agrees to make reasonable efforts to limit PHI to the "minimum necessary" to accomplish the intended purpose of the use, disclosure, or request;
- Will not directly or indirectly receive remuneration in exchange for any PHI;
- Agrees to promptly report to the group health plan any improper access, use, or disclosure of PHI or breach of unsecured PHI (as defined under HIPAA); and,
- Must return or destroy PHI at the end of the contract if feasible to do so. In not feasible, the business associate must ensure that no improper use of disclosure of PHI occurs.

Section XI: The Relationship between the Group Health Plan and BCBSMT Under HIPAA

BCBSMT recognizes the importance of maintaining the confidentiality and security of member PHI. We are committed to preserving the security and confidentiality of the information received and maintaining safeguards to protect PHI against unauthorized access, use, or disclosure. As such, BCBSMT has spent significant time examining how HIPAA affects business relationships with fully insured and self-insured group health plans and plan sponsors. BCBSMT believes the policies it has implemented to ensure HIPAA compliance would allow both BCBSMT and you to continue to administer coverage. In addition, BCBSMT's Notice of Privacy Practices is available on its website at www.bcbsmt.com.

A. Fully Insured Group Health Plans. As a general rule, BCBSMT will only provide summary health information for the purposes previously discussed and enrollment/disenrollment information to the plan sponsor. By following this protocol, a fully insured group health plan **is not** required to meet the 13 privacy rule requirements listed in Section VIII(B), page 9.

B. Fully Insured Group Health Plans that Receive PHI and Self-Insured Group Health Plans. A fully insured group health plan that receives PHI or a self-insured group health plan must satisfy the 13 privacy rule requirements listed in Section VIII(B), page 9, regardless of the type of information received. The plan sponsors must comply with the plan document amendments listed in Section VIII(B), page 9, if the plan sponsor creates, receives, or maintains PHI. To receive PHI from BCBSMT, we will require the following actions:

1. BCBSMT will enter into a business associate agreement that specifies the functions BCBSMT will perform for the group health plan.
2. All releases of PHI will be made to plan sponsors whose identity will be verified by BCBSMT. All requests for specific written reports must be made in writing to the attention of the BCBSMT Marketing department.

Section XII: Making the Decision – What Employers Should Be Doing Now

A. Basic Structure of Your Health Benefit Plan

Before deciding the path your company (as the employer) will take to become compliant, you must first understand and analyze the HIPAA Privacy Rule as it applies to your health benefit plans. You can begin to plan your strategy by answering the following questions:

- 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 (TPA)?
- How involved is the employer in the operation of the plan?
- What kind of information does the employer receive or need concerning 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)?

B. PHI and Your Plan Sponsor and Group Health Plan

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

Impact on Employers

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/ePHI, it will need to comply with the full range of requirements imposed by HIPAA.

Section XIII: BCBSMT Privacy and Security Offices, Questions and Complaints

BCBSMT's Privacy Office is responsible for ensuring BCBSMT's compliance with HIPAA, responding to privacy-related complaints, and addressing privacy requirements. The Privacy Office can be reach at:

Attention: Privacy Office
Blue Cross and Blue Shield of Montana
P.O. Box 4309
Helena, MT 59604

E-mail: PrivacyOffice@bcbsmt.com
FAX: 406.437.7883

BCBSMT's Security Office is responsible for technical compliance with HIPAA, HITECH and state requirements, investigating security incidents and providing recommendations to better secure data, personnel and resources. The Security Office can be reach at:

Attention: Security Office
Blue Cross and Blue Shield of Montana
P.O. Box 4309
Helena, MT 59604

E-mail: Justin_Elkins@bcbsmt.com
FAX: 406.437.7830