



HIPAA Title II Blue Book

*Health Insurance Portability
and Accountability Act of 1996*

Title II

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, you should consult your attorney.

Overview of HIPAA

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is legislation enacted by the federal government to streamline the health care industry and to provide additional rights and protections to participants in health plans.

The law includes five sections, or Titles, 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 of HIPAA Title II, sometimes called Administrative Simplification.*

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

- health plans (including group health plans);
- health care clearinghouses; and
- health care providers conducting electronic transactions.

HIPAA Title II has a direct impact on group health plans, like yours, and a number of indirect implications for employers sponsoring group health plans (a.k.a. plan sponsors), as well as Business Associates such as agents, brokers and third party administrators.

An Introduction to HIPAA Title II

HIPAA Title II, sometimes called Administrative Simplification, has two primary areas of regulation: (1.) the standardization of certain electronic 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:

- Electronic Transactions and Code Sets Requirements
- 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 one-year extension from the government or if the covered entity is a small health plan). Anthem has filed for, and received, a one-year extension for compliance with the Electronic Transactions Requirements. Covered entities must be compliant with the Unique Identifiers Rules 26 months after the final rule is published.

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

- Privacy Rule
- Security Rule

Covered entities must be compliant with the Privacy Rule by April 2003 and with the Security Rule by April 2005.*

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

Health Information — Health information means any information, whether oral or recorded in any form or medium, that:

- is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and
- relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

**Note that small health plans have an additional year to comply with the Privacy Rule and Security Rule.*

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 example: name, SSN, address, DOB, certificate number). PHI is individually identifiable information that is transmitted or maintained electronically, on paper, orally or in any form or medium.

Summary Health Information (SHI) — SHI 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 Title II.*

Group Health Plan (GHP) — The employee welfare benefit plan (fully insured and self insured). GHP is the component of the employer that includes individuals requiring 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 or 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 individual information.

Plan Sponsor/Employer — 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 Title II regulations regard the group health plan and the plan sponsor/employer as two separate entities.

HIPAA Title II

Penalties for Noncompliance

HIPAA Title II includes both civil and criminal penalties for noncompliance.

- **Maximum \$25,000 fine annually (for each violated requirement)** for simple noncompliance with HIPAA requirements

No penalty will be assessed if it is determined that the failure to comply was not willful and 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/or one-year prison term** for knowingly *and* wrongfully using, obtaining or disclosing PHI
- **Maximum \$100,000 fine and/or five-year prison term** for using, obtaining or disclosing PHI through false pretenses
- **Maximum \$250,000 fine and/or 10-year prison term** for using, obtaining or disclosing PHI for commercial advantage, personal gain or malicious harm

Violations of HIPAA Title II that carry civil (monetary) penalties will be investigated and enforced by the Department of Health and Human Services' (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, health plan or group health plan should have observed in protecting the individual's health information.

HIPAA Title II

Transactions Requirements

A standard set of code terminology and electronic transaction formats will allow all health care providers, clearinghouses and health plans 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 also must follow the transaction standards.

The standard transactions addressed in the current Transactions and Code Sets Requirements, 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.

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 example, 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 Title II Rule because employers are not covered entities.

HIPAA Title II

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 safeguards required by this Rule:

Administrative Safeguards — Policies and procedures used to select security controls and govern behaviors relating to the protection of PHI.

Physical Safeguards — Policies, procedures and physical controls used to protect PHI housed within facilities, for example, establishing restricted, locked areas where PHI is stored.

Technical Safeguards — Policies, procedures and technology controls used to protect PHI contained within computer systems, for example, requiring a password to read computer files containing PHI.

By using all three types of security safeguards, covered entities will be able to better protect the confidentiality, integrity and availability of PHI.

Impact on Employers

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.

HIPAA Title II

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 individual 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
- use of 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 of disclosures
- 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/employer. *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. As the sponsor of these plans, employers are indirectly impacted.

HIPAA Title II

A group health plan is not subject to some HIPAA requirements if it meets two criteria:

- The plan provides benefits solely through an insurance contract with an insurer or HMO (i.e., is fully insured); *and*
- 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).
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/ASO 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/ASO group health plans must:

1. **Designate a privacy official** who is responsible for the development and implementation of the 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.

HIPAA Title II

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.

Plan Sponsors/Employers

The impact on a plan sponsor/employer will vary depending on whether it receives PHI, SHI or no health information at all.

If the plan sponsor/employer needs no health information at all (PHI or SHI)

The Privacy Rule will have no impact on the plan sponsor/employer.

If the plan sponsor/employer needs no PHI, but only SHI or information on whether an individual is enrolled or disenrolled from an insurer or HMO

The impact of the Privacy Rule will be minimal. SHI may be released to a plan sponsor/employer if the plan sponsor/employer agrees to only use the information to:

- obtain premium bids for providing health insurance coverage to the group health plan; or
- modify, amend or terminate the group health plan.

If a plan sponsor/employer requires PHI to manage its health benefits program

The impact of the Privacy Rule will be greater. Before the plan sponsor/employer may receive PHI from the group health plan, 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

HIPAA Title II

abide by them. Group health plans are prohibited from disclosing PHI to the plan sponsor/employer unless and until it receives the certification.

The plan sponsor/employer must agree to:

- only disclose PHI as permitted by the plan documents or as required by law.
- 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 plan sponsor/employer.
- ensure “adequate separation” of records and employees is established and maintained between the group health plan and the plan sponsor/employer.
- ensure that the plan sponsor/employer’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.
- report any improper use or disclosure of PHI of which it becomes aware to the group health plan.
- allow individuals to inspect and obtain copies of PHI about themselves.
- allow individuals to request to amend PHI about themselves.
- provide individuals with an accounting of certain disclosures of PHI upon request.
- 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.
- if feasible, return or destroy all PHI when it is no longer needed.

It may be relatively easy to certify that the plan sponsor/employer 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.

Important Note: Anthem will not provide PHI to a plan sponsor/employer even if the group health plan obtains the certification. (See page 13 for details.)

HIPAA Title II

Your Relationship with Anthem Under the Privacy Rule

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

Fully Insured Group Health Plans

Fully insured group health plans will normally include traditional premium-based and alternative-funded plans. As a covered entity, Anthem is permitted to and will provide to fully insured group health plans the minimum necessary PHI to run the Organized Health Care Arrangement (OHCA). Anthem will determine how much and if PHI is necessary to run the OHCA. Anthem is also permitted to and will provide SHI and enrollment/disenrollment information to fully insured group health plans (even those who elect not to receive PHI).

To specifically address questions about routine activities and how Anthem will handle these under the Privacy Rule, refer to the following:

Group Customer Service (e.g., telephone interaction): When performing group customer service functions, Anthem will be allowed to disclose a minimum amount of PHI to the fully insured group health plan, as necessary, to run the OHCA. The PHI may be disclosed to a group health plan representative only (as opposed to the plan sponsor/employer). In addition, Anthem will review requests from fully insured group health plans to disclose PHI to business associates or other parties acting on behalf of the group. These requests will normally be approved if the disclosure could have been made directly to the group.

HIPAA Title II

If Anthem determines that the requested PHI is not necessary to run the OHCA, PHI will only be disclosed as follows:

- 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.
- 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 health plan representative.
- 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. (Anthem will accept Anthem's Authorization form or forms developed by the group that are compliant with federal and state law. Your sales representative can provide you with copies of Anthem's forms.)

Reporting: As a general rule, Anthem will provide reports that contain only SHI, enrollment or disenrollment, or de-identified information to fully insured group health plans. These reports will be provided upon request (verbal, written, fax or e-mail). PHI reports will be provided on an exception basis. Fully insured group health plans should submit requests for PHI on Anthem's PHI Report Request form. Anthem will determine if the PHI is needed to run the OHCA.

Billing: For fully insured group health plans, billing will follow a process similar to the reporting process.

Fully Insured Group Health Plans that Do Not Receive PHI

Fully insured group health plans must notify Anthem in writing of their choice not to receive PHI and that they elect to only receive SHI or enrollment/disenrollment information.

Upon receipt of this request, Anthem will not provide PHI in any manner (e.g., phone, reports, bills).

HIPAA Title II

By following this protocol, a fully insured group health plan will not be required to meet the eight privacy requirements detailed on pages 8 and 9. Remember, the group health plan or a plan sponsor/employer can still receive SHI or information on whether an individual is enrolled or disenrolled from an insurer or HMO.

Self-insured/ASO Group Health Plans

A self-insured/ASO group health plan must complete the 10 privacy requirements detailed on pages 8 and 9. To help ensure that these group health plans continue to receive the PHI they are currently receiving from Anthem to administer the group health plan, we will take the following actions:

- We will enter into a Business Associate Agreement that specifies the functions Anthem 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, and vice versa.
- Before responding to an individual who has contacted us on behalf of a member or a self-insured/ASO group health plan, we will verify the identity of the person, and ascertain that he/she is representing the group health plan and not the plan sponsor/employer, before responding to him/her.

Plan Sponsors/Employers

As a corporate policy, we will *not* provide PHI to a plan sponsor/employer in any format (e.g., phone, reports, bills) without a valid authorization from the member. The plan sponsor/employer still can receive SHI or information on whether an individual is enrolled or disenrolled from the plan.

Note that the group health plan (fully insured and self-insured) may share PHI with its plan sponsor/employer provided the group health plan complies with the Privacy Rule requirements set forth on page 10.

HIPAA Title II

Making the Decision – What Employers Should be Doing Now

Before deciding the path your company will take to become compliant, you, as plan sponsor/employer for your group health plan, must first understand and analyze the HIPAA Title II 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 fully 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 types 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 sponsors/employers

- 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/employer accomplish its business goals by performing the plan administration functions without receiving any PHI?

If the plan sponsor/employer feels that it must receive or use PHI to achieve its goals, then the plan sponsor/employer will need to comply with the HIPAA privacy requirements outlined in this booklet in order to receive PHI from the group health plan.

HIPAA Title II

Group health plan

- Is the plan fully insured or self-insured/ASO?
- If fully insured, does the group health plan need to receive PHI to administer the health plan?*
- If self-insured/ASO, how will the plan meet all of the HIPAA administrative requirements?
- If self-insured/ASO, 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 created or 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.*

Anthem HIPAA Program Management Office

Anthem created its HIPAA Program Management Office (HPMO) in January 2000 to ensure the necessary focus that HIPAA demands and to continually monitor Anthem's progress toward HIPAA compliance. The HPMO is comprised of program managers with responsibilities that include project consulting, communications and reporting. These program managers report to the Director of Anthem's National HIPAA Program who, in turn, reports to an Executive Sponsor and the Executive Steering Committee, thereby, establishing complete oversight and facilitation across the entire organization.

To learn more about Anthem's HIPAA compliance efforts, we encourage you to periodically visit the Employers and Benefits Manager's web pages on **anthem.com**. Simply select Employers & Benefits Managers, then click on the appropriate state.

HIPAA Title II

Summary Guide — Privacy Rule

Use the information below as a quick reference to help ensure your company is in compliance with the listed Privacy Rule requirements. (A group health plan is not subject to some HIPAA requirements if it is fully insured and does not create or receive PHI.)

Remember, under HIPAA, there are two components of an employer – the group health plan and the plan sponsor. HIPAA regulations may vary for your company depending on which component wishes to receive PHI, and how much information each component needs.

Group Health Plans (Employees who administer health benefits on behalf of the employer)

Type of Funding	Receive Personal Health Info (PHI)?	Receive Summary Health Info (SHI)?	Privacy Requirements
Fully Insured GHP	✓ No	✓ Yes	<ol style="list-style-type: none"> 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 GHP or Self-insured/ ASO GHP	✓ Yes	✓ Yes	<ol style="list-style-type: none"> 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); 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. 3. Designate a privacy official who is responsible for the development and implementation of the group health plan's policies and procedures; 4. Designate a contact person (or office) who is responsible for receiving complaints filed under the Privacy Rule; 5. Establish policies and procedures concerning PHI that comply with the Privacy Rule; 6. Train all members of the workforce on the group health plan's PHI policies and procedures; 7. 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; 8. 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; 9. 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; and 10. 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.

HIPAA Title II

These guidelines are provided as an informational service only. This 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, you should consult your attorney.

Plan Sponsors/Employers

Type of Funding	Receive Personal Health Info (PHI)?	Receive Summary Health Info (SHI)?	Privacy Impact
Plan sponsor/ employer (Fully insured and Self-insured/ASO)	✓ No	✓ No	No impact.
Plan sponsor/ employer (Fully insured and Self-insured/ASO)	✓ No	✓ Yes	Minimal impact. Plan sponsor/ employer must agree that it will only use SHI to obtain premium bids for providing health insurance coverage to the group health plan, or to modify, amend or terminate the group health plan.
Plan sponsor/ employer (Fully insured and Self-insured/ASO)	✓ Yes	✓ Yes	Maximum impact. Plan documents must be amended to incorporate the following provisions. The plan sponsor/ employer must: <ol style="list-style-type: none"> 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/ employer; 3. Ensure “adequate separation” of records and employees is established and maintained between the group health plan and the plan sponsor/ employer; 4. Ensure agents and subcontractors (e.g., benefits consultants) agree to abide by the same restrictions and conditions as the plan sponsor/ employer in regard to the use of PHI received from the group health plan; 5. Report any improper use or disclosure of PHI of which it becomes aware 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 certain disclosures of PHI upon request; 9. 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; and 10. If feasible, return or destroy all PHI when it is no longer needed.



In Colorado: Anthem Blue Cross and Blue Shield is the trade name of Rocky Mountain Hospital and Medical Service, Inc.
In Connecticut: Anthem Blue Cross and Blue Shield is the trade name of Anthem Health Plans, Inc.
In Indiana: Anthem Blue Cross and Blue Shield is the trade name of Anthem Insurance Companies, Inc.
In Kentucky: Anthem Blue Cross and Blue Shield is the trade name of Anthem Health Plans of Kentucky, Inc.
In Maine: Anthem Blue Cross and Blue Shield is the trade name of Anthem Health Plans of Maine, Inc.
In Nevada: Anthem Blue Cross and Blue Shield is the trade name of Rocky Mountain Hospital and Medical Service, Inc.
In New Hampshire: Anthem Blue Cross and Blue Shield is the trade name of Anthem Health Plans of New Hampshire, Inc.
In Ohio: Anthem Blue Cross and Blue Shield is the trade name of Community Insurance Company.
In Virginia: Anthem Blue Cross and Blue Shield is the trade name of Anthem Health Plans of Virginia, Inc.
(excluding the city of Fairfax, the town of Vienna and the area east of State Route 123.)
Independent licensees of the Blue Cross and Blue Shield Association.
® Registered marks Blue Cross and Blue Shield Association.