



Independent Insurance Agents



Brokers of America, Inc.



MEMORANDUM ON FINAL HIPAA PRIVACY REGULATIONS

This Memorandum regarding the Final HIPAA Privacy Regulations is not intended to provide specific advice about individual legal, business or other questions. It was prepared solely for use as a guide, and is not a recommendation that a particular course of action be followed. If specific legal or other expert advice is required or desired, the services of an appropriate, competent professional, such as an attorney, should be sought.

September 30, 2002

On August 14, 2002, the Department of Health and Human Services (HHS) published its final revised rules governing the privacy of personal health information.¹ These rules – which implement the privacy provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) – are a regulatory labyrinth designed to protect all medical records and other health information held or disclosed by certain entities in any form, whether communicated electronically, on paper or in oral conversations. All covered entities are required to be in compliance with these new rules by **April 14, 2003.**²

This memorandum analyzes the final HIPAA regulations and outlines compliance options for agents and brokers. It begins with a brief overview of the rules. Following the overview are seven Sections that each addresses a particular aspect of the rules. Section I explains what type of information is protected under the rules and to whom the regulatory requirements apply. Section II discusses the general rules for compliance with HIPAA. Section III discusses when protected information may be disclosed without an opt-in. Section IV provides options for compliance when an opt-in may be required (such as for shopping a group health plan). Section V discusses the rules applicable to “business associates” of covered entities. Section VI

¹ 67 Fed. Reg. 53182 (August 14, 2002). The final rules established “Standards for Privacy of Individually Identifiable Health Information,” to be codified at 45 C.F.R. parts 160 and 164, pursuant to the requirements of Section 264 of HIPAA, which amended the Social Security Act by adding Sections 1171 through 1179, 42 U.S.C. § 1320d – 1329d-8. The rules were published first by the Clinton Administration on the eve of its departure from office, on December 28, 2000, but were revisited several times, both formally and informally by the Bush Administration during 2001 and 2002.

² As explained below, it is not clear whether agents, brokers and third-party administrators are covered directly by the rules or are covered only indirectly through the “business associate” provisions. In most respects, it does not matter – the same obligations will be imposed on the activities of agents, brokers and TPAs either way, with two exceptions. First, agents selling health insurance products to individuals on behalf of health insurance carriers may satisfy their HIPAA obligations through the carriers’ compliance program. Second, HHS has no direct enforcement authority over individuals and entities that are not directly regulated under the rules.

discusses the impact of the new health privacy rules on the Gramm-Leach-Bliley Act (GLBA) financial information privacy rules and on state privacy regulations. Finally, Section VII outlines the rules for compliance by agents and brokers under three specific situations:

- (1) Where an insurance agent or broker sells health insurance directly to an individual;
- (2) Where an insurance broker sells a group health plan to an employer; and
- (3) Where an insurance agent/third party administrator sets up and/or manages a self-insured health plan that is covered by stop loss insurance.

Two Appendices are included to facilitate compliance efforts. Appendix 1 contains a sample privacy notice that complies with both HIPAA and GLBA. Appendix 2 contains a memorandum addressing HIPAA's rule regarding standards for electronic health care transactions. As explained in more detail in Appendix 2, essentially all employer benefit plans and any agent, broker or TPA that processes claims or participates in the plan participant enrollment or premium payment process will need to be in compliance with one or more of the code set requirements by October 16th of this year unless a one-year extension is requested by October 15th. Applying for an extension of the electronic transactions regulations compliance date *does not* extend the April 14, 2003 compliance date for the HIPAA privacy obligations discussed in the remainder of the memorandum.

OVERVIEW OF THE RULES

The HIPAA rules apply to "health plans," "health care clearinghouses" and most "health care providers." Collectively, these categories are referred to as "covered entities." The "health plan" definition is broad and, as a result, illogical. The most conservative interpretation is that it includes insurance agents and brokers, as well as any other insurance entity licensed to engage in the business of insurance in a State. (*See* Section I.B, below). Even if they were not covered directly by the definition of "health plan," however, agents and brokers nevertheless would be required to comply with the HIPAA rules as a result of their relationship with other covered entities. The HIPAA compliance requirements apply to all "business associates" of covered entities that receive or are exposed to protected health information in the course of providing services for those entities. Because they unquestionably perform functions for other covered entities – such as group health plans and insurance companies – agents and brokers thus are charged with compliance as "business associates" under the rules.

Several types of insurance benefits are exempt from HIPAA regulation, which means that personal health information gathered in the course of offering these benefits is *not* subject to the compliance requirements. Excepted benefits include workers' compensation, life, disability, property and casualty, and automobile insurance. Agents and brokers that sell both covered and excepted benefits (*e.g.*, life agents that also sell long term care insurance) will have the option of complying with HIPAA for all of their activities *or* segregating their activities (and the

information collected in connection with covered and non-covered activities) and complying with HIPAA only to the extent they are handling information protected by the rules. Section I.C addresses the rules relating to such “hybrid entities” in more detail.

Reinsurers also are exempt; however, a covered entity’s performance of reinsurance-related activities (such as placing stop-loss insurance or handling stop-loss payments for a self-insured plan) is subject to the rules. As a practical matter, coverage of such activities is inconsequential, because in most cases permission to use and disclosure of protected health information to perform these activities will be presumed.

The rules impose four general compliance requirements on covered entities (each of these requirements is discussed in more detail in Section II):

- (1) **Notice.** Covered entities generally must maintain a HIPAA privacy policy notice and provide that notice to recipients of health care and health insurance benefits at their time of enrollment and at least once every three years thereafter. The notice content requirements are similar (but not identical) to those imposed under the GLBA, and must include statements concerning the individual’s rights, the covered entity’s duties, and the types of information uses and disclosures that may be made.
- (2) **“Opt-In.”** In general, HIPAA establishes an opt-in regime for the use or disclosure of protected health information (as opposed to the opt-out regime of the GLBA). Thus, in order to use or disclose protected health information, a covered entity must do one of the following:
 - Determine that the use or disclosure does not require an opt-in.
 - Rely on one of three versions of the information from which certain identifiers have been stripped and comply with the rules for using such filtered information.
 - Obtain written permission from the individual (an “opt-in”).

An executed “opt-in” can remain valid for the duration of a plan participant’s term of employment if it is so stated on the authorization form.

- (3) **Access.** A covered entity must permit individuals to access and amend their protected health information. If the entity does not maintain the information, it must inform the individual where to direct the request. The access rules also include a requirement that covered entities provide individuals upon request with an “accounting of disclosures” made for certain purposes, such as marketing.

- (4) **Administration.** Covered entities must designate an individual to serve as privacy compliance officer and an individual to receive and respond to complaints and inquiries about the entity's privacy policies and practices. A covered entity also must implement data security policies, such as a procedure to enable it to verify the identity of the individual requesting protected information, and ensure that the information it discloses is the "minimum necessary" to carry out the purpose for which the information was requested.

The deadline for compliance with all four sets of requirements is April 14, 2003. HHS' Office of Civil Rights has enforcement authority and may levy substantial civil penalties for general non-compliance. The Office also may charge violators with a federal crime for the wrongful disclosure of protected information;³ however, no private right of action exists to enforce the regulations or to collect damages for wrongful disclosure.

I. WHAT IS PROTECTED AND WHO MUST PROTECT IT

A. Protected Health Information (PHI)

The rules protect *all forms* (oral, written, electronic)⁴ of "individually identifiable health information" – referred to herein as protected health information or "PHI" – which is information (including demographic information) that meets three conditions:

- (1) The information is created or received by a health care provider, health plan, insurer, agent, broker, employer, or health care clearinghouse;
- (2) The information 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; and
- (3) The information either identifies the individual or provides a reasonable basis for believing that it can be used to identify the individual.⁵

³ 42 U.S.C. §1176(a); 65 Fed. Reg. 82,381 (Dec. 28, 2000).

⁴ The rules expand the definition of protected health information from the congressional mandate to encompass *all individually identifiable health information transmitted or maintained by a covered entity, regardless of form*. Arguably, HHS exceeded the scope of its statutory authority by enlarging the universe of protected information to cover non-electronic information.

⁵ 45 C.F.R. § 164.501.

B. Who Must Comply?

Because the rules turn on the definition of “covered entity,” it is essential to understand to whom that term refers. Three types of entities are covered:

- (1) “Health plans.”
- (2) “Health care clearinghouses.”
- (3) “Health care providers” who transmit health information in electronic form in connection with a covered transaction.⁶

1. “Health Plans”

Insurance agents and brokers are neither health care clearinghouses nor health care providers. The definition of “health plan,” however, appears to bring them directly within the rules. “Health plan” means an individual or group plan that provides or pays the cost of medical care. Significantly, a “health plan” is defined to include the following:

- (1) **A health insurance issuer.**
- (2) A group health plan.
- (3) A qualified HMO.
- (4) An issuer of a long-term care policy, excluding a nursing home fixed indemnity policy.
- (5) An employee welfare benefit plan or any other arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees or two or more employers.
- (6) A high risk pool that is a mechanism established under State law to provide health insurance coverage or comparable coverage to eligible individuals.
- (7) Any other individual or group plan, or combination of plans, that provides or pays for the cost of medical care.⁷

The definition of “health insurance issuer” incorporates a broader range of persons and entities than otherwise are considered insurance issuers. The definition is:

⁶ 45 C.F.R. § 160.102.

⁷ 45 C.F.R. §160.103. This list is not exhaustive. Several other specific health care programs (such as the veterans health care program, the programs of public agencies, and parts of the Medicare and Medicaid programs) also are included.

An insurance company, insurance service, or insurance organization (including an HMO) that is licensed to engage in the business of insurance in a State and is subject to State law that regulates insurance.⁸

On its face, this definition encompasses *anyone* that is a health insurance organization or service licensed to engage in the business of insurance in a State. Because HIPAA appears to consider all insurance licensees – including insurance companies as well as agents and brokers – to be “health insurance issuers,” they appear to be covered entities under the rules.

2. Business Associates

Even if they do not fall within the “health insurance issuer” definition, agents and broker nevertheless would be required to adhere to the HIPAA compliance obligations because they unquestionably are “business associates” of other covered entities (*e.g.*, health plans or insurance carriers). “Business associates” are persons that perform functions “on behalf of” covered entities (other than as members of their workforce) involving the use or disclosure of protected information, including:

- Claims processing or administration;
- Data analysis, processing or administration;
- Utilization review;
- Quality assurance;
- Billing;
- Benefit management; and
- Practice management.⁹

3. Introduction to Group Health Plans

Under HIPAA, a “group health plan” is a *separate legal entity* that owes its own compliance obligations under the rules. A “group health plan” is a fully-insured or self-insured employee benefit welfare plan that provides medical care, including items and services paid for as medical care, to employees (or their dependents) directly or through insurance reimbursement or otherwise, that has:

- (1) 50 or more participants; *or*
- (2) An administrator *other than the employer* (*e.g.*, a TPA) that established and maintains the plan.¹⁰

⁸ 45 C.F.R. § 160.103.

⁹ 45 C.F.R. § 160.103. Services may include legal, actuarial, consulting and accounting services. There is a narrow exception to the business associate definition for “conduits.” Any organization through which health information passes without that organization ever accessing the information is not considered to be a business associate. For example, the U.S. Postal Service is a conduit. Similarly, financial institutions that process consumer-conducted debits, credits, electronic fund transfers, etc., are considered to be conduits, not business associates.

¹⁰ 45 C.F.R. § 160.103.

Only plans with fewer than 50 participants that are administered internally by the employer itself are not covered. In general, the rules governing group health plans are more complicated than the rules governing other covered entities because multiple entities are involved in the provision of benefits, including a plan sponsor. Although the plan sponsor – typically an employer – is not itself a covered entity, the health privacy rules regulate the flow of information between the group plan and plan sponsor. For example, in order to disclose protected health information to a plan sponsor, the group health plan must ensure that the plan documents restrict uses and disclosures of information by the plan sponsor to those that are consistent with the rules.¹¹

C. Excepted Benefits

Certain types of insurance benefits are exempt from HIPAA, which means that insurers, agents and brokers that provide *only* these types of benefits are not covered entities and therefore are not required to comply with HIPAA in the course of offering these benefits. Specifically, the rules exempt:

- (1) Life insurance.
- (2) Coverage only for casualty, accident, or disability income insurance, or any combination thereof.
- (3) Liability insurance, including general liability insurance and automobile liability insurance, and coverage issued as a supplement to liability insurance.
- (4) Workers' compensation or similar insurance.
- (5) Automobile medical payment insurance.
- (6) Credit-only insurance.
- (7) Coverage for on-site medical clinics.
- (8) Other similar insurance coverage under which benefits for medical care are secondary or incidental to other insurance benefits.¹²

1. “Hybrid Entities”

More commonly, insurers, agents and brokers will provide both excepted benefits and covered benefits. For example, a life agent also may sell health insurance or long term care

¹¹ 45 C.F.R. § 164.504(f)(1)(i). Requirements for plan documents are addressed in § 164.504(f)(2).

¹² Public Health Service Act (PHSA), 42 U.S.C. § 300gg-91(c)(1).

insurance. The rules permit such “hybrid entities” to designate the components of its business that are health care components – *i.e.*, any part of its practices that performs “covered functions,” such as selling covered benefits – and the components that are not. To accomplish this, the entity simply must place a document in its own internal files making this designation. Then the entity must segregate its covered and uncovered activities by establishing firewalls that preclude persons participating in the unprotected activities from accessing the protected information.¹³

2. Reinsurance / Stop-Loss Insurance

While neither reinsurers nor stop-loss insurers are covered entities, activities related to “ceding, securing or placing a contract for stop-loss insurance,” expressly constitute covered “health care operations” under the rules.¹⁴ Technically, this means that the use of PHI to place a contract for reinsurance or stop-loss insurance is governed by HIPAA. As a practical matter, however, the fact that HIPAA purports to govern stop-loss activities is inconsequential because no opt-in is required for a self-insured health plan to use or disclose PHI to place a contract for stop-loss insurance. (*See* Sections III.B and VII.C).

3. Excepted Benefits

In contrast, an opt-in is required to use PHI to secure a contract for any of the above-listed “excepted benefits,” such as workers’ compensation benefits or life insurance. “De-identified” information – PHI from which 18 identifying factors have been removed (*see* Section IV.A) – also may be used, but such information may not be sufficient to place coverage.

4. Workers Compensation

The HIPAA rules do not interfere with an agent/broker’s ability to obtain health information necessary to process workers compensation claims; however, they may interfere slightly with the amount of information that a health care provider initially is willing to disclose. From a health care provider’s perspective, all health information is the same – it is covered by the rules and therefore protected. The “minimum necessary” rule creates a substantial incentive for health care providers to limit the health information that they disclose.

There is no question, however, that HIPAA expressly permits all covered entities to disclose PHI “as authorized by and to the extent necessary to comply with laws relating to workers compensation” or to comply with other similar programs that “provide benefits for work-related injuries or illnesses without regard to fault.”¹⁵ In other words, there is nothing in the HIPAA rules that requires claims to be paid if the information necessary to pay or otherwise redress the claim has not been disclosed (from the perspective of the carrier, agent/broker or employer). Benefits thus may be withheld until adequate information is received. Accordingly, health care providers’ refusal to disclose necessary information may be more of an initial administrative glitch than a permanent hurdle.

¹³ 45 C.F.R. § 164.504.

¹⁴ 65 Fed. Reg. at 82,568 and 82,576 (explaining that reinsurers and stop-loss insurers do not pay for the cost of medical care but insure health plans and providers against unexpected losses).

¹⁵ 45 C.F.R. § 164.512(l).

II. GENERAL RULES FOR COMPLIANCE

There are four basic components of HIPAA compliance: (1) notice requirements; (2) use and disclosure opt-in requirements; (3) access requirements; and (4) administrative requirements. Each of these is addressed in a general fashion, below. Specific scenarios applicable to agents and brokers are discussed in Section VII.

A. Notice Requirements

In general, an individual must be given adequate notice of the uses and disclosures of protected information that may be made by the covered entity, and notice of the individual's rights and the covered entity's duties with respect to PHI.¹⁶ A covered entity's use and disclosure of protected health information must be consistent with its privacy notice.¹⁷ Provision of a HIPAA privacy notice does not eliminate the need to provide a GLBA notice and, similarly, provision of a GLBA notice does not discharge the HIPAA obligation. Both notices, however, may be combined in the same document.

A covered entity's privacy notice must contain elements similar to those required under other privacy regimes, such as the GLBA. The notice must describe the individual's rights, the covered entity's duties, and the types of uses and disclosures that the covered entity may make of PHI without first obtaining an opt-in.

In general, a notice must be provided to all "health plan enrollees" – all participants in group health plans and all owners of individual health insurance policies – no later than April 14, 2003.¹⁸ With respect to participants that enroll after the plan's compliance date, they must receive notice at the time of enrollment. Provision of notice is sufficient if it is provided to the named insured of a policy under which coverage is provided to the insured and dependents. Beyond providing the initial notice to plan participants, a health plan has two ongoing notice requirements. First, it must provide a notice to all individuals in the plan within sixty days of making any material change to the notice. Second, it must remind plan participants at least once every three years of the availability of the notice and the means to obtain it.

1. Group Health Plans

Special notice rules apply to group health plan arrangements. The key point is that the notice rules differ depending on whether benefits are offered through an insurance contract or whether the plan is self-insured. The basic rule is that an individual should receive notice from whomever he or she receives benefits. Thus, where a plan is secured entirely by an insurance contract, the insurer (and not the plan or agent/broker) in most cases will provide notice. Self-insured plans, on the other hand, must provide their own privacy notice to enrollees

¹⁶ 45 C.F.R. § 164.520.

¹⁷ 45 C.F.R. § 164.502(i).

¹⁸ "Small health plans," meaning plans with annual receipts of \$5 million or less, automatically have one extra year – until April 14, 2004 – to comply.

(typically through the plan administrator). These notice rules are addressed in more detail in Sections VII.B and C.

2. Joint Notices

The rules permit joint notices by two covered entities in certain circumstances. For agents and brokers, the joint notice rule operates like the Agent Exception in the GLBA. Agents acting on a single insurer's behalf can opt to be covered by the insurer's HIPAA privacy notice. (See Situation 1, discussed in Section VII). Provision of the notice by of the entities it covers is sufficient for compliance with HIPAA.¹⁹ Entities participating in an "organized health care arrangement" also may avail themselves of the joint notice rule. (See Sections IV.A and VII.B).

3. Electronic Notice

If a covered entity maintains a web site that provides information about customer services and benefits, then the covered entity must post its health privacy notice on the web site and make the notice available electronically, such as via e-mail.²⁰ To provide the notice via e-mail, the covered entity first must obtain an agreement from the individual to receive the notice via e-mail. Under either method, the individual retains the right to obtain a paper copy of the privacy notice from the covered entity upon request.

B. The "Opt-In" Requirement

This Section presents the general rules governing a covered entity's use and disclosure of PHI. The circumstances under which information can be used and disclosed without an affirmative opt-in are discussed in Section III; the options for shopping a plan's coverage are outlined in detail in Section IV; and the nuances applicable to agents/brokers under each of the three core scenarios are discussed in Section VII.

Prior to using or disclosing protected information, a covered entity or its business associate must do one of three things:

- (1) Determine that the use/disclose is permitted and thus that no opt-in is required;
- (2) Use a version of the information from which identifying factors have been stripped; or
- (3) Obtain an affirmative, written authorization.

If an affirmative, written authorization is received, it may remain valid for the tenure of an individual's employment if the authorization so states.

¹⁹ 45 C.F.R. § 164.520(d)(3).

²⁰ Individuals should be able to print and/or download the notice. 45 C.F.R. §164.520(c)(3)(i).

It is important to remember that the rules refer both to information “use” *and* information “disclosure.” In contrast to privacy regulations under the GLBA or the Fair Credit Reporting Act that are concerned primarily with information disclosure, the HIPAA rules regulate both the way in which a covered entity may *use* information *and* the way in which it may *disclose* that information.²¹

C. Access Requirements and the “Accounting of Disclosures”

The third category of requirements with which a covered entity and its business associates must comply concerns an individual’s access to PHI. As a practical matter, the access rules may not affect insurance agents and brokers as much as the other rules because individuals are more likely to seek access to their medical records from health care providers, and agents and brokers are less likely to have this information in their files in any event. Nevertheless, the access rules require compliance by all covered entities.

A covered entity must provide an individual with access to protected health information that the entity creates, receives or maintains about that individual.²² Individuals have the right to request an amendment or correction of such information.²³ The information to which the entity must provide access is information maintained as a “designated record set,” which includes, at a minimum, information regarding enrollment, payment, claims adjudication and any case or medical management records. The covered entity’s obligation to provide access extends to any protected information that is created or received by its business associates.

A covered entity must include in its privacy notice a statement alerting individuals to their right to access protected information. Covered entities may require individuals to submit access requests in writing and may impose a reasonable, cost-based fee for providing access, but these requirements must be noted in the privacy notice.²⁴ If an individual requests information that the covered entity does not have, the entity must tell the individual where to direct his or her request if it knows where such information may be accessed.²⁵

In addition, individuals generally have a right to receive a written “accounting of disclosures” of protected health information made by a covered entity or its business associates in the six years prior to the date on which the accounting is requested. There are a few key exceptions to this rule. The “accounting of disclosures” need not include disclosures made to the individual or disclosures that occurred prior to the covered entity’s compliance date.²⁶

Moreover, the accounting need not include disclosures made to carry out “treatment,” “payment,” or “health care operations” (these terms are defined in Section III). In the group health plan context, that means that covered entities need not account for any disclosures related

²¹ “Use” includes the covered entity’s own use of protected information (*i.e.*, utilization within an entity). “Disclosure” refers to a covered entity’s release, transfer, provision of access to, or divulging in any manner of protected information *outside the entity*, including disclosures to business associates.

²² 45 C.F.R. § 164.524.

²³ 45 C.F.R. § 164.524.

²⁴ 45 C.F.R. § 164.524(c)(4).

²⁵ 45 C.F.R. § 164.524(d)(3).

²⁶ 45 C.F.R. § 164.528.

to paying claims, shopping the plan or adding a new covered benefit. If a plan (or its broker) discloses PHI to shop for an excepted benefit (*e.g.*, disability insurance), however, that disclosure would have to be noted.

D. Administrative Requirements

1. Personnel Designations

Covered entities must designate an individual who will act as privacy compliance officer and an individual to receive and respond to complaints and inquiries about the entity's privacy policies and practices. These individuals must receive adequate training by the covered entity in order to ensure their compliance with the rules.

2. Verification Requirement

Covered entities must institute policies and procedures designed to verify the identity and authority of the individual or entity requesting access to PHI before an information disclosure takes place.²⁷ This requirement is limited to obtaining documentation supporting the identity and authority of requestors who are not known to the covered entity. If the covered entity knows the requestor, no further verification is required.²⁸

4. Document Retention

Covered entities must maintain (in written or electronic form) all of their policies and procedures concerning the protection of health information. These policies and procedures can be as simple as noting, such as in the case of life insurance agents, that information is collected, used one time, and not retained. A covered entity also must maintain copies of all written communications required by the rules (such as authorization forms that it receives), and must document and maintain documentation of any activity or designation for which the rules require documentation.

5. “Minimum Necessary” Standard

Even where the use or disclosure of protected health information is permitted, a covered entity must make reasonable efforts to limit the information to the “minimum necessary” to accomplish the intended purpose of the use, disclosure or request. This is referred to as the “minimum necessary standard.” The rule applies when the covered entity is using, disclosing PHI *or* requesting it from another covered entity. Significantly, the rule does not apply to any disclosures to health care provider for purposes of treatment.²⁹

The minimum necessary standard basically requires covered entities to implement procedures for ensuring that only the employees who need to know PHI have access to it and for

²⁷ 45 C.F.R. § 164.514(h).

²⁸ Knowledge may take the form of a known place of business, address, phone or fax number, or human being. 65 Fed. Reg. at 82,547.

²⁹ 45 C.F.R. § 164.502(b).

avoiding “data dumps” when only limited information is requested. The standard for determining the minimum necessary amount varies depending on whether the information at issue is “used,” “routinely requested or disclosed,” or “non-routinely requested or disclosed.”³⁰

- For **information uses**, a covered entity must identify the persons in the entity’s workforce who need access to carry out their duties, the categories of information to which they need access, and the conditions that will apply to such access. The conditions must limit access to only the identified persons and identified categories of information necessary to carry out job responsibilities.
- For **routine requests and disclosures**, the covered entity must establish policies and procedures that limit the disclosure of protected information to the amount and type necessary to carry out the purpose of the request or disclosure. Individual review of each request or disclosure is not necessary.
- For **non-routine requests or disclosures**, the covered entity must develop criteria designed to limit disclosures to only the information necessary to accomplish the purpose for which the disclosure is sought. Non-routine requests and disclosures must be reviewed individually in accordance with the criteria.

6. Business Associate Administrative Compliance

Business associates of covered entities are required to have comparable administrative policies and procedures in place to the extent that they perform functions on behalf of a covered entity, such as a group health plan. Business associate rules are addressed in more detail in Section V.

III. WHEN PHI MAY BE USED/DISCLOSED *WITHOUT* AN OPT-IN

The final revised HIPAA rules expand the circumstances in which an individual’s consent to use PHI will be presumed, thus eliminating the need for an opt-in in many cases.

A. Performance of *All* “Treatment” And “Payment” Functions

A covered entity may use or disclose PHI for its own “treatment” or “payment” activities, the “treatment” activities of any health care provider and the “payment” activities of any health care provider or other covered entity without obtaining an opt-in. (Treatment and payment are defined below). For example, an agent/broker may:

- Use PHI to perform its own payment activities.

³⁰ 45 C.F.R. § 164.514(d).

- Disclose PHI to a group health plan for the plan’s payment activities.
- Disclose PHI or to a doctor or hospital providing treatment to an individual (or group health plan enrollee) to whom it has sold insurance.

“**Treatment**” means the provision, coordination or management of health care by a health care provider. “**Payment**” refers to activities undertaken by a health plan or insurance provider to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits, or to obtain or provide reimbursement for the provision of health care. Examples include:

- Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims.
- Risk adjusting amounts due based on enrollee health status and demographic characteristics.
- Billing, claims management, collection activities, obtaining payment under a contract for stop-loss insurance, and related health care data processing.
- Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges.
- Utilization review activities, including pre-certification and preauthorization of services, concurrent and retrospective review of services

B. Performance of an Entity’s Own “Health Care Operations”

In addition, covered entities may use and disclose PHI for the performance of any of *its own* “health care operations” without an opt-in. “**Health care operations**” refers to activities including the following:

- Underwriting, premium rating; and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits (but not “excepted benefits”).
- Ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance).

- Quality assessment and improvement activities.
- Reviewing the competence or qualifications of health care providers.
- Conducting or arranging for medical review, legal services and auditing functions, including fraud and abuse detection.

The primary importance of this rule is its effect on the ability of **self-insured plans** (and agents or brokers operating on their behalf) to carry out necessary functions such as replacing benefits or obtaining contracts for stop-loss insurance. No opt-in is necessary for self-insured plans to perform such functions.

Unless a plan is able to take advantage of the “organized health care arrangement” provisions discussed in Section IV.A, however, the same is not true where covered benefits are fully secured by contracts of insurance. The reason is that the rules do not consider a health insurance carrier’s use of PHI to perform underwriting activities – or a broker’s use of PHI to shop for additional or replacement coverage – to be performance *by the plan* of its *own* “health care operations.” In fact, the revised rules specifically exclude from the list of disclosures for which consent is presumed disclosures between two entities (*e.g.*, an insurer and a plan or its broker) for one to perform the other’s “underwriting or premium rating.”³¹

C. Disclosures to the Individual

Protected information may be disclosed to the individual that is the subject of the information without an opt-in.³²

D. Disclosures to Business Associates

Disclosures between a covered entity and its business associates – and use of information by the business associate on the covered entity’s behalf – is permitted without an opt-in as long as a valid business associate contract is in place. Business associate contracts are addressed in Section V.E.

E. Disclosures Required By Law

Other disclosures permissible without an opt-in include disclosures made to a public health authority for the purpose of controlling disease and disclosures to a health oversight agency for activities including audits and civil, administrative or criminal proceedings,³³ and disclosures to HHS to determine compliance with the rules.³⁴

³¹ 45 C.F.R. § 164.506(c)(4). In addition, consent is not presumed for any disclosures between two entities for “health care operations” unless both have a relationship with the individual that is the subject of the information. Many carriers and most agents/brokers will not have that relationship.

³² 45 C.F.R. § 164.502(a)(1)(i).

³³ 45 C.F.R. § 164.512.

³⁴ 45 C.F.R. § 164.502(a)(2)(ii).

F. Conditioning Services on Consent

There are two caveats to the presumed consent rules discussed above. First, if an agent/broker elects to seek consent, it must abide by the terms and conditions of the consent document. Second, insurers may be required to obtain consent under a more restrictive State law. (See Section VI). If consent is sought or required, it may condition enrollment in a health plan on the provision of consent, so long as the consent is requested at the time of enrollment.

G. Disclosures Requiring Only An “Opt-Out”

For a limited category of uses and disclosures, an oral request and the individual’s opportunity to object (opt-out) is sufficient. This “opt-out” approach is reserved for uses and disclosures of an individual’s protected health information to family members, relatives or friends, when the information is directly relevant to that person’s involvement in the individual’s care (or payment for care), or would serve to notify those persons of the individual’s location, condition or death.³⁵ In this situation, a covered entity simply must provide verbal notice to the individual of the intended information use or disclosure and the opportunity for the individual to object. If the individual does not object, the information can be used or disclosed for the limited purposes described above. In situations where the individual is not present, or the opportunity to object cannot practically be provided because of the individual’s incapacity or an emergency circumstance, the covered entity may use its own discretion to determine whether the disclosure is in the best interest of the individual.

H. Additional Agreed-Upon Restrictions

Although an individual may request that further restrictions be imposed on his information, a covered entity is never required to agree to the imposition of any additional restrictions. That said, it must adhere to any restrictions to which it has agreed.³⁶ The only caveat is that a covered entity must accommodate reasonable requests by individuals to receive protected information in a confidential manner, or at an alternative location (such as in a sealed envelope). For such a restriction to apply to health plans (or agents/brokers), the individual must demonstrate that the disclosure of the information may endanger him.³⁷

³⁵ 45 C.F.R. § 164.510.

³⁶ 45 C.F.R. § 164.522.

³⁷ 45 C.F.R. § 164.522(b).

IV. COMPLIANCE OPTIONS FOR SHOPPING A PLAN AND ADDING EXCEPTED BENEFITS

There are at least two situations that agents and brokers will face in which consent is not presumed and either an affirmative opt-in will be required or the information to which they have access will be limited. These two situations are:

- (1) In the case of a group health plan fully insured by contracts of insurance – to obtain full claims information from the insurer and use it to add benefits to, amend or replace the plan.
- (2) To use PHI for any activity that does not fall within the definition of “treatment, payment or health care operations,” including placing a contract for an excepted benefit (life insurance, disability insurance or workers compensation) or “marketing” any other product or service to the individual.

A. Replacing/Amending A Fully Insured Group Health Plan

The ability to obtain information necessary to perform functions related to the supplementation or replacement of group health plans, including modifying or amending group plans and soliciting bids from prospective issuers is critical for obtaining a better price and terms for insurance coverage. The HIPAA rules are ambiguous with respect to agents/brokers’ ability to receive full claims information without affirmative authorization from each plan participant. The preamble to the HIPAA rules suggests several options that may be pursued – discussed below – but it is unclear whether these options will prove viable in practice. The main downside to all of the options (except obtaining an authorization) is that none *requires* the carrier in possession of the claims history to disclose the necessary information to the plan or agent/broker.

1. Rely On “Organized Health Care Arrangement” Rules

Agents/brokers can obtain information necessary to shop a fully insured group health plan without an opt-in by relying on the rules governing “organized health care arrangements” (OCHAs).³⁸ With respect to group health plans, an OCHA includes: the plan, the health insurance carrier and any agent, broker or TPA acting on the plan’s behalf. The rules expressly permit entities participating in an OCHA to share PHI in at least one circumstance where consent otherwise would not be presumed – that is, for purposes of carrying out *each other’s* health care operations.³⁹ The rule applies even where these entities do not have a current relationship – such as where a group health plan requires PHI from a former carrier.

³⁸ 67 Fed. Reg. 53,182, 53,217-18 (August 14, 2002).

³⁹ In contrast, consent is presumed for an entity to use or disclose PHI for *its own* health care operations. See Section III.B, above.

To qualify for this special sharing rule applicable to OCHAs, the entities in the arrangement must disclose the nature of their sharing practices in their HIPAA privacy notice. In essence, they must state that they share PHI with each other as necessary to carry out the treatment, payment and health care operations of the OCHA. The notice must identify each entity participating in the arrangement.⁴⁰

2. Use a Stripped Version of the Information

As an alternative to relying on the organized health care rules or seeking an affirmative authorization, agents/brokers have the option of using a more limited set of plan data – data that has been stripped of most personal and demographic information – to obtain replacement coverage or add benefits – that is, if potential replacement insurers are willing and able to price coverage based on such information. The rules identify three types of such limited information, discussed below. The problem with all three types of stripped data is that no one can *require* an insurance company to provide this information to it (in practice, many insurance companies indeed are refusing to turn over such information).

“Summary Health Information.” One alternative is to rely exclusively on “summary health information,” which a plan can request from the insurer that provides its benefits. “Summary health information” means protected health information that – literally – *summarizes* a plan’s claims history, expenses, or types of claims, but with respect to which all individual level data have been removed.⁴¹ This alternative may be a viable solution when the group plan at issue is very large and individual-level claims information is unnecessary.

If individual level data is required, however, the rules permit the assignment of “unique identifiers” – such as numbers from 1 to 100 for each participant in a 100-person plan – to individuals such that individual-level information may be disclosed in a wholly anonymous fashion. That said, agents and brokers – and the plans they represent – do not control the information that they receive from carriers. Thus, they cannot require carriers that formerly insured a group health plan to generate information in an appropriate summary format.⁴²

“Limited Data Set.” The revised rules contain a new method of obtaining data potentially sufficient to “shop a plan.” In order to trigger this rule, the covered entity – in this case an insurance carrier – would have to enter into a “data use” agreement with either the group plan or the plan’s agent/broker/TPA expressly permitting the recipient to use a limited set of information for a particular purpose – such as for shopping for replacement coverage.⁴³ The recipient entity would have to agree to abide by certain conditions (similar to the business associate contract conditions), including using appropriate safeguards to prevent unauthorized

⁴⁰ Covered entities participating in an OCHA may satisfy the notice obligation with a joint notice. *Each entity* must agree to abide by the terms of the notice, and the notice must identify each entity participating in the arrangement.

⁴¹ 45 C.F.R. §§ 164.504; 164.514(b)(2). The “identifiers” that must be removed are the same, broad factors required to “de-identify” information (see below), except that zip code information need only be aggregated to the five-digit zip code (as opposed to the initial three digits as required for de-identification).

⁴² Currently, group health plan data from a carrier is provided in an unmodified format – *i.e.*, via a “data dump” rather than in a format in which that data has been manipulated.

⁴³ 45 C.F.R. § 514(e).

disclosures of information and reporting any unauthorized uses of which it becomes aware. There are two primary downsides to this approach. First, securing these agreements may prove administratively infeasible. Second, carriers cannot be required to enter into these agreements and may resist doing so.

The limited data set to which the contracting party would be entitled would consist of PHI from which the following 16 “identifiers” – of the individual that is the subject of the PHI or of any relatives, employers or household members of the individual – were removed.⁴⁴ Notably, dates of claims and full zip codes remain included in the information.

- (1) Names;
- (2) Street address – but town, State and zip code may remain;
- (3) Telephone numbers;
- (4) Fax numbers;
- (5) Electronic mail addresses;
- (6) Social security numbers;
- (7) Medical record numbers;
- (8) Health plan beneficiary numbers;
- (9) Account numbers;
- (10) Certificate/license numbers;
- (11) Vehicle identifiers and serial numbers, including license plate numbers;
- (12) Device identifiers and serial numbers;
- (13) Web Universal Resource Locators (URLs);
- (14) Internet Protocol (IP) address numbers;
- (15) Biometric identifiers, including finger and voice prints; and
- (16) Full face photographic images and any comparable images.

As in the case of summary health information, individual level data may be obtained through the assignment of unique identifiers that cannot be traced to the individual plan enrollees.

De-identification. A third alternative is to “de-identify” PHI, rendering it wholly unprotected by the rules.⁴⁵ De-identification involves stripping two factors in addition to the 16 listed above. First, in terms of geographic information, only the first three digits of a zip code may be provided. Second, in terms of dates, only the year in which a claim was made may remain. As compared to the limited data set alternative, however, de-identification may present fewer administrative burdens because no data use agreements are required – the information simply must be stripped before it is disclosed to the agent, broker or plan requesting it. As in the case of summary health information, individual level data may be obtained through the assignment of unique identifiers that cannot be traced to the individual plan enrollees. Once PHI has been properly de-identified, it can be used for any purpose because it is no longer information protected by the HIPAA rules.

⁴⁴ Such removal must be done by the covered entity in possession of the information, *i.e.*, the insurance carrier(s) that provides the plan’s benefits.

⁴⁵ 45 C.F.R. § 164.502(d).

3. Obtain an Affirmative Authorization

The third option for complying with the opt-in rules in situations where an opt-in is required is, of course, to obtain an opt-in. There are a number of upsides to this approach, including the following:

- Full compliance with the HIPAA rules is assured.
- An authorization overrides more restrictive state laws.⁴⁶
- Insurance carriers *are not prohibited by any federal or state law or regulation* from providing the requested information if the individual has authorized it.
- The administrative burdens are not unbearable because, going forward, enrollment in the plan can be conditioned on receipt of the authorization. For plans currently in place, however, benefits may be conditioned only on authorizations sought prior to a plan's HIPAA compliance date (prior to April 14, 2003). An authorization may remain valid for the duration of an enrollee's employment unless it is revoked.

Conditional Authorizations. If a group health plan decides to seek authorizations from group plan enrollees, it may make enrollment or the continuation of benefits contingent on the receipt of the authorization if two conditions are met. The authorization must be sought: (1) prior to (or at) enrollment, and (2) only for the purpose of making eligibility, underwriting or risk rating determinations.⁴⁷ Enrollment in a group plan *cannot* be conditioned on an authorization to use or disclose PHI for any other purpose, such as for marketing or to add excepted benefits to the plan.

There is an important caveat to the rule limiting collection of a conditional authorization to time of enrollment – if the authorization is collected before the April 14, 2003 compliance date, the continuation of benefits can be conditioned on execution of the authorization; however, only PHI created or received prior to April 14, 2003 can be disclosed pursuant to such an authorization. The ability to collect such a conditional authorization from current enrollees expires on April 14, 2003.⁴⁸

No Reuse/Redisclosure. The rules impose a reuse/redisclosure limitation on health insurance providers and health plans that receive PHI for the purpose of underwriting, premium rating, or other activities relating to the creation, renewal, or replacement of a contract of health

⁴⁶ For example, carriers would *not* be able to deny access to claims information based on the controversial California laws requiring them to do so if authorizations were collected under which plan participants affirmatively consented to such access.

⁴⁷ This exception *does not* allow a plan to condition enrollment on the receipt of an authorization under which the plan's insurer would disclose protected information to the plan for insurance contract replacement-related purposes. This issue is discussed at length in Section IV.

⁴⁸ 45 C.F.R. 164.532(b) (authorization transition provisions).

insurance or health benefits. If an insurer or plan receives protected information for one of these purposes, and *benefits are not placed with that insurer or plan*, the information that it received cannot be disclosed for any other purpose, except as required by law.⁴⁹

Elements Of A Valid Authorization. An authorization must use specific language to describe the purpose for which it is sought. An authorization cannot be combined with a privacy notice. In general, two authorizations may be contained in the same document,⁵⁰ but a conditional authorization sought for purposes of eligibility, underwriting or risk rating determinations must be presented in a separate document. An authorization must contain certain basic elements, including a description of the information to be used or disclosed that identifies the information, the names of the persons (or types of persons) to whom the covered entity may make the requested use or disclosure, and a statement as to the date or event that will trigger termination of the authorization.

B. Marketing Other Products (Including Contracts For Excepted Benefits)

The general rule is that an authorization is required to use or disclose PHI to market any insurance product or service that the individual did not specifically request; the only question is whether the activity at issue constitutes “marketing.”⁵¹

“Marketing” is defined broadly to include two categories of activities. The first category covers any arrangement between a covered entity and another entity whereby the covered entity discloses PHI to the other entity, in exchange for payment, for the other entity to make a communication about its own product or service that encourages individuals to purchase or use that product or service. In this case, the authorization must expressly state that such remuneration is involved.

The second category is broader and does not require an arrangement between two entities. It includes any communication by a covered entity about a product or service that encourages purchase or use of the product or service. However, there are several key exceptions. Communications made for the following purposes are expressly excluded from the definition of “marketing:”

- (1) To describe a health-related product or service (or payment for the product or service) that is provided by, or included in a plan of benefits, of the entity making the communication, including communications about:
 - The entities participating in a health care provider network or health plan network;
 - Replacement of or enhancements to a health plan; and

⁴⁹ 45 C.F.R. § 164.514(g).

⁵⁰ Documents that create “compound authorizations” (where it is unclear what the individual is authorizing) are prohibited.

⁵¹ 45 C.F.R. § 164.501.

- Health-related products or services available only to a health plan enrollee that add value to but are not part of a plan of benefits.
- (2) For treatment of the individual; or
 - (3) For case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers or settings of care to the individual.

An affirmative authorization is required for a covered entity to obtain, use and disclose PHI for any communication that constitutes “marketing.” Using PHI to secure a contract for excepted benefits – such as life insurance or disability insurance – fits into this category and thus requires affirmative authorization. There are two narrow exceptions where an authorization is not required:

- In face to face communications with the individual; or
- For promotional gifts of nominal value.⁵²

V. COMPLIANCE RULES FOR “BUSINESS ASSOCIATES”

As noted above, the rules impose obligations on “business associates” that receive protected information from or on behalf of covered entities, and to covered entities that disclose protected information directly or indirectly to “business associates.” The primary obligation is the requirement that a valid confidentiality-like agreement be in place between the business associate and the covered entity to ensure protection of PHI by contract. In terms of the other compliance obligations (notice, opt-in, access, and administrative requirements), business associate rules constitute a second layer of regulations – they do not supersede or displace the rules that are generally applicable to covered entities.

A. Notice Requirements

The general rule is that business associates that are not covered entities – *e.g.*, lawyers or accountants – need not provide or maintain HIPAA privacy policy notices. The benefit of this exception is not as meaningful for insurance agents and brokers, because they must provide GLBA notices to all of their customers regardless. Because the two notices (GLBA and HIPAA) can be combined in the same document (*see* Appendix 1), the costs associated with compliance as a covered entity (versus solely as a business associate) are outweighed by the benefits – ensuring full compliance with the rules.⁵³

⁵² 45 C.F.R. § 164.508(a)(3).

⁵³ If an agent and health insurance carrier are legally separate entities but subject to common ownership or, moreover, control, they may designate themselves as “affiliated covered entities” and provide only one notice. Common control exists if an entity has the power to influence or direct the actions or policies of another entity. Common ownership exists if an entity or entities possess an ownership or equity interest of 5 percent or more in

B. Using and Disclosing PHI

The primary significance of the business associate rules is their impact on the use and disclosure requirements. Covered entities may disclose protected information to their business associates (and business associates may receive information from another party on the covered entity's behalf) without an opt-in, as long as a valid "business associate contract" is in place. This contract essentially protects the information exchanged between the covered entity and third party business associates from unauthorized uses or disclosures and dictates that all limitations that apply to the covered entity's uses and disclosures also apply to the business associate.

C. Access Requirements

Whether an entity is covered directly by the rules or only by virtue of the business associate contract does not matter in terms of the access requirements because a covered entity's obligation to provide access extends to any PHI that is maintained by its business associates. Under the terms of the business associate contract, the business associate must agree to comply with the same access obligations that the HIPAA rules impose. Accordingly, insurance agents and brokers will be required to comply with the full array of access requirements whether or not they consider themselves covered directly by the rules.

D. Administrative Requirements

The same principles that apply to the notice requirements apply to the administrative requirements. Business associates that are not covered entities need not comply with these requirements; however, business associates will be required by contract to discharge other – albeit more limited – administrative obligations, such as having policies and procedures in place to ensure compliance with the applicable requirements; making its records available to HHS for inspection; and returning or destroying all PHI that it has received at the termination of its relationship with the covered entity.

E. Requirements for Valid Business Associate Contracts

In general, the contract must state that the business associate will:

- (1) Not use or further disclose PHI other than as permitted or required by the contract or as required by law, and use safeguards to prevent any other uses or disclosures;
- (2) Ensure that any subcontractors to whom it provides PHI agree to the same restrictions and conditions that apply to the business associate, and report to the covered entity any use or disclosure of the information not provided for by its contract of which it becomes aware;

another entity. 45 C.F.R. § 164.504(d)(1). Non-affiliated covered entities also may provide a single notice under the "joint notice" provisions discussed in Section II.A.

- (3) Make protected health information available in accordance with the HIPAA access requirements, incorporate any necessary amendments, and provide an accounting of disclosures if requested;
- (4) Make available to HHS its internal practices, books, and records relating to the use and disclosure of the protected health information that it has received from the covered entity, or that it has created or received on behalf of the covered entity, for purposes of determining the covered entity's compliance; and
- (5) Return or destroy at the termination of the business associate contract all protected health information that it has received from the covered entity, or that it has created or received on behalf of the covered entity, that the business associate still maintains in any form.

In addition, the contract must authorize termination if the covered entity determines that the business associate has violated a material term of the contract. A covered entity violates the rules if it has actual knowledge of a pattern or practice of the business associate that constitutes a material breach or violation of the associate's obligation under the contract, unless the covered entity takes reasonable steps to cure the breach or end the violation.

VI. RELATIONSHIP TO GLBA AND STATE LAW

A. HIPAA Regulations Generally Preempt State Health Privacy Laws

In terms of their effect on state health privacy laws, the HIPAA regulations create a federal floor of privacy protection. This means that the HIPAA rules preempt state health privacy laws that do not provide at least as much protection. Conversely, they do not supersede state privacy laws that provide a greater degree of protection. There are few limited exceptions. The rules do not preempt certain enumerated categories of state laws, such as laws pertaining to health care fraud or abuse, controlled substances, reporting on health care delivery, and reporting of diseases, injuries, births, deaths and child abuse. The rules also contain a catchall exception for state laws that serve a compelling need related to public health, safety or welfare and for which the Secretary finds that the need outweighs the intrusion of privacy.

The rules contain a mechanism for requesting an exception to federal preemption. Anyone may obtain an exception to federal preemption by following certain procedures outlined in the rules. Requests must be submitted in writing to the Secretary of HHS and must include, among other things, the specific rule for which the exception is requested, the effect of the exception, and an analysis of how the State law is more stringent. If granted, an exception determination lasts until either the particular federal privacy provision or state law at issue changes or the Secretary revokes the exception based on a finding that the grounds for the

exception no longer exist. An exception determination does nothing to eliminate conflicting state health privacy laws.

B. NAIC/NCOIL Model Acts Govern “Excepted Benefits”

The HIPAA rules govern health information gathered in connection with the sale or servicing of a health plan. Insurers that do not sell health insurance nevertheless are exposed to health information in the course of selling financial products or services. Insurers selling workers’ compensation, life or disability insurance fall into this group. Although these insurance benefits are exempt from HIPAA coverage, they are still financial products or services as defined by the GLBA. Any health information that is collected in conjunction with selling a financial service (including any insurance service) is treated by the GLBA as nonpublic personal financial information.⁵⁴

At the state level, this means that insurers who gather health information while selling non health-insurance products will have to protect that health information in accordance with the NAIC and NCOIL state privacy models, depending on which has been adopted in a particular State. Both models include health information privacy provisions that require agents and brokers to obtain affirmative authorizations (*i.e.*, an opt-in) from individuals before their nonpublic PHI may be shared with any other party essentially for all non-policy purposes. Uses of protected information to amend, replace, add benefits to or administer a group benefits plan are exempted from the NAIC/NCOIL opt-in requirements.⁵⁵

VII. RULES APPLIED TO AGENTS/BROKERS IN THREE SITUATIONS

A. Situation 1: An Agent Selling Individual Health Insurance Policies

1. The Agent Must Comply With All Core Obligations

Any insurance agent or broker that is selling health insurance policies to individuals must comply with the four core HIPAA requirements. As a practical matter, this means that the agent must give all of its health insurance clients a HIPAA privacy notice (that can be combined with – but does not replace – its GLBA notice; a sample is included in Appendix 1), and comply with the rules’ authorization, access and administrative requirements.⁵⁶

⁵⁴ HHS believes that the HIPAA and GLBA regulations do not conflict as applied to members of the insurance industry. Its assertion is based on the fact that no federal agency has jurisdiction to apply or enforce GLBA regulations with respect to members of the insurance industry. This assertion may not be correct as a matter of law and, regardless, HHS admits that there may conflicts at the state level.

⁵⁵ Alternatively, in States that have adopted the NAIC Model GLBA regulations, an agent or broker who is exposed to health information may choose to comply with the HIPAA rules instead of the NAIC model. *See* NAIC Privacy of Consumer Financial and Health Information Regulation Model Act, Section 20.

⁵⁶ Satisfaction of these rules in many cases may be easier than some believe. For example, to the extent an agency does not retain protected information, the access requirements essentially would be meaningless and the administrative requirements can be satisfied simply by instituting a policy to that effect and training agency employees on this policy.

Joint Notice. If the agent qualifies for the “Agent Exception” under the GLBA, it may rely on the HIPAA privacy notice provided by the insurer as long as that notice expressly states that it also covers the agent.

Hybrid Agencies. For a single agency performing both covered and non-covered functions (e.g., selling both health insurance and life insurance), the agency must comply with the HIPAA rules for all of its health insurance customers. It also should designate itself as a “hybrid entity” by placing a document in its files stating which of its activities are covered and which are not (or that are not part of designated covered components of the business); and by ensuring that employees that are performing uncovered activities do not have access to the protected information gathered in connection with its covered activities. (See discussion of “hybrid entities” in Section I.C.)

2. Application of the Opt-In Rule

Payment Functions. No opt-in is required for the agent to use or disclose PHI to carry out payment activities.

Agent Doing Own Premium Rating. No opt-in is required for the agent to use PHI to do its own premium rating because consent is presumed for performance of one’s own “health care operations” (which includes premium rating). If, however, an agent obtains PHI for the purpose of shopping that information around to several companies, which each does its own premium rating, the agent will be required to obtain an opt-in.

Agent Placing Insurance For Only One Company. HIPAA does not require an agent to obtain an opt-in to carry out any policy-related functions that he or she performs on behalf of a single insurance company. (But an opt-in could be required under a more restrictive state law).

Agent Shopping For Coverage Among Several Companies. The agent must obtain an authorization to shop PHI around to multiple companies because the rules do not consider such activity to be an activity for which consent is presumed.

“Marketing” Activities/Excepted Benefits. The agent (or a carrier for which the agent is working exclusively) also must obtain an authorization to perform any functions that do not fall within the definition of treatment, payment or its (or its carrier’s) own health care operations. Such functions include most marketing communications and rating or placing a contract for excepted benefits.

3. Business Associate Contracts With The Insurer

An agent must enter into a business associate contract with an insurer if the agent is acting on the insurer’s behalf in placing or servicing covered benefits. An agent also may want to enter into a business associate contract with a carrier if the agent intends to use PHI obtained for that carrier to place a contract for excepted benefits for that carrier. In this situation, only a single opt-in is required for both to use the information if a business associate contract is in place.

B. Situation 2: A Broker Selling Fully-Insured Group Health Benefits

In this situation, we assume that the broker is selling group health benefits to an employer. The broker may be assisting in the replacement or renewal of the plan, or may be selling the employer an additional benefit to add to the plan. We assume that the benefits are secured by a contract of insurance. We also assume that the broker is *not acting* as a post-sale third party administrator (TPA) of the plan. Self-insured plans and TPAs are discussed in Situation 3.

1. The Plan Is A Separate Legal Entity

The HIPAA rules consider a group plan itself to be a *separate legal entity* – separate from the employer/plan sponsor and separate from the insurance carrier that provides benefits to plan participants. This can be a concept that is difficult to grasp, but it is important in terms of applying the rules to the different entities involved in a group health plan arrangement.

In layperson terms, a group health plan is the package of benefits provided to plan enrollees.⁵⁷ In legal terms, a group health plan is any employee welfare benefit plan (fully or self-insured) to the extent that the plan provides medical care (including items and services paid for as medical care) to employees or their dependents, directly or through insurance, reimbursement or otherwise. The definition encompasses plans with 50 or more participants, *or* plans of any size that are not administered by the employer who established and maintains the plan. Only employer-administered plans with fewer than 50 participants do not meet this definition (self-insured plans with fewer than 50 participants administered by a TPA, for example, *are regulated* under the HIPAA rules).

2. The Broker is *Not* Required to Provide Notice To Plan Participants; However, The Plan May Be Required To Maintain A Notice And The Broker Must Provide A GLBA Notice To the Plan

An individual has a right to receive notice from whomever he or she receives health benefits. To the extent that group health plan enrollees receive benefits through a contract with a health insurer or HMO, *the health insurer or HMO must provide the individual with the privacy notice. The broker in this situation is not required to provide a separate privacy notice to plan participants.* An individual enrolled in a group health plan has a right to notice *either* from the issuer through which he or she receives benefits *or* from the plan. Accordingly, the broker does not owe a separate notice to plan enrollees.

The same general rule applies to the group plan itself – the plan need not provide notice to enrollees as long as it is fully secured by an insurance contract. (If the plan is self-insured, however, it must provide its own notice. *See* Situation 3.) There is one caveat. If a plan creates or receives PHI *in addition to* “summary health information” (defined in Section IV.A) and

⁵⁷ Courts typically find that a “plan, fund or program” exists if a reasonable person can ascertain the intended benefits, a class of beneficiaries, the source of financing and procedures for receiving benefits. *Donovan v. Dillingham*, 688 F.2d 1367, 1373 (11th Cir. 1982)(en banc).

enrollment/disenrollment information (information that an individual is enrolled in or has disenrolled from a plan), the plan itself must maintain its own privacy policy notice and provide that notice to any person upon request.

It is important to remember that the broker still must comply with the GLBA notice obligation, which requires it to provide an annual privacy notice to the plan itself. Nothing in HIPAA alters this obligation or the information that the notice must contain.

3. Application of the Opt-In Rule

Shopping the Plan. In order to evaluate alternative or replacement benefit plans – or “shop a plan” – the broker must be able to obtain, use and share plan enrollees’ claims history. As discussed in Section IV.A, a group health plan (and broker acting on its behalf) has three options when it comes to obtaining information necessary to shop a plan. The plan may:

- (1) Attempt to rely on the rules that permit sharing within organized health care arrangements – as long as its insurer’s privacy notice recognizes the organized health care arrangement and agrees to the information use and disclosure.
- (2) Rely on a version of the information from which identifying factors have been removed, assuming that the information is sufficient to obtain replacement coverage and the entity in possess of the information – the carrier – agrees to provide the information in the stripped format.
- (3) Obtain a conditional authorization from plan enrollees at the time of enrollment that permits the use of claims information for amending benefits or obtaining replacement coverage.

Contracts For Excepted Benefits. The use or disclosure of PHI to place a contract for excepted benefits requires an authorization. However, properly de-identified information may be used for any purpose, including placing a contract for excepted benefits, if in fact that information is sufficient for premium-rating purposes.

Workers’ Compensation Rules. The HIPAA rules do not interfere with an employer or an agent/broker’s ability to obtain PHI necessary to process workers compensation claims; however, they may interfere with the amount of information that a health care provider initially may be willing to disclose. From a health care provider’s perspective, all health information is the same – it is covered by the rules and therefore protected. The “minimum necessary” rule creates a substantial incentive for health care providers to limit the health information that they disclose.

There is no question, however, that HIPAA permits all covered entities to disclose PHI to the extent necessary to comply with workers compensation laws.⁵⁸ In other words, there is nothing in the HIPAA rules that requires claims to be paid if the information necessary to pay or otherwise redress the claim has not been disclosed (from the perspective of the carrier, agent/broker or employer). Benefits thus may be withheld until adequate information is received.

4. The Group Plan Contract With The Carrier

If the group plan would like to take advantage of the organized health care arrangement option, it should ensure that its contract with the carrier requires the carrier to include in the notice it provides to plan participants the following statements:

- (1) The notice is being provided jointly on behalf of both the insurer and the group plan;
- (2) The insurer and the group plan are offering benefits pursuant to an organized health care arrangement; and
- (3) The insurer may provide protected information to the group plan for the group plan to use for its own health care operations.

If the group plan would like to utilize one of the forms of cleansed information that the rules permit (*e.g.*, de-identified information), its contract with the insurer should dictate that the insurer will provide such information in the desired form upon request. In addition, if the group plan would like to share summary health information with the plan sponsor, the insurer's notice (and the plan's notice, if it maintains one) both must include a statement informing plan beneficiaries of this intent.

5. Who Obtains the Opt-In?

In this situation, the broker is a business associate of the group health plan, because the functions that the broker performs – which include servicing, amending and replacing the plan – are performed on the plan's behalf.⁵⁹ If a valid business associate contract is in place between the broker and plan, only one authorization is required for both to be able to use the protected information that they obtain from the carrier. (Otherwise, the plan and the broker would need separate authorizations from plan participants to obtain the same information for the same purpose.)

In Situation 2, the plan is the entity that will seek the authorization and then permit the broker-business associate to use it on the plan's behalf. Although it may seem more logical to assume that the broker represents *the employer* (versus the plan), the HIPAA rules are adamant

⁵⁸ 45 C.F.R. § 164.512(l).

⁵⁹ A broker is not a business associate of the carrier when it shops a plan, because he is not representing any one carrier's interests.

about keeping PHI away from employers in the absence of express authorizations. In order to ensure the broker's access to necessary information from the plan, the business associate contract should state that he or she represents *the plan*, as opposed to the employer or plan sponsor.

6. Conditioning Services on Receipt of Authorization

Services generally cannot be conditioned on the receipt of an authorization. However, a covered entity may make enrollment in a health plan and receipt of benefits contingent on the receipt of an authorization for purposes related to underwriting or premium rating – but not to place a contract for excepted benefits – as long as two conditions are met.

- First, the authorization must be sought prior to enrollment. Authorizations sought after enrollment cannot be conditional.
- Second, the authorization must be specifically for uses and disclosures enabling the agent or insurer to make an eligibility determination relating to the individual, or for its underwriting or risk rating determination. Enrollment cannot be conditioned on an authorization to use or disclose PHI for another purpose, such as for “marketing.”

As discussed in Section IV.A, if an authorization is **collected before the April 14, 2003 compliance date**, the continuation of benefits (to current plan enrollees) can be conditioned on execution of the authorization; however, only PHI created or received prior to April 14, 2003 can be disclosed pursuant to such an authorization. The ability to collect such a conditional authorization from a current plan enrollee expires on April 14, 2003.

7. The Broker Must Comply With Administrative Requirements, But The Group Health Plan Is Exempt

If a group health plan provides benefits solely through a contract of insurance and does not create or receive information in addition to summary health information or information that an individual is a plan participant, then the plan itself is exempt from complying with most of the rules' administrative requirements (*e.g.*, designating a privacy compliance officer).⁶⁰ For those types of group health plans, the issuer of the contract – the carrier – is responsible for complying with the administrative requirements.

The broker, however, must comply with the administrative obligations on its own and is not exempt by the carrier's satisfaction of these obligations for the plan. This means simply that the broker must designate a privacy compliance officer, appoint an individual to handle complaints, and implement safeguards to prevent unintended disclosures of protected health information and to document any complaints received.

⁶⁰ 45 C.F.R. § 164.530(k). The group health plan is not entirely exempt from the documentation requirements. All group plans, regardless of whether they are secured by a contract of insurance, must maintain copies of amended plan documents. 45 C.F.R. § 164.530(k)(2).

8. Both The Broker And The Plan Must Comply With Access Requirements

Unlike the notice and administrative requirements, the access requirements apply to all covered entities and do not contain special rules for group health arrangements. Thus, all covered entities, including the broker and the plan in this situation, must comply. The access rules are not particularly onerous, however, for entities like the broker that do not maintain group plan participants' PHI.

Covered entities must permit an individual to request access to obtain copies of PHI about the individual that is maintained in a "designated record set." (A designated record set includes, at a minimum, a health plan's information regarding enrollment, payment, claims adjudication and any case or medical management records.) If a covered entity does not maintain the information that is the subject of an access request, the covered entity simply must inform the individual where to direct his or her request (if the entity knows where such information may be accessed). Presumably, brokers will not maintain individuals' protected health information, but individuals typically request access to such information from brokers. If and when such requests are made, a broker discharges its access obligations simply by informing individuals of where to direct their requests (assuming that the broker does not have the information).

C. Situation 3: An Agent/Broker Acting As A TPA of A Self-Insured Group Plan

Regardless of size, the self-insured plan or fund at issue in Situation 3 is a "group health plan" subject to the compliance requirements because it is administered by someone other than the employer who established and maintains the plan (*i.e.*, a TPA). As a result, the group health plan rules discussed in Situation 2 generally apply here, but with two important variations specifically applicable to self-insured group health plans:

- A self-insured plan must provide its own notice to enrollees.
- Both the TPA and the plan must comply with access and administrative requirements.

1. The TPA Is A Business Associate Of The Plan

Regardless of whether it is a covered entity,⁶¹ a TPA is a business associate of the plan that it administers. "Plan administration" activities are activities that meet the definition of "payment" or "health care operations" but are not functions to modify, amend, or terminate the plan or solicit bids from prospective issuers. Plan administration functions include billing, claims management, quality assurance, claims processing, auditing, monitoring, and management of carve-out plans (such as vision and dental). Plan administration does not include

⁶¹ If a TPA is not licensed and is not required to be licensed, it is clear that it is *not* a covered entity under the rules.

the performance of any employment-related functions or functions in connection with any other benefits or benefit plans.⁶²

As a result, the TPA and the plan must enter into a business associate contract. In addition, a TPA may contract with its own agents or subcontractors to perform functions on its behalf. For example, the TPA may delegate management of a plan's pharmacy benefits to a third party. In that case, the TPA should have a business associate contract in place with the third party to ensure that the third party adheres to the restrictions and conditions imposed on TPA's own uses or disclosures of PHI.⁶³

2. The Self-Insured Plan Must Provide a Privacy Notice to Enrollees, But The TPA Does Not Owe A Separate Notice To Plan Enrollees

The group health plan notice rules provide that an individual has a right to receive notice from whomever he or she receives health benefits. If an individual enrolled in a group health plan receives benefits through a contract with a health insurer or HMO, the health insurer or HMO (and not the group plan) provides the individual with the privacy notice. If an individual receives health benefits that are *not* secured by an insurance contract – as under a self-insured plan – the plan itself must provide the individual with notice.

In Situation 3, the self-insured plan must provide notice to the plan's enrollees. As a practical matter, the TPA probably will provide and maintain this notice *on behalf of* the self-insured plan, but the TPA is not obligated to provide its own notice to plan enrollees under the rules. Under the GLBA, however, TPAs licensed under State law still must provide an annual privacy notice to *the plan* disclosing their information sharing practices.

TPAs that provide notice on a plan's behalf should be aware that, in addition to the other notice content requirements, a group health plan notice must include a statement indicating that protected information may be disclosed to the plan sponsor. Thus, under HIPAA, a group health plan may not disclose (or permit a health insurance issuer to disclose) any PHI to a plan sponsor unless the group health plan's notice includes this statement. A sample notice a TPA can provide on behalf of a plan is included in Appendix 1.

3. Application of the Opt-In Rule

Stop-Loss Insurance. No affirmative authorization is required for a self-insured plan (or TPA acting on its behalf) to use or disclose PHI for placing, ceding or replacing a contract for reinsurance or stop-loss insurance. (See Section III.B). The only exceptions to this rule are where the covered entity elects to seek consent (*see* Section III.F), or where a more restrictive state law requires it.

Contracts For Excepted Benefits/Marketing. An authorization is required to use or disclose PHI to place contracts for excepted benefits or to conduct any other activity that constitutes "marketing." Even for self-insured plans, these activities are outside of any exception

⁶² 65 Fed. Reg. at 82,508.

⁶³ 65 Fed. Reg. at 82,506.

and beyond the scope of those situations in which no opt-in is required. However, de-identified information, which is unprotected under the rules, may be used or disclosed for any and all purposes.

4. Both the Plan and The TPA Must Comply With the Access and Administrative Requirements

Group health plans are exempt from complying with the rules' administrative requirements only if they provide benefits solely through a contract of insurance and do not create or receive information in addition to summary health information or information that an individual is a plan participant. By its own terms, this exemption does not apply to self-insured plans. Accordingly, the self-insured plan must comply with the rules' administrative requirements, such as designating a privacy compliance officer.

A TPA that is a covered entity under the rules also must be in compliance with the rules' administrative obligations. The TPA's own administrative compliance obligations are separate from and in addition to any administrative compliance obligations it assumes on behalf of the plan. Similarly, both the TPA and the plan are required to comply with the rules' access requirements.

5. Disclosures to Plan Sponsors

A TPA must be aware of and must comply with the special rules governing amendments to plan documents and disclosures to plan sponsors. Because there is no issuer in this situation acting as the plan's fiduciary, the TPA will be responsible for implementing these requirements on the plan's behalf.

6. Standardized Electronic Code Sets

HIPAA's standards for electronic transactions and code sets apply to anyone that enrolls or disenrolls plan participants, processes premium payments or participates in claims processing or administration, including TPAs that perform these functions for group health plans. A discussion of these standards – and a form for filing an extension of the compliance deadline from October 16, 2002 to October 16, 2003 – is included in Appendix 2.

We hope this is helpful.

APPENDIX 1 –
SAMPLE HIPAA/GLBA NOTICE

APPENDIX 1: AGENT AND TPA/PLAN SAMPLE PRIVACY NOTICE

For Agents Selling Individual Health Policies. As discussed in the attached memorandum, HIPAA requires an agent selling individual health insurance policies to give all of its health insurance clients a HIPAA-compliant privacy notice. (See Section VII.A). Providing a HIPAA notice, however, neither supplants nor discharges an agent's GLBA notice requirements. All insurance products – health or otherwise – are considered financial products under the GLBA. Health insurance agents thus should ensure that the notice that they are providing satisfies the requirements of both statutes. The following sample notice satisfies both HIPAA and the GLBA. Additional elements may be required in order to satisfy the requirements of a more restrictive state law or if you are posting this notice on a web site.

For TPAs Providing Notice on Behalf of Self-Insured Plan. A self-insured plan also must provide a HIPAA-compliant privacy notice to all plan enrollees. A TPA of a self-insured plan probably will assume this responsibility on behalf of the plan. (See Section VII.C in the attached Guide). With the addition of one statement regarding disclosures to plan sponsors, and one statement regarding placing contracts for reinsurance, the following notice also may be used to satisfy HIPAA's notice requirements for a self-insured plan. We have inserted placeholders for these statements in the fourth paragraph of the sample notice. Additional elements may be required in order to satisfy the requirements of a more restrictive state law or if you are posting this notice on a web site.

PRIVACY NOTICE

This notice is in effect as of [insert date].

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

1. Statement of Our Duties

We are required by law to maintain the privacy of your personal health information and to provide you with this notice of our privacy practices and legal duties. We are required to abide by the terms of this notice. We reserve the right to change the terms of this notice and to make any new provisions effective to all of the personal health information that we maintain about you. If we revise this notice, we will provide you with a revised notice by mail.

2. Statement of Your Rights

You have a right to know how we may use or disclose your personal health information. This notice informs you of those uses and disclosures. There are certain uses and disclosures of your personal health information that we are permitted or required to make by law without your permission. For all other uses and disclosures, we first must obtain your permission. In addition, you have the following rights:

- The right to request that we place additional restrictions on our uses and disclosures of your personal health information. However, we are not obligated to agree to impose any such additional restrictions.
- The right to access, inspect and copy the protected information pertaining to you that we maintain in our files about you, and the right to have us correct or amend any information that we create in error. Requests to access or amend your health information should be sent to the contact person and address provided in paragraph 6.
- The right to receive an accounting of the disclosures of your personal health information that we make for purposes other than activities related to your treatment, or our payment functions or other health care operations.
- The right to request that you receive communications of personal health information in a confidential manner.
- *[If you provide this notice electronically, you must also include this statement: “The right to obtain a paper copy of this notice from us on request.”]*

3. Information We Collect About You

We collect the following categories of information about you from the following sources:

- Information that we obtain directly from you, in conversations or on applications or other forms that you fill out.
- Information that we obtain as a result of our transactions with you.
- Information that we obtain from your medical records or from medical professionals.
- Information that we obtain from other entities, such as health care providers or other insurance companies, in order to service your policy or carry out other insurance-related needs.

4. Permissible Uses and Disclosures of Protected Information

- **To Carry Out Treatment Functions.** We may use or disclose your health information without your permission for health care providers to provide you with treatment.
- **To Carry Out Payment Functions.** We may use or disclose your health information without your permission to carry out activities relating to reimbursing you for the provision of health care, obtaining premiums, determining coverage, and providing benefits under the policy of insurance that you are purchasing. Such functions may include reviewing health care services with respect to medical necessity, coverage under the policy, appropriateness of care, or justification of charges.
- **To Carry Out Certain Operations Relating To Your Benefit Plan.** We also may use or disclose your protected health information without your permission to carry out certain limited activities relating to your health insurance benefits, including reviewing the competence or qualifications of health care professionals and conducting quality assessment activities. *[If a TPA is providing this notice on behalf of a self-insured plan, it should include in the foregoing list: “placing contracts for stop-loss insurance.”]*
- **In Situations Permitted Or Required By Law.** We also may use or disclose your protected health information without your written permission for other purposes permitted or required by law, including the following *[insert all that apply⁶⁴]*:
 - As authorized by and to the extent necessary to comply with workers compensation or other no-fault laws.

⁶⁴ We recognize that some of these may not apply to insurance providers; however, it is better to be over-inclusive because anything that you do not specify in this section of your notice is something for which you will need affirmative consent or authorization.

- To a health oversight agency for activities including audits or civil, criminal or administrative proceedings.
- To a public health authority for purposes of public health activities (such as to the Food and Drug Administration to report consumer product defects).
- To a law enforcement official for law enforcement purposes or in response to a court order or in the course of any judicial or administrative proceeding.
- To organ procurement organizations, or to other entities for approved research purposes.
- To a government authority, including a social service or protective services agency, authorized to receive reports of abuse, neglect or domestic violence.
- **For Any Purposes To Which You Have Not Objected.**⁶⁵ In certain limited circumstances, we may use or disclose your protected health information after we have given you an opportunity to object and you have not objected. For example, if you do not object, we may use limited information about you to maintain an office directory, to notify family members or any other person identified by you regarding issues directly related to such person’s involvement with your care or payment for that care, or in emergency circumstances.
- **For Purposes For Which We Have Obtained Your Written Permission.** All other uses or disclosures of your protected health information will be made only with your written permission, and any permission that you give us may be revoked by you at any time.
- *[If a TPA is providing this notice on behalf of a self-insured plan, it also must include a paragraph notifying individuals that it may make disclosures of protected information to plan sponsors pursuant to the restrictions imposed on the plan sponsors in the plan documents.]*

5. Complaints About Misuse of Health Information

You may complain either directly to us or to the Secretary of Health and Human Services if you believe that your rights with respect to our protection of your health information have been violated. To file a complaint with us, you may *[insert statement about how the individual may file a complaint with you, such as “by submitting a complaint in writing that includes as many details (such as names and dates) as possible”]*. You will not be retaliated against in any way for filing a complaint.

6. Our Practices Regarding Confidentiality and Security

⁶⁵ This paragraph is optional. If you want to use or disclose protected health information for any of the purposes specified in this paragraph, you should include this disclosure.

We restrict access to nonpublic personal information about you to those employees who need to know that information in order to provide products or services to you. We maintain physical, electronic, and procedural safeguards that comply with federal regulations to guard your nonpublic personal information.

7. Our Policy Regarding Dispute Resolution

Any controversy or claim arising out of or relating to our privacy policy, or the breach thereof, shall be settled by arbitration in accordance with the rules of the American Arbitration Association, and judgment upon the award rendered by the arbitrator(s) may be entered in any court having jurisdiction thereof.

8. Contact Person For Filing Complaint or Obtaining Further Information

[Insert your organization's contact information, including the name or title and telephone number of the person in your organization that you designate to receive complaints about any misuses of health information or to provide further information about any issue mentioned in the notice. While this a requirement under HIPAA but not the GLBA, it may be easier for you and your customers to designate someone in your organization to respond to complaints or inquiries about any of the topics in your notice – regardless of whether they relate to health or financial privacy.]

**APPENDIX 2 –
STANDARDS FOR ELECTRONIC TRANSACTIONS**

APPENDIX 2: STANDARDS FOR ELECTRONIC TRANSACTIONS

In addition to the core HIPAA privacy requirements discussed in the Guide, HHS also has promulgated a second, completely separate set of “Standards For Electronic Transactions” regulations that require all health care providers, health insurance companies, group health plans, and any agent or broker that processes enrollment, premium payment or claims information (including, most prominently, third-party administrators) to conduct such transactions utilizing standardized code sets prescribed by HHS.⁶⁶ These new standards establish standard data content, codes, and formats for submitting electronic claims and for other administrative health care transactions. All health care providers will be able to use the electronic format to bill for their services, and all health insurers and group health plans will be required to accept and utilize these standards to both process such claims and to administer other aspects of health plans.

The compliance deadline for having these code sets fully implemented in order to facilitate electronic data exchanges is October 16, 2002. Except for “small health plans,” any entity required to comply with these rules will receive an automatic one-year extension of this compliance date *provided that* such an extension is requested on or before October 15, 2002, and a proposed plan for achieving compliance before the new October 16, 2003 deadline is submitted with the request. “Small health plans” – any health insurer or group health plan with annual receipts of \$5 million or less – automatically receive such an extension and do not need to file such a request.⁶⁷ **RECEIVING A COMPLIANCE DATE EXTENSION DOES NOT EXTEND THE APRIL, 2003 DATE FOR COMPLIANCE WITH THE HIPAA PRIVACY RULES DISCUSSED IN THE ATTACHED MEMORANDUM.**

This Appendix is divided into two sections. Section 1 briefly outlines the core electronic code sets obligations and explains to whom such obligations apply from the agent/broker perspective. Section 2 provides directions for applying for the compliance date extension.

A copy of the form for filing extensions is available at: www.cms.hhs.gov/hipaa. The form included there is a model only. Covered entities have the option of submitting their own version of a compliance plan that provides equivalent information. The same web site contains additional information on how to file alternative submissions.

SECTION 2: BASIC OBLIGATIONS

Use of the HHS-prescribed code sets is mandated if you are an employer-sponsored group health plan (whether it is fully insured or self insured), a third party administrator of such a plan, or an agent or broker who participates in any of these insurance-related transactions in relation to such a plan.⁶⁸

⁶⁶ See 65 Fed. Reg. 50,312 (August 17, 2000), *codified at* 45 C.F.R. Parts 160 and 162.

⁶⁷ See Administrative Simplification Compliance Act, Pub. L. 107-105, 115 Stat. 1003 (2001).

⁶⁸ Regardless of whether an insurance agent or broker is a “covered entity,” the electronic code set provisions specifically dictate that any entity performing such functions on behalf of a group health care plan or otherwise must agree to comply with these requirements. See 45 C.F.R. § 162.923.

- health care claims processing,
- eligibility inquiries,
- referral certification and authorization,
- health care claim status inquiries,
- enrollment,
- payment and remittance,
- health plan premium payments, and
- coordination of benefits.⁶⁹

These new code set standards primarily affect agents and brokers that function as third party administrators. To the extent that agents and brokers are involved in claims processing, enrolling or disenrolling plan participants, or processing premium payments or in communicating any such information to health care providers or health insurers, they are required to learn, implement, and communicate electronically using these new code sets.

The new electronic transactions and code set standards are aimed at creating a new coding infrastructure to replace the existing health care administrative system. This means that all physicians, hospitals, other practitioners, insurers, and coding professionals will need to learn a new coding vocabulary that differs from the terminology they now use to, for example, enroll plan participants, process participant premium payments, and document medical procedures, medical claims and remittance forms, and fees schedules.

⁶⁹ See 45 C.F.R. §§ 162.1000 (general requirement); 162.1002 (identifying the precise medical data code sets that must be used for the processing of health care claims); 162.1102 (identifying the code sets and procedures that must be used to process health care claims transactions); 162.1202(a) (requiring use of The NCPDP Telecommunication Standard Implementation Guide, Version 5 Release 1, September 1999, and equivalent NCPDP Batch Standard Batch Implementation Guide, Version 1 Release 0, February 1, 1996, to process requests to determine whether a plan enrollee is eligible for a retail benefit); 162.1202(b) (requiring use of ASC X12N 270/271 – Health Care Eligibility Benefit Inquiry and Response, Version 4010, May 2000, Washington Publishing Company, 004010X092 for all other dental or health-related eligibility for benefits inquiries); 162.1302 (identifying the code sets and procedures that must be used in conjunction with requests for an authorization for health care and referrals), 162.1402 (identifying the code sets that must be used in conjunction with inquiries related to the status of a pending health claim); 162.1502 (requiring the use of ASC X12N 834 – Benefit Enrollment and Maintenance, Version 4010, May 2000, Washington Publishing Company, 004010X095 to process enrollments and disenrollments in health plans); 162.1602 (identifying the standards that must be used to process health care payment and remittance advice); 162.1701 (requiring the use of ASC X12N 820 – Payroll Deducted and Other Group Premium Payment for Insurance Products, Version 4010, May 2000, Washington Publishing Company, 004010X061 for processing health plan premium payment transactions); 162.1801 (identifying the standards that must be used to coordinate the payment of benefits). All of the ACS X12N specifications – which will be the specifications with which non-self-insured group health plans (and agents and brokers engaging in these activities on their behalf) primarily will need to comply – can be obtained from the Washington Publishing Company either through its web site (<http://www.wpc-edi.com>) or by contacting the company directly at PMB 161, 5284 Randolph Road, Rockville, Maryland, 20852; telephone 301-949-9740; or fax 301-949-9742. The NCDP standards related to retail drug benefits can be obtained from the National Council for Prescription Drug Programs through its website (<http://www.ncdp.org>) or by contacting NCDP directly at 4201 North 24th Street, Suite 365, Phoenix, Arizona, 85016, telephone 602-957-9105; or fax (602-955-0749). Information regarding the claims processing standards can be obtained through the HHS website (www.hhs.gov).

SECTION 2: OBTAINING AN EXTENSION

II. How to Qualify for an Extension

“Small health plans” – health insurers and group health plans (and their brokers, agents and TPAs) with annual receipts of \$5 million or less – automatically qualify for the extended October 16, 2003 compliance date and need do nothing further to secure that extension. All other entities whose activity’s require compliance with the new electronic code set rules must submit an extension request and a properly completed compliance extension plan **by October 15, 2002**. If this is done, such entity’s will automatically receive the one-year extension. HHS encourages covered entities to submit compliance extension plans electronically using the model compliance plan on the HHS website.⁷⁰ To submit a model compliance plan form electronically, go to <http://www.cms.hhs.gov/hipaa/hipaa2/ASCAForm.asp>. One of the benefits of filing on-line is that HHS will provide an on-line confirmation number as acknowledgement of the extension.⁷¹ HHS, however, also will accept compliance extension plans submitted on paper. If a compliance plan cannot be submitted electronically, it must be printed and mailed to HHS at the following address: Model Compliance Plans, Centers for Medicare and Medicaid Services, P.O. Box 8040, Baltimore, MD 21244-8040.⁷²

II. How to File an Extension

The HHS model compliance extension form requires that compliance plans contain only summary information regarding compliance activities, including: (1) an analysis reflecting the extent to which the covered entity already is, and the reasons why the covered entity is not, in compliance and why an extension thus is necessary; (2) budget, schedule, work plan, and implementation strategy for achieving compliance; (3) planned use of contractors or vendors; (4) assessment of compliance problems; and (5) a timeframe for testing to begin no later than April 16, 2003.⁷³ This required summary information is the same regardless of whether it is provided to HHS electronically using the HHS model compliance extension form, printed and mailed, or using an alternative version of a compliance plan.

Other than the covered entity contact information, almost all of the answers are selected by checking boxes next to the answer choice options provided on the form or by providing target dates by which the specified activities will have been conducted.

A. Covered Entity and Contact Information

1. Name of Covered Entity

⁷⁰ Although, HHS encourages covered entities to submit compliance extension plans electronically using the model compliance plan, covered entities have the option of submitting their own version of a compliance plan that provides equivalent information, rather than use the HHS model compliance form.

⁷¹ For those filing electronically, the confirmation number will be the only notice of the extension.

⁷² HHS will not acknowledge receipt of paper submissions. For proof of delivery, we suggest you use a U.S. Postal Service return receipt and, of course, obtain a postmark of October 15, 2002.

⁷³ See Health Insurance Reform: Standards for Electronic Transactions; Announcement of the Availability of a Model Compliance Plan, 67 Fed. Reg. 18,216, 18,217 (Dep’t of Health and Human Services April 15, 2002).

If filing for multiple, related covered entities that are operating under a single implementation plan, list their names, tax identification numbers and Medicare identification numbers. Compliance plans for unrelated multiple covered entities or for related covered entities that are not included under the same implementation plan must be filed separately. As a practical matter, a non-self-insured group health plan probably will find it necessary to file an individual request unless it is jointly operated with another plan or if another plan is related to the same employer family. A broker processing an extension request on behalf of its clients therefore probably will need to submit a separate request for each client. Theoretically, a TPA may be able to take advantage of the single filing for “multiple related covered entities that are operating under a single implementation plan” if the TPA is going to oversee the implementation plan for all of its clients. The term “related covered entities” is not defined, however, making it unclear whether this is permissible. The safer course would be to have each client submit a separate request (or submit it on their behalf) unless two or more plans are jointly operated or are related to the same employer family.

2. Tax Identification Number

Indicate each responding covered entity’s IRS Employer Identification Number (“EIN”). If there is no EIN, enter the covered entity’s social security number.

3. Medicare Identification Number

Indicate the identification number that applies to each responding covered entity. If the covered entity is not a Medicare provider, it is not necessary to enter any identification number in (3).

4. Type of Covered Entity

Describe the covered entity category that applies to the respondent by checking all boxes that apply.

5. Authorized Person

Provide the name of the person who is authorized to request the extension. This might be the individual physician, business/practice manager, a corporate officer, chief information officer or other individual who is responsible for certifying that the information provided is accurate and correct. If filing for multiple covered entities, the same person must be authorized to request the extension for all listed covered entities. Otherwise, a separate compliance plan must be filed to indicate the authorized person for each respective covered entity.

6. Title of the person(s) identified as an Authorized Person(s).

7. Mailing address of Authorized Person(s).

8. City/State/Zip of Authorized Person(s).

9. Telephone number of Authorized Person(s).

B. Reason(s) an Extension is Necessary (Question 10)

Check all the applicable boxes.

C. Implementation Budget (Question 11)

Provide information regarding the estimated financial impact of HIPAA compliance on the organization.

D. Implementation Strategy (Question 12)

This section inquires about overall awareness of the HIPAA Transactions and Code Set Standards, Operational Assessment, and Development and Testing.

1. Implementation Strategy Phase One (HIPAA Awareness)

To complete the HIPAA Awareness phase, a covered entity must obtain information regarding HIPAA Transactions and Code Set Standards, discuss this information with vendors, and conduct preliminary staff education. If this phase has been completed check the “yes” box and skip to Question 14. If this phase is not completed, check the “no” box, and answer Questions 13 (describing when the organization started or plans to start this activity) and Question 14 (indicating when the organization completed or plans to complete this activity).

2. Implementation Strategy Phase Two (Operational Assessment)

To complete the Operational Assessment phase, a covered entity must inventory the HIPAA gaps in the organization; identify internal implementation issues and develop a plan to address them; and consider and decide whether to use a vendor or other contractor to assist the organization in becoming compliant with the HIPAA Transactions and Code Set Standards. If this phase is completed check the “yes” box for Question 15 and skip to Question 20. If this phase is not completed, check the “no” box and answer questions 16 through 20. Questions 16 through 18 require an indication of the covered entity’s progress for these tasks, and projected/actual start and completion dates for this phase are required in the boxes for Questions 19 and 20.

3. Implementation Strategy Phase Three (Development and Testing)

To complete the Development and Testing phase, a covered entity must finalize development of applicable software and install it; complete staff training on how to use the software; and complete all software and systems training. If this phase is completed check the “yes” box for Question 21 and skip to Question 26. If this phase is not completed, check the “no” box and answer all questions 22 through 26. Show any progress regarding these tasks in Question 22 and 23. Indicate the projected/actual development start dates in Question 24,

projected/actual initial internal software testing date in Question 25, and final testing completion date in Question 26.⁷⁴

Before you submit your compliance plan you may revise your entries by clicking on “Clear Plan.” However, once Questions 1 through 26 are complete you may submit the compliance plan by clicking “Submit Electronically” or print it and follow the above-mentioned instructions for paper submissions.

⁷⁴ *See id.*