



Independent Insurance Agents

Brokers of America, Inc.



OFFICE OF THE GENERAL COUNSEL

HIPAA PRIVACY RULE **EFFECTIVE APRIL 14, 2003** **FREQUENTLY ASKED QUESTIONS AND ANSWERS**

These FAQs are not intended to provide specific advice about individual legal, business or other questions. They were prepared solely as a guide, and are 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 should be sought.

May 26, 2003

1. What are the basics of HIPAA?

The Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) has been called the most important health care legislation since Medicare. HIPAA includes important protections for individuals by governing the use, disclosure and transmission of health care information by health care providers that bill electronically, almost all insurers and health plans, and health care clearinghouses (“Covered Entities”) and third-party entities that do work for them (“Business Associates”).

The heart of HIPAA is the “Privacy Rule.” The goal of the Privacy Rule is laudable -- protect the confidentiality of health care information that can identify individuals (individually identifiable health information or “IIHI”) by limiting its use or disclosure by Covered Entities and others with access to it, and by giving individuals federal rights with respect to their own IIHI (which is called protected health information or “PHI” in the hands of a Covered Entity).

The Privacy Rule provides that PHI can only be used or disclosed by a Covered Entity in connection with the treatment of the individual, payment for either treatment or coverage under a health plan, or some of the Covered Entity’s internal business activities unless the individual has given specific, time limited revocable permission (“authorization”), or as required or permitted by other law. Any other use or disclosure by a Covered Entity violates the law.

NOTE: These Frequently Asked Questions and Answers on the HIPAA Privacy Rule were prepared by the Baltimore office of the law firm of Venable, Baetjer, Civiletti & Howard, LLP at the request of IIABA.

2. *What am I? Am I a Covered Entity?*

As a broker or independent agent, am I a Covered Entity under HIPAA?

It is what you do, not what you call yourself, that determines whether you are directly (i.e., a Covered Entity) or indirectly by contract (a Business Associate) or just indirectly (everybody else) affected by the HIPAA Privacy Rule. Assuming that you are not a health care provider, you could be either a clearinghouse or a health plan, each of which is a Covered Entity. Although the normal activities of a broker or independent agent should not rise to the level needed to become either of these covered entities. As explained below, we do not believe that under normal circumstances a broker or independent agent would be a Covered Entity.

Clearinghouse

Traditional brokerage activities do not amount to the level or type of activity that would make you a health care clearinghouse, but additional or value added services could create a trap for the unwary. A clearinghouse is essentially a translator that takes in health payment information in one format (either paper or electronic) and translates this information into one of the standard electronic transactions that health plans and insurance companies will be required to use after October, 2003. Some of those standard transactions (see *Glossary* for a list of the standard transactions) involve insurer to insurer or employer to insurer communications, including premium payments, eligibility inquiries and enrollment and disenrollment information.

A Covered Entity must use the standard transactions when communicating electronically with another Covered Entity. However, since you are not a Covered Entity, you will not be required to use the standard transactions in your dealings. It is possible, however, that insurers eventually will want to use the standard formats with everyone. If you engage in any of the standard transactions on behalf of your clients, do not transform the data into or from a standard electronic format. You can receive and send information that does not meet the standard format at either end, or receive and send standardized electronic transactions without becoming a clearinghouse. If, however, you receive data in one format and send it out in the standard electronic format, or vice versa, you will be deemed a clearinghouse and therefore subject to most of the requirements of the Privacy Rule¹.

Health Plan

You are a Covered Entity if you, alone or in connection with others, act as a “health plan”. A health plan “means an individual or group plan that provides, or pays the cost of, medical care”. 42 USC 1320d(5); 45 CFR 160.103. While you could engage in activities that would make you into a (probably unlicensed) health plan, we expect that your normal activities of arranging for individuals or commercial enterprises to obtain health plan coverage in one form or another would not rise to the level of a “health plan.” The statute lists 16 specific types of health plans and the regulations add one catch-all category. All of the listed health plans clearly and logically “provide or pay the cost of” medical care. Applying logic and the definition of

NOTE: These Frequently Asked Questions and Answers on the HIPAA Privacy Rule were prepared by the Baltimore office of the law firm of Venable, Baetjer, Civiletti & Howard, LLP at the request of IIABA.

health plan, you are not a health plan when you arrange for one entity to purchase health insurance from an insurer or other health plan.

However, some concern has been voiced because the statute and regulations refer to the definition of “health insurance issuer” from other parts of HIPAA, which defines issuer to mean “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. Such term does not include a group health plan”. Most of you are licensed as brokers or agents under your state’s insurance law. HIPAA does not define the “business of insurance” and does not otherwise discuss the role of agent or broker in any of the many hundreds of pages in the various preambles to HIPAA. We note that third party administrators fall within the same definition in many states, and the Privacy Rule preamble generally discusses third party administrators as business associates, not health plans. In the absence of any indication that HIPAA intended to enumerate insurance brokers and agents as if they were the health plans they sell to third parties, we do not believe that you will be regarded as a health plan, or a Covered Entity, when you engage in your normal business activities. You do not act as a plan that provides or pays the cost of medical care, and should not fall within the definition of a health plan. Absent extraordinary circumstances, you are not a Covered Entity.

3. *Am I a Business Associate of a Covered Entity?*

These are really two different questions. The first question is to determine whether you act as a business associate of a company or individual when you assist them in obtaining health care coverage. The second is whether you act as a business associate of the insurer that provides the coverage. If you are employed by an insurance company that offers health insurance, you are a member of the workforce of a Covered Entity and not a business associate. *[As used in this memo, health insurance includes health, dental, vision, long term care, medical savings accounts and similar types of insurance. It does not include workers compensation, life, disability, automobile, casualty or similar insurance. See Question 7.]*

What is a business associate?

A “business associate” is a person or entity that performs certain functions or activities that involve the use or disclosure of individually identifiable health information on behalf of, or to provide services to, a Covered Entityⁱⁱ. Therefore, each of the following requirements must be present to make you a business associate and trigger the requirement of a business associate agreement:

1. The party you contract with must be a Covered Entity under HIPAA. Individuals, employers and plan sponsors are not covered entities when they purchase or obtain health insurance, although the health plan the employer sponsors or funds is. Insurers and HMOs and group health plans are all covered entities;
2. You must receive or create individually identifiable health information (IIHI);
3. You must receive, create or use the IIHI in the course of doing something for the Covered Entity. If you receive the protected health information to do something on your own behalf, you are not a business associate; or

NOTE: These Frequently Asked Questions and Answers on the HIPAA Privacy Rule were prepared by the Baltimore office of the law firm of Venable, Baetjer, Civiletti & Howard, LLP at the request of IIABA.

4. You must be providing one of the specified servicesⁱⁱⁱ and the Covered Entity discloses IIHI to you in order for you to provide the services.

Am I a business associate of an individual when I arrange for them to buy health insurance?

NO, because an individual is not a Covered Entity.

Am I a business associate of a company when I represent it to buy health insurance?

PROBABLY, IF you receive IIHI from or on behalf of the company and use it to negotiate the price of the health insurance, or to design it, or otherwise act on their behalf in any situation that involves your receipt of IIHI either from them or from someone else acting on their behalf.

NO, IF you do not receive such information. If you use information that does not reach the level of IIHI, you should not be considered to be a business associate. For instance, IIHI can be “de-identified”, in which case it is not IIHI and your receipt of that information will not make you a business associate. You may receive *summary health information*^{iv}, in which case it still may be IIHI (depending on the level of detail) and you would be considered a business associate if you received it from them or from some other business associate of theirs.

One of the most difficult concepts in HIPAA is the difference between an employer or plan sponsor (which is not a Covered Entity) and the plan they sponsor (which is). If all of your dealings and transactions are with or on behalf of the employer/plan sponsor, a business associate agreement should not be required because the employer/plan sponsor is not a Covered Entity.

Am I a business associate of the insurer when I sell their product?

YES, if you receive or use IIHI in the course of your representation. The “Frequently Asked Questions” released in December 2002 by the Office of Civil Rights (OCR) describe the circumstance of an agent representing an insurer, and describe the agent as the insurer’s business associate, in describing the new marketing rules. However, if you do not receive IIHI, you are not a business associate. Please keep in mind that the definition of IIHI is quite expansive, and it includes most summary health information.

4. *What is the difference in compliance obligations between a business associate and a Covered Entity?*

A Covered Entity is subject to HIPAA. If you are a Covered Entity, by April 14, 2003, you must:

- Develop, post and distribute a Notice of Privacy Practices (“Notice”) that describes what you will do with IIHI and informs individuals about their rights under HIPAA. The method and timing of distribution varies with the type of Covered Entity.
- Appoint your Privacy Officer.

NOTE: These Frequently Asked Questions and Answers on the HIPAA Privacy Rule were prepared by the Baltimore office of the law firm of Venable, Baetjer, Civiletti & Howard, LLP at the request of IIABA.

- Develop policies and procedures regulating your use and disclosure of PHI, and identifying by job description permitted internal and external uses and flow of PHI.
- Identify and train your workforce members, including unpaid volunteers, with access to PHI.
- Establish a complaint procedure for individuals.
- Establish and enforce a sanction procedure for violations.
- Implement reasonable technical and physical safeguards for PHI in your possession or under your control.
- Establish document retention procedures (everything needs to be kept for six years).
- Secure patient records containing PHI so that they are not readily available to those who do not need them, and adopt policies to guard against having your work force request, use or disclose more than the minimally necessary information needed to accomplish the task for which the PHI is requested, used or disclosed.
- Honor the individual's new federal rights to inspect, request an amendment to, and obtain an accounting of unauthorized disclosures of, their own PHI.
- Identify all of, and review/amend/establish written contracts with, your Business Associates to make them protect PHI in their possession. The government provided a model contract that you can use.
- If you sponsor a health plan, and want more than very limited PHI from your health plan, you must amend your Plan to permit and protect such disclosures

A Covered Entity is also liable for its violations of HIPAA. However, a Covered Entity is not liable for the HIPAA violations of its Business Associates, as long as it has a business associate agreement in place and honors its terms. That agreement requires it to terminate the agreement of a non-compliant business associate, or refuse to send any PHI to any entity that does not sign as Business Associate agreement.

A Business Associate is not subject to HIPAA, and therefore has only those obligations it assumes under its Business Associate agreement. For instance, a business associate does not have to have a Notice of Privacy Practices, appoint a Privacy Officer, or adopt policies and procedures. It must take reasonable steps to protect the confidentiality of any PHI in its possession and agree not to disclose any information in a manner not permitted by the agreement. It must also ensure that it can live up to the particular terms of the agreement. The model agreement is posted on the website of the Department of Health and Human Services ("HHS") Office of Civil Rights ("OCR"), which enforces the Privacy Rule (<http://www.os.dhhs.gov/ocr/hipaa/contractprov.html>). OCR described the difference in the following terms:

The HIPAA Privacy Rule does not "pass through" its requirements to business associates or otherwise cause business associates to comply with the terms of the Rule. The assurances that covered entities must obtain prior to disclosing protected health information to business associates create a set of contractual obligations far narrower than the provisions of the Rule, to protect information generally and help the Covered Entity comply with its obligations under the Rule.

Business associates, however, are not subject to the requirements of the Privacy Rule, and the Secretary cannot impose civil monetary penalties on a business associate for breach

NOTE: These Frequently Asked Questions and Answers on the HIPAA Privacy Rule were prepared by the Baltimore office of the law firm of Venable, Baetjer, Civiletti & Howard, LLP at the request of IIBA.

of its business associate contract with the *Covered Entity*, unless the business associate is itself a Covered Entity. For example, covered entities do not need to ask their business associates to agree to appoint a privacy officer, or develop policies and procedures for use and disclosure of protected health information.

The business associate agreement is a contract, and the business associate may be liable to the Covered Entity for any violations under contract law even though it is not subject to civil penalties under HIPAA. Pay close attention to contract provisions that are not required by HIPAA, but may be added by covered entities. These include indemnity provisions, audit and inspection provisions (other than the right of the Secretary of Health and Human Services to investigate a complaint), the imposition of the obligation to respond to individuals (unless their IIHI is in your possession), and unusual or unilateral mitigation provisions. We strongly recommend that you include a no third party beneficiary clause as well to limit the chance that individuals will bring actions alleging that you have violated the terms of a contract intended to benefit them.

5. *Will an agency's E&O policy cover any HIPAA exposures in connection with a Business Associate Agreement?*

We suspect that you will be sent a business associate agreement that contains an indemnity provision (not required) and a mitigation provision (required). Many E & O policies contain a provision that excludes from coverage contractually assumed obligations. We encourage you to discuss with your insurer whether, or when, indemnity provisions will be deemed to fall within this exclusion. Many insurers may take the position that indemnities that increase liability, or only work in one direction, may trigger the exclusion. Remember, the indemnity will not just reduce your coverage – if it applies, your coverage for other acts will remain intact, but your indemnity obligation under the Business Associate agreement may not be covered at all.

6. *How is an employer different from a health plan?*

As noted above, an employer is not a Covered Entity. IIHI contained in employment records, including Family and Medical Leave Act records, workers compensation records or disability records, is not subject to HIPAA. However, if the employer offers health (including dental, vision, flexible savings accounts and employee assistance programs) insurance to its employees, the Plan (whether fully or self insured) is a Covered Entity. Most plans (even ERISA self insured plans) have no employees and are little more than a legal fiction. Therefore, in any dealings with an employer on behalf of its health plans for its employees, take care in articulating which entity you are dealing with.

7. *What are the obligations of each?*

The employer has no direct obligations under HIPAA (although other laws protect much of the same type of information in its hands). The Plan has all of the obligations of a Covered Entity. We note that employers who provide coverage through a fully insured health product can substantially reduce their HIPAA obligations compared to self-insured plans (usually managed

NOTE: These Frequently Asked Questions and Answers on the HIPAA Privacy Rule were prepared by the Baltimore office of the law firm of Venable, Baetjer, Civiletti & Howard, LLP at the request of IIABA.

by a third party administrator). A Plan is not subject to many of the costly Privacy Rule standards if it i) provides health benefits solely through an insurance contract(s) with a health insurance issuer or HMO, and ii) does not create or receive IIIHI other than “summary health information” to determine pricing or coverage, or information as to whether an individual participates in the Plan.

To receive any IIIHI other than listed above from its Plan (whether fully or self insured), the employer must amend its Plan documents to:

- Describe the permitted uses and disclosures;
- Specify that disclosure is permitted only upon receipt of a certification from the employer that it has amended its Plan and agreed to certain conditions regarding the use and disclosure of PHI;
- Provide adequate firewalls to protect against disclosure;
- Adopt policies and identify and train the classes of employees who will have access to PHI;
- Restrict access solely to the employees identified and only for the functions performed on behalf of the Plan; and
- Provide a mechanism for resolving noncompliance.

8. *What types of IIIHI are subject to HIPAA, what is not?*

IIIHI contained in the employment records of an employer from any source other than its health plan is not subject to HIPAA. IIIHI contained in any of the legislatively excluded types of insurance products (See Question 9) are not subject to HIPAA. Only IIIHI in the possession of a Covered Entity, or in the possession of a Business Associate, is subject to HIPAA. Other laws (federal and state) protect much of the same information, but do not contain the elaborate procedures and limitations found in the Privacy Rule.

9. *What types of insurance are not subject to HIPAA? Is long term care insurance covered?*

HIPAA specifically excludes from the definition of a “health plan” any policy, plan, or program to the extent that it provides, or pays for the cost of, excepted benefits, which are listed in section 2791(c)(1) of the Public Health Service Act, 42 U.S.C. 300gg-91(c)(1). See 45 CFR 160.103. Excepted benefits include any (or any combination thereof) of the following policies, plans or programs:

- Casualty and Property Insurance Liability insurance, including general liability insurance and automobile liability insurance.
- Life insurance policies
- Coverage only for accident, or disability income insurance, or any combination thereof.
- Coverage issued as a supplement to liability insurance.
- Workers’ compensation or similar insurance.
- Automobile medical payment insurance.
- Credit-only insurance.

NOTE: These Frequently Asked Questions and Answers on the HIPAA Privacy Rule were prepared by the Baltimore office of the law firm of Venable, Baetjer, Civiletti & Howard, LLP at the request of IIABA.

- Coverage for on-site medical clinics
- Other similar insurance coverage, under which benefits for medical care are secondary or incidental to other insurance benefits.

Long term care insurance is covered by HIPAA, but a nursing home fixed indemnity policy is not.

These policies may involve IIHI, but the issuers of these policies do not have to comply with HIPAA, and information in their possession (or in yours when you are acting on their behalf) is not subject to HIPAA. Issuers and brokers of excepted policies may be indirectly affected, because you may need information from health care providers who are Covered Entities to underwrite or manage the policies. Since the providers may be subject to HIPAA, they will require an authorization from the individual whose information is sought to disclose it to you. We note that nothing is required when dealing directly with the patient, but many disclosures are made directly to the issuer or broker, and authorizations will be required in those instances. See Question 10.

10. What type of authorization form must life insurance agents use?

HIPAA requires an “authorization” from the person whose IIHI is being disclosed for any disclosure by a Covered Entity (such as a health care provider) that is not otherwise permitted or required by HIPAA. The basic rule is that disclosures for treatment of the individual, payment (including payment activities of the insurer as well as payment to providers) or the Covered Entity’s internal operations do not require authorization, nor do disclosures required by law or made to the individual themselves. Other disclosures (such as by a physician to an insurer in connection with their examination of an individual who is seeking to obtain an insurance policy, including a policy for excluded benefits such as a life insurance or disability policy) will generally require the patient’s authorization. Even if you aren’t a Covered Entity, the physician or health care provider probably is, and they can not release the results of their exam without the individual’s authorization.

If you need such information, you must either get it directly from the individual or get the individual to sign an authorization. The authorization requires more detail than your existing release. A sample authorization is attached.

Generally, a Covered Entity (such as a physician) can not condition treatment or service on signing an authorization. However, that is not the case when the purpose of the physician’s examination of the individual is to apply for excepted insurance, because the physician’s services are rendered specifically to provide the report to a third party. Similarly, the individual normally has the right to withdraw an authorization at any time. That right can not be exercised to deprive an insurer of its right to underwrite or defend a policy.

11. Does HIPAA restrict an agency’s ability to market other products to a customer with health insurance?

Generally, a Covered Entity cannot use IIHI for marketing purposes without the express authorization of the individual. There are exceptions. The OCR has noted that:

NOTE: These Frequently Asked Questions and Answers on the HIPAA Privacy Rule were prepared by the Baltimore office of the law firm of Venable, Baetjer, Civiletti & Howard, LLP at the request of IIABA.

The HIPAA Privacy Rule excludes from the definition of “marketing,” communications about replacements of, or enhancements to, a health plan. Therefore, notices about changes in deductibles, co-pays and types of coverage, such as prescription drugs, are not marketing. Likewise, a notice to a family warning that a student reaching the age of majority on a parental policy will lose coverage, then offering continuation coverage, would not be considered marketing. Nor are special health care policies such as guaranteed issue products and conversion policies considered marketing. Similarly, notices from a health plan about its long term care benefits would not be considered marketing.

However, you should not mail to insureds under a health plan “promotional material about insurance products that are considered to be ‘excepted benefits,’ such as accident only policies. It would likewise be marketing for health plans to describe other lines of insurance, such as life insurance policies. Generally, such communications require authorizations.”

You can, however, describe anything if you are meeting with the individual face to face:

In the specific case of face-to-face encounters, the HIPAA Privacy Rule allows health plans and their business associates to market both health and non-health insurance products to individuals.

In those circumstances in which you are a business associate of a Covered Entity Insurer, your business associate agreement states that you cannot use or disclose IIHI in any manner that would be prohibited if the Covered Entity used or disclosed the IIHI. This would include the prohibition on marketing without authorization. The sale of IIHI to another entity for its marketing efforts is particularly bad, and could lead to stringent penalties. When you are not a business associate, the Privacy Rule does not apply. You will need to distinguish those circumstances subject to HIPAA from those that are not, particularly when the same insurer issues both covered policies (health, dental, vision, etc.) and excepted policies.

12. *Are business associates required to restrict their uses and disclosures to the minimum necessary? May a Covered Entity reasonably rely on a request from a Covered Entity’s business associate as the minimum necessary?*

As noted above, a Covered Entity’s contract with a business associate may not authorize the business associate to use or further disclose the information in a manner that would violate the HIPAA Privacy Rule if done by the Covered Entity. See 45 CFR 164.504(e)(2)(i). Thus, a business associate contract must limit the business associate’s uses and disclosures of, as well as requests for, protected health information to be consistent with the Covered Entity’s minimum necessary policies and procedures. If you are acting as a business associate, you can only request, use or disclose the minimum IIHI necessary to do the task at hand. A Covered Entity is permitted to reasonably rely on requests from a business associate of another Covered Entity as the minimum necessary. It is suggested that you conduct some training on this issue if you execute business associate agreements with a Covered Entity, such as an insurer. You could request their minimum necessary policy to serve as a base, particularly if they state in your business associate contract that you must follow their policies.

NOTE: These Frequently Asked Questions and Answers on the HIPAA Privacy Rule were prepared by the Baltimore office of the law firm of Venable, Baetjer, Civiletti & Howard, LLP at the request of IIABA.

13. *Do I have to provide individuals with access to their protected health information or an accounting of disclosures, or an opportunity to amend protected health information?*

YES, if your business associate agreement requires it. The Privacy Rule does not regulate business associates. Covered Entities are responsible for meeting Privacy Rule requirements with respect to individual rights, including the rights of access, amendment, and accounting (45 CFR 164.524, 164.526, and 164-528). With limited exceptions, a Covered Entity is required to provide an individual access to his or her protected health information in a designated record set. This includes information in a “designated record set” of a business associate, unless the information held by the business associate merely duplicates the information maintained by the Covered Entity. The business associate contract must provide that the business associate will make such PHI available if and when needed by the Covered Entity to provide an individual with access to the information. Review any business associate contract sent to you to see if it requires you to provide access directly to individuals, and if it provides sufficient time to respond to inquiries.

The same analysis applies to the amendment of PHI in your records (or copies) when requested by the Covered Entity. The business associate contract must provide that you will make information available to the Covered Entity in order for it to fulfill its obligation to the individual to provide an accounting. As with access and amendment, the business associate contract that the business associate may require you to provide the accounting directly to individuals, and must be carefully reviewed to ascertain the exact duties you are accepting.

14. *What happens if I don't sign the Business Associate agreement?*

If one is required, the Covered Entity can no longer use your service.

ⁱ A clearinghouse normally does not need to use or distribute a Notice of Privacy Practices, but most of the other requirements imposed on a Covered Entity apply.

ⁱⁱ (1) Except as provided in paragraph (2) of this definition, business associate means, with respect to a Covered Entity, a person who:

(i) On behalf of such covered entity or of an organized health care arrangement (as defined in §164.501 of this subchapter) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, performs, or assists in the performance of:

(A) A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or

(B) Any other function or activity regulated by this subchapter; or

(ii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in §164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of individually identifiable health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.

(2) A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (1)(ii) of this definition to or for such organized health care arrangement, does not, simply through the performance of such function or activity or the provision of such service, become a business associate of other covered entities participating in such organized health care arrangement.

(3) A covered entity may be a business associate of another covered entity.

NOTE: These Frequently Asked Questions and Answers on the HIPAA Privacy Rule were prepared by the Baltimore office of the law firm of Venable, Baetjer, Civiletti & Howard, LLP at the request of IIBA.

ⁱⁱⁱ “legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services”

^{iv} **Summary health information** means information, that may be individually identifiable health information, and

(1) That summarizes the claims history, claims expenses, or type of claims experienced by individuals for whom a plan sponsor has provided health benefits under a group health plan; and

(2) From which the information described at §164.514(b)(2)(i) has been deleted, except that the geographic information described in §164.514(b)(2)(i)(B) need only be aggregated to the level of a five digit zip code.

^v The provision of value-added items or services (VAIS) is a common practice, particularly for managed care organizations.

Under the HIPAA Privacy Rule, communications may qualify under the marketing exception for a communication about a health plan’s plan of benefits, even if the VAIS are not considered plan benefits for the Adjusted Community Rate purposes. To qualify for this exclusion, however, the VAIS must meet two conditions. First, they must be health-related. Therefore, discounts offered by Medicare + Choice or other managed care organizations for eyeglasses may be considered part of the plan’s benefits, whereas discounts to attend movie theaters will not. Second, such items and services must demonstrably “add value” to the plan’s membership and not merely be a pass-through of a discount or item available to the public at large.

HIPAA GLOSSARY

This Glossary presents selected major terms defined in the HIPAA Privacy Rule. Familiarity with these terms will greatly contribute to your overall understanding of the Privacy Rule. In addition, you may refer to the full text of the Privacy Rule and §§160.103, 160.202, and 164.501 for additional defined terms.

Authorization. Authorization is required by the Privacy Rule for uses and disclosures of Protected Health Information not otherwise allowed by the Rule. An Authorization is a detailed document that gives Covered Entities permission to use or disclose Protected Health Information for specified purposes, which are generally other than treatment, payment, or health care operations, or to disclose Protected Health Information to a third party specified by the individual. An Authorization must specify a number of elements, including a description of the Protected Health Information to be used and disclosed, the person authorized to make the use or disclosure, the person to whom the Covered Entity may make the disclosure, an expiration date, and, in some cases, the purpose for which the information may be used or disclosed. With limited exceptions, covered entities may not condition treatment or coverage on the individual providing an Authorization.

Business Associate. A Business Associate is any person or entity that performs certain functions or activities that involve the use or disclosure of Protected Health Information on behalf of, or provides service to, a Covered Entity. Business Associate functions and activities include claims processing or administration, data analysis processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing. Business Associate services include legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, and financial services.

NOTE: These Frequently Asked Questions and Answers on the HIPAA Privacy Rule were prepared by the Baltimore office of the law firm of Venable, Baetjer, Civiletti & Howard, LLP at the request of IIABA.

Business Associate Agreement. The Privacy Rule mandates that covered entities have a Business Associate Agreement with each of their business associates. The Business Associate Agreement must (i) describe the permitted and required uses of Protected Health Information by the business associate, (ii) provide that the business associate will not use or further disclose the Protected Health Information other than as permitted or required by the contract or as required by law, and (iii) require the business associate to use appropriate safeguards to prevent a use or disclosure of the Protected Health Information other than as provided for by the contract.

Contact Officer/Contact Office. The Contact Officer or Contact Office is the person or office that the Covered Entity designates to receive complaints and disseminate information related to the entity's handling of Protected Health Information. The Contact Person or Contact Office can be the organization's Privacy Officer or an entirely different person. Business Associates do not have to have a Contact Officer.

Covered Functions. Covered Functions means those functions of a Covered Entity the performance of which makes the entity a health plan, health care provider, or health care clearinghouse.

Covered Entity. Covered Entity means (1) a health plan, (2) a health care clearinghouse, or (3) a health care provider who transmits any health information in electronic form in connection with a transaction covered by the Privacy Rule.

Designated Record Set. Designated Record Set means a group of records maintained by or for a Covered Entity that is: (i) the medical records and billing records about individuals maintained by or for a covered health care provider; (ii) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (iii) used in whole or in part, by or for the Covered Entity to make decisions about individuals. "Record" means any item, collection, or grouping of information that includes Protected Health Information and is maintained, collected, used, or disseminated by or for a Covered Entity.

Disclosure. Disclosure means the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.

Group Health Plan. Group Health Plan means an employee welfare benefit plan, including insured and self-insured plans, to the extent 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, that: (1) has 50 or more participants; or (2) is administered by an entity other than the employer that established and maintains the plan.

DHHS. DHHS stands for the Department of Health and Human Services.

Electronic Transmissions. Electronic Transmissions include transmissions using all media, even when the transmission is physically moved from one location to another using magnetic tape, disk, or compact disk medial. Transmissions over the Internet, Intranet, leased lines, dial-up lines, private networks are all included. Facsimiles are excluded.

NOTE: These Frequently Asked Questions and Answers on the HIPAA Privacy Rule were prepared by the Baltimore office of the law firm of Venable, Baetjer, Civiletti & Howard, LLP at the request of IIABA.

Health Care. Health Care means care, services, or supplies related to the health of an individual. Health care includes, but is not limited to, the following: (1) preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and (2) sale of dispensing of a drug, device, equipment, or other item in accordance with a prescription.

Health Care Clearinghouse. Health Care Clearinghouse means a public or private entity, including a billing service, repricing company, community health management information system or community health information system, and “value-added” networks and switches, that does either of the following functions: (1) processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction; or (2) receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.

Health Care Component. Health Care Component means a component or combination of components of a hybrid entity designated by the hybrid entity as a Health Care Component.

Health Care Operations. Health Care Operations are certain administrative, financial, legal, and quality improvement activities of a Covered Entity that are necessary to run its business and to support the core functions of treatment and payment.

Health Care Provider. Health Care Provider is any individual or organization that furnishes, bills, or is paid for furnishing health care services in the normal course of business.

Health Information. Health Information means any information, whether oral or recorded in any form or medium, that: (1) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (2) related 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.

Health Plan. Health Plan means an individual or group plan that provides, or pays for, medical care. A Health Plan includes a group health plan, a health insurance issuer, an HMO, Medicare, Medicaid, an issuer of a long-term care policy, and an employee welfare benefits plan.

Hybrid Entity. Hybrid Entity means a single legal entity: (1) that is a Covered Entity; (2) whose business activities include both covered and non-covered functions; or (3) that designates health care components.

Individual. Individual means the person who is the subject of Protected Health Information.

NOTE: These Frequently Asked Questions and Answers on the HIPAA Privacy Rule were prepared by the Baltimore office of the law firm of Venable, Baetjer, Civiletti & Howard, LLP at the request of IIABA.

Individually Identifiable Health Information. Individually Identifiable Health Information (“IIHI”) is information that is a subset of health information, including demographic information collected from an individual, and: (1) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) 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 (i) that identifies the individual; or (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Law Enforcement Official. Law Enforcement Official means an officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to: (1) investigate or conduct an official inquiry into a potential violation of law; or (2) prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

Marketing. Marketing means making a communication about a product or service that encourages recipients of the communication to purchase or use the product or service. Generally, if the communication is marketing, then the communication can occur only if the Covered Entity first obtains an individual’s authorization. Face to face communications with the individual and promotional gifts with a nominal value are excluded from the definition of marketing.

Minimum Necessary Standard. The Minimum Necessary Standard requires covered entities to evaluate their practice and enhance protections as needed to limit unnecessary or inappropriate access to Protected Health Information. The HIPAA Privacy Rule requires a Covered Entity to make reasonable efforts to limit use, disclosure of, and requests for Protected Health Information to the Minimum Necessary to accomplish the intended purpose. Disclosures for treatment purposes (including requests for disclosures) between health care providers and disclosures under an Authorization are explicitly exempted from the Minimum Necessary requirements.

Notice of Privacy Practices. The HIPAA Privacy Rule gives individuals a fundamental new right to be informed of the privacy practices of their health plans and of most of their health care providers, as well as to be informed of their privacy rights with respect to their personal health information. Health plans and covered health care providers are required to develop and distribute a Notice of Privacy Practices that provides a clear explanation of these rights and practices. The Notice is intended to focus individuals on privacy issues and concerns, and to prompt them to have discussions with their health plans and health care providers and exercise their rights. Business Associates do not need to have a Notice of Privacy Practices.

Payment. Payment encompasses the various activities of health care providers to obtain payment or be reimbursed for their services and of a health plan to obtain premiums, to fulfill their coverage responsibilities and provide benefits under the plan, and to obtain or provide reimbursement for the provision of health care.

NOTE: These Frequently Asked Questions and Answers on the HIPAA Privacy Rule were prepared by the Baltimore office of the law firm of Venable, Baetjer, Civiletti & Howard, LLP at the request of IIABA.

Privacy Officer. The Privacy Officer is the person designated by the Covered Entity to develop, implement, and oversee the entity's compliance with the HIPAA Privacy Rule. The Privacy Officer may also serve as the entity's Contact Person.

Protected Health Information. Protected Health Information means Individually Identifiable Health Information that is (i) transmitted by electronic media; (ii) maintained in any medium described in the definition of electronic media; or (iii) transmitted or maintained in any other form or medium. Protected Health Information excludes individually identifiable health information in educational records covered by the Family Educational Rights and Privacy Act ("FERPA") and employment records held by a Covered Entity in its role as employer.

Psychotherapy Notes. Psychotherapy Notes means notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record. Psychotherapy Notes excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.

Required By Law. Required By Law means a mandate contained in law that compels an entity to make a use or disclosure of Protected Health Information that is enforceable in a court of law. Required By Law includes, but is not limited to, court orders and court-ordered warrants; subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to health care providers participating in the program; and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.

Secretary. Secretary refers to the Secretary of Health and Human Services or his or her designee.

Small Health Plan. Small Health Plan means a health plan with annual receipts of \$5 million or less.

State Law. State Law means a constitution, statute, regulation, rule, common law, or other State action having the force and effect of law.

TPO. TPO stands for treatment, payment, and health care operations.

Transaction. Transaction means the transmission of information between two parties to carry out financial or administrative activities related to health care. It includes the following types of information transmissions: (1) health care claims or equivalent encounter information; (2) health care payment and remittance advice; (3) coordination of benefits; (4) health care claim status; (5)

NOTE: These Frequently Asked Questions and Answers on the HIPAA Privacy Rule were prepared by the Baltimore office of the law firm of Venable, Baetjer, Civiletti & Howard, LLP at the request of IIABA.

enrollment and disenrollment in a health plan; (6) eligibility for a health plan; (7) health plan premium payments; (8) referral certification and authorization; (9) first report of injury; (10) health claims attachments; and (11) other transactions that the Secretary may prescribe by regulation.

Treatment. Treatment means the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

Use. Use means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

Workforce. Workforce means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a Covered Entity, is under the direct control of such entity, whether or not they are paid by the Covered Entity.

AUTHORIZATION FOR THE USE OR DISCLOSURE OF HEALTH INFORMATION

I hereby voluntarily authorize **[insert name of addressee]** to release my Protected Health Information ("PHI"), as follows:

(Please print clearly and complete all parts of this form. If you do not fill in the form completely, your request will not be processed and the incomplete authorization will be returned to you.)

I. Individual Information

Name: _____
Address: _____

NOTE: These Frequently Asked Questions and Answers on the HIPAA Privacy Rule were prepared by the Baltimore office of the law firm of Venable, Baetjer, Civiletti & Howard, LLP at the request of IIABA.

Phone: _____
SSN#: _____

II. Identification of Person or Organization Receiving Information

My Protected Health Information may be disclosed to the following person(s) or organization(s): *(attach more sheets if necessary)*

Name: _____
Address: _____
Phone: _____

III. Purpose(s) for the Release or Disclosure of Information

Disclosures to be made at the request of the individual

Other *(please specify)*: _____

IV. Description of Information to be Released or Disclosed *(check all appropriate)*

Lab Results

X-Rays

Diagnostic Testing Results

Medical Record

Results of Medical Examination to be used in making underwriting decisions about the individual's application for insurance to cover (specify _____)

Other: *(please specify)* _____

V. Other Important Information

Your signature below means that you understand and agree to the following:

The Protected Health Information provided under this authorization may include diagnosis and treatment information, including information pertaining to chronic diseases, behavioral health conditions, alcohol or substance abuse, communicable diseases (including HIV/AIDS), and/or genetic marker information. These records will be included in the information we will make available to the individual or organization you have identified above.

NOTE: These Frequently Asked Questions and Answers on the HIPAA Privacy Rule were prepared by the Baltimore office of the law firm of Venable, Baetjer, Civiletti & Howard, LLP at the request of IIABA.

The information to be disclosed may be protected by law. Information disclosed under this authorization may be redisclosed by the recipient and no longer protected by federal privacy regulations.

Your ability to receive health care treatment from the Practice will not be affected if you do not sign this form. However, without your signature, your request to release the information described above will not be honored.

You may receive a copy of this form if you ask for it by writing to the address listed at the bottom of this page.

This authorization will expire one year from the date you sign this authorization. If you sign this form, you may revoke the authorization at any time by notifying the Practice in writing at the address below. Revoking this authorization will not have any effect on actions that the Practice took in reliance on the authorization before the Practice received notice of your revocation.

VI. Signature of Individual or Individual's Representative

Signature of Individual or Representative

Date

If this authorization is signed by an individual's representative, the following additional information must be provided:

Name of personal representative (please print)

Relationship to the individual, including authority for status as representative

Return this completed form to the Office identified below in person or by mailing it to:

NOTE: These Frequently Asked Questions and Answers on the HIPAA Privacy Rule were prepared by the Baltimore office of the law firm of Venable, Baetjer, Civiletti & Howard, LLP at the request of IIABA.