

*in this issue*

**from the President**

The Privacy deadline has passed. So, now what? page 2

**Marketing Communications and HIPAA**

What does HIPAA consider Marketing, and how does this affect your business? page 2 & 3

**Business Associate Agreement Instructions**

Visual instructions on filling out your Business Associate Agreements. page 4 & 5

**Q & A**

Do I need a Business Associate Agreement with Small Claims Court? Do providers need to get a Business Associate Agreement from insurance companies? and answers to other questions. page 6 & 7

## Business Associates

### What is a HIPAA Business Associate?

A Business Associate (BA) is any person or organization who is not your employee but does work on your behalf and has have access to your Protected Health Information (PHI).

Under the original HIPAA legislation of 1996, Congress granted the Department of Health and Human Services (HHS) the statutory right to regulate the health care industry. HHS could not regulate the financial, legal, computer or any industry other than health care. However, HHS realized that there would be times when a health care provider, in the course of operating their business, would need to share PHI with an outside person or organization. To protect this PHI when it was shared with the outside person or organization, HHS specified that providers would need to get a Business Associate Agreement (contract) with the outside person or organization in order to provide continuity of HIPAA's protection of PHI.

### Who are HIPAA Business Associates?

When you are determining who your Business Associates are, ask yourself the following two questions:

1. Is this person or business performing some function or task on behalf of the practice?
2. Will this person or business have access to the practice's Protected Health Information (PHI) while performing the task or function?

If you answered yes to both questions, then the person or business is a HIPAA Business Associate (BA) of your practice and must be given a Business Associate Agreement (contract) to sign. For example, someone who comes into your practice to work on your computer systems would probably be a BA since they would be

continued on page 7

It's May 2003. The first major deadline of HIPAA has passed. So, now what? As we have stated throughout this process there are no "HIPAA police". And we've also been pretty adamant that HIPAA compliance is NOT a destination but an ongoing process. The absence of an active force ensuring compliance does not lessen the fact that, HIPAA is here to stay.

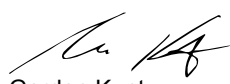
Purchasing Agent 77's HIPAA*Now!* Toolkit is the most important step you have taken toward compliance. We hope you have found our toolkit to be as easy to use as we created it to be. Our toolkit (whether you realize it or not) reduced your compliance effort significantly. If you've waded into the troubled HIPAA waters, you have likely found that it was not as difficult as you had been told or envisioned. Though not a small, insignificant task, your efforts will be rewarded by peace of mind and the knowledge that your patient's privacy is being protected.

Compliance with any law or regulation requires many parts to work together in harmony. One of the keys to HIPAA compliance is the reliance on the cooperation of many others. The preparation and cooperation of your business associates to sign and return your Business Associate agreement is one of those harmonic requirements. Hopefully you have had success at getting your business associates to "feel the pain" and to understand the necessity of your relationship becoming more formalized when it comes to the protection of patient privacy. Losing control over documents is probably the biggest area of concern to a health care provider. A well established Business Associate agreement is your best defense and insurance that your business associates see things as you do when it comes to your patients' privacy.

Agent 77 is here to help you with all-things-HIPAA! We will continue to keep you abreast of any significant changes in the law (like the finalization of the Security regulations in February 2003 and the ultimate enforcement deadline for Security compliance by April 2005). Your purchase of the HIPAA*Now!* Toolkit included a six month trial subscription of our customer support and periodic newsletters (provided as needed to update you on the latest in HIPAA news).

Maybe you received a letter that stated your free subscription was about to expire. Don't get caught off guard. Remember, one of the requirements of HIPAA compliance is that your Privacy Officer stay current on HIPAA related matters. At Agent 77, it is our job to help you stay current and complete on HIPAA issues. Contact us at 1-800-629-6500 or complete the enclosed form to renew your subscription.

Thank you for putting your confidence in Agent 77 as your HIPAA expert! We appreciate you!



Gordon Kuntz  
CEO Agent 77 Inc.

Most of us don't want to be marketed to without our permission, thus the popularity of "do not call" lists and anti-spam filters. Many people are tired of being marketed to by the medical community, especially the drug companies. This is as true for your patients as for the populace at large. HIPAA helps to protect your patients from unwanted marketing.

### **HIPAA Marketing Restrictions in the Privacy Regulations**

Under the HIPAA privacy regulations, marketing is defined: "to make a communication about a product or service that encourages the recipients of the communication or purchase or use the product or service."

HIPAA privacy regulations state you must have the individual's prior written authorization to use or disclose Protected Health Information (PHI) in any marketing communication.

However, HIPAA does give some exceptions to this definition of marketing. These exceptions (described in detail below) include:

- Communications about a patient's treatment. This includes:
  - Case management or care coordination including prescription reminders
  - Directions or recommendations for alternative treatments or therapies
  - Recommending additional treatments at other providers
  - Explaining additional benefits or services available in the patient's provider network
- Health-related products or services offered by the covered entity
- Any face-to-face communications

HIPAA privacy goes on to define marketing as: "An arrangement between a covered entity and any other entity whereby the covered entity discloses protected health information to the other entity, in exchange for direct or indirect remuneration, for the other entity or its affiliate to make a communication about its own product or service that encourages recipients of the communication to purchase or use that product or service."

This part of the definition to marketing has no exceptions. The individual must authorize these marketing

# and HIPAA

communications before they can occur. This means that the provider cannot sell patient lists to another company for the other companies' marketing efforts. Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party's own purposes. Moreover, covered entities may not sell lists of patients or enrollees to third parties without obtaining authorization from each person on the list.

## Exceptions to the HIPAA Privacy Marketing Regulations

### For Treatment:

It is not marketing for a doctor to make a prescription refill reminder even if a third party pays for the communication, as the prescription refill reminder is considered treatment. Similarly, it is not marketing when a doctor or pharmacy is paid to recommend an alternative medication to patients. Communications about alternative treatments are excluded from marketing. The simple receipt of remuneration does not transform a treatment communication into a commercial promotion of a product or service.

Furthermore, covered entities may use a legitimate business associate to assist them in making such permissible communications. For instance, if a pharmacist has been paid by a third party uses a mail house to send out prescription refill reminders to the pharmacist's patients, neither the mail house nor the pharmacist needs a prior authorization.

HIPAA privacy also allows covered entities to distribute items commonly known as promotional gifts of nominal value without prior authorization, even if such items are distributed with the intent of encouraging the receiver to buy the products or services. This exception generally applies to items and services of a third party, whether or not they are health-related, or items and services of the covered entity that are not health-related. A covered doctor, for instance, may send patients items such as pens, note-pads, and cups embossed with a health plan's logo without prior authorization. Similarly, dentists may give patients free toothbrushes, floss and toothpaste.

Treatment exceptions also include recommending a patient to a specialist for additional treatment.

For example, a dentist may refer a patient to a specialist for additional treatment such as orthodontia, or endodontic treatments or a physician may recommend treatments to a specialist, even specialists not in the physician's network.

## For Health-Related Products or Services Offered by the Covered Entity

The HIPAA Privacy Rule excludes communications made to describe a covered entity's health-related product or service (or payment for such product or service) provided by the covered entity, or included in a plan of benefits. Thus, it would not be marketing for a physician who has developed a new anti-snore device to send a flyer describing it to all of her patients. Nor would it be marketing for an ophthalmologist to send existing patients or members discounts for eye-exams or eye-glasses. Similarly, it would not be marketing for a dentist to let patients know about teeth whitening or other services they offer.

However, it would be considered marketing for a provider to make communication about a non-health-related product or service, unless that communication was made face-to-face in the provider's office.

## In Face-To-Face Communications

In face-to-face encounters, the HIPAA Privacy Rule allows covered entities to give or discuss products or services, even when not health-related, to patients without a prior authorization. This exception prevents unnecessary intrusion into the doctor-patient relationship. Physicians may give out free pharmaceutical samples, regardless of their value, hospitals may give infant supplies to new mothers, and providers may leave general circulation materials in their offices for patients to pick up during office visits.

# Business Associate Agreement Instructions

BA Business Name  
example: AA Cleaning Service

**BUSINESS ASSOCIATE AGREEMENT**

Date you filled the BA Agreement out

This Business Associate Agreement ( Agreement ) is made effective \_\_\_\_\_, 20\_\_\_\_  
( Effective Date ) by and between \_\_\_\_\_ (the Business Associate ) and  
\_\_\_\_\_ (the Covered Entity ).

Practice Name  
example: John Q DDS

Type of BA  
example: Cleaning Service

WHEREAS, Business Associate is a \_\_\_\_\_ and Covered Entity is a \_\_\_\_\_;

Type of Practice  
example: General Dentist

Prior Annual/Verbal/  
Maintenance  
Contract or Agreement  
If there is no prior agreement, this paragraph can be removed or you can refer to a "Oral" agreement with the BA.

WHEREAS, the parties have a prior \_\_\_\_\_ Agreement dated \_\_\_\_\_ (the "\_\_\_\_ Agreement") under which Business Associate regularly uses and/or discloses Protected Health Information in its performance of the Services described below. This Agreement is intended to serve as an Addendum to the \_\_\_\_\_ Agreement.

WHEREAS, both parties are committed to complying with the Standards for Privacy of Individually Identifiable Health Information (the "Privacy Regulation") and other regulations issued under 45 CFR parts 142 and 160-164 pursuant to the Health Insurance Portability and Accountability Act of 1996 (collectively, "HIPAA").

The parties hereby agrees as follows:

1. **Permitted Uses and Disclosures.**
  - 1.1 Services. Pursuant to the \_\_\_\_\_ Agreement, Business Associate provides services ("Services") for Covered Entity that involve the use and disclosure of Protected Health Information. Except as otherwise specified herein, Business Associate may make any and all uses of Protected Health Information necessary to perform its obligations under the \_\_\_\_\_ Agreement. All other uses not authorized by this Agreement are prohibited.
  - 1.2 Business Activities of Business Associate. Unless otherwise limited herein, Business Associate may disclose the Protected Health Information in its possession to third parties for the purpose of its proper management and administration or to fulfill any present or future legal responsibilities of Business Associate, provided that Business Associate represents to Covered Entity, in writing, that the disclosures are in compliance with HIPAA and any applicable state laws or regulations governing health information.
  - 1.3 Additional Activities of Business Associate. Business Associate may:
    - a. Aggregate the Protected Health Information in its possession with the Protected Health Information of other covered entities that Business Associate has in its possession through its capacity as a business associate with other covered entities provided that the purpose of such aggregation is to provide Covered Entity with data analyses relating to the Health Care Operations of Covered Entity. Under no circumstances may Business Associate disclose Protected Health Information of one Covered Entity to another Covered Entity absent the explicit authorization of Covered Entity.
    - b. De-identify any and all Protected Health Information provided that the de-identification conforms to the requirements of HIPAA and further provided that Covered Entity maintains the documentation required by HIPAA.

Title of Prior Agreement

Prior Annual/Verbal/  
Maintenance  
Contract or Agreement

**2. Use and Disclosure of Protected Health Information**

2.1 Responsibilities of Business Associate. With regard to its use and/or disclosure of Protected Health Information, Business Associate hereby agrees to do the following:

- a. Use and/or disclose the Protected Health Information only as permitted or required by this Agreement or as otherwise required by law.
- b. Report to the designated Privacy Officer of Covered Entity, in writing, any use and/or disclosure of the Protected Health Information that is not permitted or required by this Agreement of which Business Associate becomes aware within 10-20 days of Business Associate's discovery of such unauthorized use and/or disclosure.
- c. Establish procedures for mitigating, to the greatest extent possible, any effects from any improper use and/or disclosure of Protected Health Information that Business Associate reports to Covered Entity.

10-20 days  
whatever you are comfortable with

**7. Miscellaneous.**

Practice Name  
if sole practioner,  
otherwise names of  
the partners

7.1 Covered Entity. For purposes of this Agreement, Covered Entity shall include all entities covered by the joint notice of information practices (or privacy notice), which includes \_\_\_\_\_.

7.2 Business Associate. For purposes of this Agreement, Business Associate shall include the named Business Associate herein. However, in the event that Business Associate is otherwise a covered entity under the Privacy Regulation, that entity may appropriately designate a health care component of the entity, pursuant to HIPAA, as Business Associate for purposes of this Agreement.

7.3 Amendments; Waiver. This Agreement may not be modified, nor shall any provision hereof be waived or amended, except in a writing duly signed by authorized representatives of the Parties. A waiver with respect to one event shall not be construed as continuing, or as a bar to or waiver of any right or remedy as to subsequent events.

IN WITNESS WHEREOF, each of the undersigned has caused this Agreement to be duly executed in its name and on its behalf effective as of \_\_\_\_\_, 20\_\_.

Date you filled the  
BA Agreement out

Your Signature

**COVERED ENTITY**

By: \_\_\_\_\_  
Print Name: \_\_\_\_\_  
Print Title: \_\_\_\_\_  
Address: \_\_\_\_\_  
Date: \_\_\_\_\_

**BUSINESS ASSOCIATE**

By: \_\_\_\_\_  
Print Name: \_\_\_\_\_  
Print Title: \_\_\_\_\_  
Address: \_\_\_\_\_  
Date: \_\_\_\_\_

# Q & A

**Q. Do I need a Business Associate Agreement with Small Claims Court?**

**A.** The Final Privacy Rules permit disclosures of health information without individual authorization for certain national priority activities and for activities that allow the health care system to operate more smoothly. All of these disclosures have been permitted under existing laws and regulations. This includes disclosures for Judicial and administrative law proceedings, such as Small Claims Court. Since these types of disclosures are specifically permitted under HIPAA, you would not need to get a Business Associate agreement with Small Claims Court.

**Q. Do providers need to get a Business Associate Agreement from insurance companies?**

**A.** HIPAA defines a business associate as: “a person or entity who provides certain functions, activities, or services for or to a covered entity, involving the use and/or disclosure of PHI” and who is not a member of the provider’s workforce. Since insurance companies are providing a service to the patient not the provider, they are *not* a business associate.

**Q. We have another dental office in the lower half of our building and he owns part of the building and has a key to our office. Do you recommend he sign a Business Associate Agreement?**

**A.** This dentist/landlord may not actually be a Business Associate (they are not doing anything “on your behalf”), but you need some sort of confidentiality agreement with them. The BA Agreement, while possibly overkill, will certainly cover this situation.

**Q. Is it true that if a practice is in violation of any HIPAA rules, the patient could sue for unlimited damage?**

**A.** There is no provision in the HIPAA law or any subsequent HIPAA regulations that allow patients to sue for damages if they feel that their privacy has been violated. The only penalties written into HIPAA is that the government can levy civil fines against a practice (capped at \$25,000 per year per statute), or for particularly egregious infractions, can level criminal fines as well as jail time. That is not to say that a patient cannot sue a provider under existing state or federal laws. HIPAA is silent on this issue and does not override existing laws. It’s just that there is no provision in HIPAA itself for redress by a patient against a provider other than reporting an infraction to the government for follow-up by a government agency.

**Q. If a Patient has a complaint do they notify us first before the Office for Civil Rights?**

**A.** By statute, a patient has the right to complain to you and/or to the Office for Civil Rights. There is nothing in the regulations that requires the patient to complain to you first. Our recommendation is that if you make it clear to patients that they can come to you with complaints and that you will deal with them fairly, honestly and promptly that they will want to come to you first. Obviously, it would be best for you to be able to resolve the complaint yourself without getting the government involved.

The office of Civil Rights has not yet announced what process they will use to investigate a complaint. We will be sure to inform you in the newsletter as soon as we hear anything on this front.

**Q. Do we have to send providers anything (procedures, NPP, Business Associate Agreement)?**

**A.** Again, the government has made it clear that there should be no barriers to communications for treating the patient. That means that providers with direct or indirect treatment relationships with a patient are not business associates of each other and do not need to send copies of their policies, procedures, NPP or any other form as long as the relationship between the providers is for treating patients.

**Q. Do Notice of Privacy Practices change? How do we keep up with them?**

**A.** Yes. HIPAA is changing and no one can tell exactly what the government and the courts will change for the HIPAA regulations. As the regulations change the NPP may also need to change. You may also want to change your NPP if circumstances change in your business. In either case, you will need to post the new NPP in your practice and you will need to keep a copy of each version of your NPP for six years from last use.

The best way to keep up with changes with the rules and regulations is to keep up your customer service subscription with Agent 77. This will give you regular newsletters with the changes as well as product updates.

**Business Associates** continued from cover

working on your behalf (installing or maintaining your computers) and they would have access to PHI on those computers.

If you answered no to either question, the person or entity is not a BA. For example, insurance companies are not BAs as they are performing a function on behalf of the patient (paying the claim), not for you.

Other examples of Business Associates include attorneys, accountants, temp agencies, business consultants, equipment sales and service vendors, clearing houses, billing services and collection agencies. Again, make sure that the person or organization passes both tests before you consider them a Business Associate. For example, if your accountant only helps you with your quarterly and annual tax preparation and is only looking at summary financial information of your practice, they would not be a BA (they fail test #2 as they do not have access to PHI). On the other hand, if they are acting as a bookkeeper, and are helping with billing or are doing a complete audit of the practice, the accountant would be a BA as they would have access to PHI.

**Contributors:**

Don Kaiser  
Gordon Kuntz  
Rob Silas  
Jeffrey Abramovitz

**Design:**

Phillip Koenig

**Contact Agent 77:**

phone: 651-686-6500  
to order: 1-800-294-2556

info@agent77.com

1120 Centre Pointe Dr. STE 800  
Mendota Heights, MN  
55120



**Tools to make your compliance even easier**

If you want to ensure easy access to our HIPAA experts, use the order form below to renew your support package. Our Staff training CD-Rom and Consulting Services provide additional ways that we can make your compliance efforts more complete and cost effective

**Provider Products**-for Dentists, Doctors, Pharmacists and other providers

**Support Package**

One year of the HIPAANow! Newsletter and unlimited access to our experts to help you with HIPAA

\$240 \_\_\_\_\_

**Staff Training CD-Rom**

A self-guided staff training CD-Rom that satisfies the staff training requirements of HIPAA's privacy and security regulations.

\$175 \_\_\_\_\_

**Health Plan Products**-for organizations with Health Plans that need to be compliant

**Support Package**

One year of the HIPAANow! Newsletter and unlimited access to our experts to help you with HIPAA

\$240 \_\_\_\_\_

**Consulting Services**

Customized services delivered on-site or over the phone to assist with any aspect of your compliance.

call for quote

Sales Tax (MN only) 6.5% \_\_\_\_\_

**payment information**

payment type:  AmEx  VISA  MC  Check

total \_\_\_\_\_

credit card number: \_\_\_\_\_ CID \_\_\_\_\_ expiration: \_\_\_\_/\_\_\_\_

if Billing address is different from shipping, fill out below

name on card: \_\_\_\_\_

business name: \_\_\_\_\_

signature: \_\_\_\_\_

contact name: \_\_\_\_\_

address: \_\_\_\_\_

**Fax form with credit card information to 651-686-6528.**

city: \_\_\_\_\_ state: \_\_\_\_\_ zip: \_\_\_\_\_

**Please make checks payable to Agent 77 and send check and completed form to:**

Agent 77  
1120 Centre Pointe Dr STE 800  
Mendota Heights MN 55120

**ship to:**

