

# Newsletter

## HIPAA Now!

Edition 4, November/December 2002

### **HIPPA and State Law:**

How does HIPAA interact with state law? What about worker's comp cases? What about the rights of minor patients? We let you know how this works and where you can find more information. Pages 4 & 5.

### **Questions & Answers:**

Does our collection agency need to be compliant? How will changes to the privacy rule be made? Our office promotes Oxyfresh products; we give samples and patients can purchase products. Do I need to obtain an authorization for this? With postcard reminder cards for appointments, can the card have the time and date of the appointment? Pages 6 & 7.

### **On Privacy:**

Your patients may request that reminders, test results and other such information be made to an address or location other than the one they list on their medical chart. And where are the Employee Confidentiality Statements? Pages 8 & 9.

### **Quick Tips:**

Getting information on the Privacy Officer is the Quick Tip subject for this month. Page 10.

### **On Security:**

How do you choose difficult to crack passwords that are also easy to remember? Page 11.

# President

## Words From The:

---

Tick, tock, tick, tock.

The HIPAA clock continues to count down the days to compliance on April 14, 2003. With less than 100 days left to go, one New Year's resolution you may want to keep is to get your office HIPAA compliant as quickly as possible. Even if you are just getting started, you can still complete all of your HIPAA activities by spending a few hours every week. As with many other New Year's resolutions, the most important thing is to get started!

Many of you may be wondering what happened to the security regulations. Well, that's a good question. We are all (still) waiting for Health and Human Services to issue the final rules. The latest indication is that the final rules will be issued some time in the first quarter of 2003, but that, as usual, comes with no guarantees. A key thing to remember is that the draft security rules represent solid business practices, and you cannot go wrong by starting to implement these draft regulations as they sit today. When the final rules come out, they are likely to be more specific about technical details, but are not expected to vary widely in the topics covered or the approaches to these issues. We continue to support the draft regulations and will let you know as soon as the rules are final. Once we have completed updating the toolkit, you will receive updated materials with the new information.

As you all know, most states have laws on the books governing patient privacy in that state. HIPAA, for the first time, provides a uniform national set of privacy standards for patient records. In this issue of the newsletter, we review how HIPAA interacts with state law. Since your state probably has extensive laws governing patient privacy and disclosures, and HIPAA is probably different in several respects, this article will help you to understand how to decide which set of rules to follow for your patients.

Also in this issue we provide a range of information sources to help you decide whom you should appoint as your privacy officer. This critically important position will not only help your practice to become HIPAA compliant, but will ensure that you stay compliant and that you handle patient complaints effectively.

By the way, we always appreciate referrals! As the time available for HIPAA compliance draws short, help out your friends by letting them know about Agent 77's HIPAANow! toolkit. You probably know several provider offices that you deal with who aren't yet HIPAA compliant and who could use a hand. Please let them know about your good experiences with the HIPAANow! toolkit – we would love to help them too! We have more than 40 seminars scheduled every month throughout the spring and are sure to have one in an area that can help your friends and associates.



Gordon Kuntz, President, Agent 77

### **Mac Vs. Windows**

We've gotten a few questions about a HIPAA*Now!* CD-ROM for Macs. In fact the HIPAA*Now!* CD-ROM works for both operating systems. For the Workbook and Guide pages, the software requirements remain the same, Microsoft Word or Adobe Acrobat Reader and a web browser are necessary to view the pages. If Mac users would like to view the training, all they need is Windows emulation software.

### **A Product for Your Business Associates**

Agent 77 is working on HIPAA*Now!* BA, a toolkit for your business associates to use to help them to understand HIPAA and their obligations under a business associate agreement. Based on the HIPAA*Now!* Toolkit but designed specifically for business associates, this product will help them to establish their own policies and procedures in support of their contractual obligations, as well as provide training for their staff that may handle PHI, giving you further assurances that they are able to fulfill their contract with you.

You will be receiving detailed information shortly about this product and how your business associates can order it. Please let your business associates know about it.

If you or any of your business associates have questions about what it means to be a business associate, please ask them to call Agent 77 at 651.686.6500 or send an e-mail to BA@agent77.com .

### **Customer Support Packages**

A reminder to those of you whose introductory Customer Support subscriptions are coming to a close: HIPAA is changing and evolving, and the Agent 77 support packages are the best way for you to stay on top of these changes. They bring the most up-to-date information on the law to your desk. There are a number of subscription options, and the best value is the Combination Subscription, which gives you a toll-free customer support number to call when you have questions, a monthly newsletter, and periodic updates to the Toolkit. The Combination Subscription is an annual subscription at a price of \$30/month. To subscribe to this or any of the other subscriptions, fill out the form on the back of this newsletter and send or fax it to Agent 77 or call us at 1-800-294-2556.

### **Tell Your Friends!**

Many small healthcare providers — doctors, dentists, chiropractors, pharmacies, etc. — remain unaware of HIPAA's impact. While larger organizations are spending hundreds of thousands of dollars on HIPAA compliance and staff awareness, many small providers have yet to act. Be sure to tell your friends and colleagues how easy it is to become compliant with HIPAA*Now!*

### **Contributors:**

Judith Brunswick  
Kristin L. Hase  
Don Kaiser  
Gordon Kuntz  
Rob Silas

### **Editors:**

Judith Brunswick  
Kristin L. Hase

### **Design:**

Kristin L. Hase

### **Contact Agent 77:**

phone: 651.686.6500  
to order: 1.800.294.2556

info@agent77.com

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

# Notes

## On the Law

---

### **HIPAA and State Law**

As you work through your HIPAA implementation, you may have noticed that the rules may conflict with your state laws. HIPAA specifically deals with these interactions.

These interactions are among the most complex aspects of HIPAA, but you needn't approach it that way.

Remember that, in general, HIPAA prevails, unless state law is more stringent than HIPAA in protecting patient privacy. Some states extend rights and benefits not covered under HIPAA.

**Bottom line:** Always follow HIPAA unless you know of state laws that give patients greater privacy rights. HIPAA is the floor, not the ceiling: It provides the national minimum standard of privacy protection for patient information.

These interactions most likely will surface in your office in workers comp cases and with minors.

A good place to start to investigate whether your state laws are more stringent than HIPAA is [http://www.healthprivacy.org/info-url\\_nocat2304/info-url\\_nocat.htm](http://www.healthprivacy.org/info-url_nocat2304/info-url_nocat.htm) . On the left rail, click on the link to view the information for your state. This site provides a thumbnail summary.

Keep in mind that attorneys general are reviewing state laws in relation to HIPAA. Your attorney or state attorney general's office can provide you with the best specific legal advice regarding state law preemption.

### **HIPAA and worker's compensation**

HIPAA looks to individual states to determine what information can be released and to whom for worker's compensation claims. HIPAA specifically states that you may disclose protected health information to comply with state and local laws relating to workers' compensation without fear of violating HIPAA privacy standards.

These disclosures are subject to minimum necessary standards, however. You must only release the minimum information needed by the requesting party (employer, insurer or state agency). You can, of course, set up standards for routine or recurring requests for worker's compensation information so that you wouldn't have to review each request individually.

The privacy regulations are for the protection of your patients. They are not intended to impede the flow of health information.

At this writing, there is little to say anecdotally about the impact HIPAA may have on how you deal with workers comp claims and issues. We will pass along any stories as we run across them.

### **HIPAA and minors**

Let's say my 15-year-old son, unbeknownst to me, decides to get a tattoo. He exhibits the wherewithal to put it in a place not visible to adults, at least not until the weather is nice again and it's too late to do anything about it. He thinks that much through. Unfortunately, teenage hygiene practices are inconsistent. He develops an infection, and, being a teenage boy, doesn't want to show it to anybody until it reaches rather large, red proportions. He panics and goes to the school nurse. She is, naturally, appalled.

Can she call me and tell me what she's discovered?

Generally, persons less than 18 years of age are considered unemancipated minors. As such, they have the authority to act as individuals with respect to their protected health information if the state allows them to obtain health care service without consent of a parent or guardian (say, at a school health clinic), or if the parent or guardian agrees to a confidential relationship between the minor and the health care provider (such as in a therapy or mental health case).

I signed a release at the beginning of the school year authorizing the school clinic to call our general practitioner if my son needed further treatment. The clinic, while within the school, is a public health facility run by the city. In an emergency, the clinic health professionals would call the parent or the emergency contact first, then the student's designated physician.

In the case of the infected tattoo, the clinic acknowledges minor consent: they would treat the infection, but if they gave him an antibiotic, they may call me to let me know. That judgment would lie with them. In the case of medication being given for a sexually transmitted disease, they would not call the parent. So student privacy generally prevails.

HIPAA Privacy defers to state or local law regarding a parent's access. This assures that state or local law governs when a parent's access to PHI is explicitly required, permitted or prohibited. Even in those instances where there may be an exception, some states may still grant parents these rights. Conversely, some states may say you cannot disclose a minor's PHI.

HIPAA is neutral on whether a minor can consent to treatment; that is, it neither specifically allows nor prohibits it and defers to state and local law.

In cases where the parent is not the personal representative of the minor and state or other law does not require parental access, HIPAA does not give the parent or guardian the right to demand access and does not require a covered entity to provide it.

**Bottom line:** Parents (or any other personal representatives) are not getting any rights that they did not have before.

Furthermore, HIPAA will affect whether a minor would have rights to his or her records. That is, a provider's determination to deny access does not affect the minor's right to information; a covered entity could deny a parent access in accordance with state or other law and may be required to provide that access to the minor.

A court of law may authorize someone other than a parent or guardian (a personal representative) to make health care decisions for a minor if it determines the responsible parties are not attentive to or are jeopardizing the minor's health or best interests.

Adults and emancipated minors control their own health information. HIPAA defines an emancipated minor as one less than 18 years old who is married, pregnant, a parent, a member of the military or self-supporting.

If state law is unclear, covered entities should continue to do as they do now to determine if access is permissible. HIPAA Privacy assumes current practices are consistent with state and other applicable law and therefore may continue. HIPAA assumes present practice meets state standards.

# Question Answer

recently asked questions and their answers

**Q** Does our collection agency need to be compliant (they will have patient information such as address, SSN, phone number, job information and account transactions as to treatment performed)?

**A** Yes. However, since your collection agency is not a “covered entity,” you will need to enforce compliance by getting a business associate contract with them to ensure that they protect your PHI. 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. This includes financial services organizations such as your collection agency.

**Q** I understand changes will be made from time to time in the HIPAA Privacy Rule. How will those changes be made? How will I know if and when they happen?

**A** A HIPAA gives Health and Human Services the authority to modify the privacy standards, but a standard can be modified only once in a 12-month period, so you’re not going to be deluged with changes.

Generally, any alterations in the Privacy Rule must be made according to the Administrative Procedure Act (a fairness-based requirement which says, among other things, that rules not published in the Federal Register cannot be enforced). HHS will publish any proposed rule changes in the Federal Register and will invite public comment. After reviewing and addressing those comments, HHS will issue a modified final rule. The APA serves you, the citizen-provider, in that it also requires HHS to notify you of any such changes.

Your HIPAANow! Newsletter provides regulatory updates to you as they are published.

**Q** Our office promotes Oxyfresh products; we give samples and patients can purchase products. Do I need to obtain an authorization for this?

**A** You must obtain an authorization for marketing-related communications prior to the communications occurring. However, there are communications which are considered exclusions from this requirement. Authorizations are required for uses and disclosures of PHI for marketing communications, except: (1) When the communication occurs face-to-face between the provider and the individual; or (2) the communication involves a promotional gift of nominal value. Based on your question, it is not clear whether or not you are “selling” or providing patient information to a third party. If you are giving information to a third party about patients who purchase the products, then you are involved in marketing communication that requires you to obtain an authorization, and you need to indicate any remuneration you are receiving for selling/providing this product. If you are NOT giving anyone PHI and you are only selling this to patients on a face-to-face basis, then you are not involved in the activity of marketing.

The key is whether or not you provide PHI to a third party. If you don't release information to a third party, then you are not engaging in marketing activities and no authorization is needed.

**Q** Can reminder postcards contain the time and date of the appointment?

**A** The HIPAA Privacy rules specifically allow for appointment cards. If you read the Notice of Privacy Practices (section 4.3.1 in your Workbook), it states that you may contact the patient to provide appointment reminders. For these to be of any practical use to the patient, it will need to include the date and time. The government said that “reminder notices for appointments, annual exams, or prescription refills are not marketing” and thus are specifically allowed. We strongly recommend against including anything about the specific procedure on the card.

# On Privacy

## Communication Requests

Your patients may request that reminders, test results and other such information be sent to an address or location other than the one they list on their medical chart.

For example, a patient could ask to have bills and lab results sent to a post office box. Or a patient may want to receive phone messages only on his cell phone rather than at home or work. Maybe one of your patients travels extensively and prefers to have all his information by email.

One HIPAA privacy officer described a call she got from a patient, irate that his doctor's office had called his home number and left a message that his prescription was ready. His wife intercepted the message. He had specifically requested in writing that any calls be directed to his office, as he had not told his wife about his visit to this particular practice.

HIPAA law states that such reasonable requests be honored.

Think of it in terms of service: You want your patients to receive correspondence in the way that is best suited to them, to ensure they are up to date and informed in the timeliest manner.

Be aware, though, that any communication over open networks, such as e-mail, will need to be encrypted unless you have specific authorization from the patient that he or she understands the risk of interception and the resulting violation of privacy.

Some practices have already implemented online electronic medical records (EMR) that allow patients to view directly their diagnoses, prescriptions, allergies, immunization history and health-maintenance schedule.

A few providers have gone with the SSL (Secure Sockets Layer), the standard protocol for Web server authentication and encryption used by most online financial institutions.

As a provider, by law, you may require that your patients make requests for alternate communications in writing. You may also, when appropriate, condition your accommodation of such a request on when and how payment will be handled. And you can require the patient to provide you with a primary permanent address you may keep on file.

Say a patient does ask to have his information sent to a post office box. As provider, you can ask if he will guarantee receipt of his mail at that location, because you have the corresponding right to know your requests for payment are going to a place where the patient will see and respond to them in a timely manner.

If the patient will not give you that guarantee, then you have the right to refuse his request for an alternate address.

---

You may not ask to know why the patient wants information sent somewhere else or by another means.

Most practices already have time-tested privacy practices in place. HIPAA is both a mandate and an opportunity to make sure your communications procedures, both internally and with your patients, have the best interests of your patients at heart in addition to bringing you into compliance with federal law.

### **Where are the Employee Confidentiality Statements?**

You may have heard that you need to have Employee Confidentiality Statements to be HIPAA compliant but you couldn't find them in the *HIPAA Now!* Workbook. In fact, Task 2.62 (Staff Information Sheet) lists employee confidentiality statements as one of the forms each of your staff members must sign. These simple legal documents state that each employee will maintain the confidentiality of patient information and not discuss any such information outside of treatment (i.e., no gossiping).

There is no such form in your Workbook, because each state, and some municipalities, regulate what these types of employee documents can and cannot contain. For that reason, Agent 77 does not provide a generic document. If you do not already have an employee confidentiality statement, you need to have an attorney familiar with state and local employment laws draw one up for you.

# Quick Tips

---

## Who's your privacy officer?

HIPAA requires the appointment of a privacy officer, but such positions did not originate with HIPAA. They've been around for decades. Privacy or compliance officers are responsible for the privacy practices of a corporation, agency or department. They must ensure that each facet of the company or department complies with its stated practices. The privacy officer may also originate or assist in developing privacy practices and policies.

A HIPAA privacy officer is responsible for ensuring that a company implements rules that protect the privacy of patient records. Appointing a privacy officer should be one of the first steps in your HIPAA implementation process.

How does a practice go about choosing a privacy officer? Common sense prevails. The senior management – the partners, the pharmacy owner – should select the privacy officer. Candidates should have office management status; they will need expertise in limiting the use and disclosure of patient records. They should be intuitive types with excellent communications skills who can interact efficiently with providers and other outside entities as well as staff workers and patients.

To get an idea of what might be expected of privacy officers, check out these websites:

**[http://privacy.med.miami.edu/glossary/gt\\_privacy\\_officer.htm](http://privacy.med.miami.edu/glossary/gt_privacy_officer.htm)**

This is a “guided tour” of HIPAA glossary entries, a quick-search reference to have at hand.

**[http://www.ehcca.com/presentations/HIPAA3/malone\\_1.pdf](http://www.ehcca.com/presentations/HIPAA3/malone_1.pdf)**

This one, with the catchy title “Who Goes to Jail?”, sounds like it should be a better read. A Chicago law firm categorized HIPAA rules under topic headlines, providing quick scanning; but it's most valuable for its references to criminal and enforcement aspects of the law.

**[http://www.nacds.org/user-assets/hipaa/update\\_nov01.pdf](http://www.nacds.org/user-assets/hipaa/update_nov01.pdf)**

The third site is an outdated page from the NACDS website, but it breaks down the differences between privacy and security officers and their requisite skills.

**<http://www.hipaadvisory.com/action/privacy/dayinlife.htm>**

The fourth gives you a bird's-eye view. If you only look at one of these sites, look at this one. “A Day in the Life of a Privacy Officer” is a Joe Friday (“Dragnet”)-type diary entry that you'll read to the end.

# On Security

---

## Psst! The Password is...

Passwords continue to be a problem for offices around the world. They are a particularly difficult problem for small offices where employees share passwords on computers or software. On the one hand, you need passwords that are not easily guessable (like the word "password" ) so that they offer some modicum of security. On the other hand, you have to have passwords that are easy enough to spell and remember so that time is not wasted trying to remember them, or worse yet, security is bypassed altogether by having the password written on a Postit note attached to the monitor or placed in a drawer by the computer. Furthermore, passwords need be changed frequently so that if someone who should not have access to files does get the password without management's knowledge, this is automatically corrected when the password is changed.

The question is, how do you maintain the security that passwords offer without disrupting the office?

One tactic you can employ is the use of themed passwords. The idea is to narrow the scope of possibilities the password could be. You could literally choose anything: state capitals, desserts, trends of the 1980's or even dance crazes. If you chose dance crazes, the first month your password could be "funkychicken"; two months later you could change it to "vogue," and then "macarena" two months after that. This way, your office gets new passwords regularly and they're easy to remember. Using something like dance crazes as a theme has the added benefit of having something visual to associate it with, so when you tell your office workers what the new password is they will likely start dancing around doing it.

A way you can create passwords that are even more secure is to take a phrase or song chorus that everybody knows and use the first letter of each word. Say you decide to use "my baloney has a first name, it's Oscar." The password would be "mbhafnio." You can combine this with the first tip and only use junk food jingles or patriotic songs like, "I'm a Yankee Doodle dandy! A Yankee Doodle do or die!" or "Iayddayddod." This tactic has the added bonus of getting to watch co-workers as they try to figure out what the first letters of each word are and type them in two-fingered.

One way you can add an extra level of difficulty for hackers is to add in capital letters and/or punctuation. You can use broad rules, like capitalizing every new word and adding a question mark at the end. Thus, "funkychicken" would be transformed to the more secure "FunkyChicken?" To employ this strategy to the phrase or chorus, just add in the correct punctuation for the phrase: "mbhanfnio" becomes "Mbhafn,iO!" and "Iayddayddod" becomes "IaYDd!AYDdod!" In which case you may want to shorten it to, "IaYDd!"

A final device you can employ to help people remember passwords is to keep a hint list in a drawer somewhere. This way the passwords are not viewable by anyone who happens by the computer. Not only that, but you can use this with the other tactics. For example, if you used a dance-craze theme, employees who need access know what the theme is as well as the punctuation scheme. Then you could leave hint like "Madonna" for the password "Vogue?" Or you could use similar words like "wacky ducky" for "FunkyChicken?" For phrase passwords, you could leave the song title for a hint, like "Yankee Doodle" for "IaYDd!AYDdod!" Or use the product as the hint -- "bologna" for "Mbhafn,iO!" If you decide to use a hint list, place it somewhere out of the way and only accessible to those who have permission to use the computer. Of course, hints should only be used if the people in your office have a really difficult time remembering passwords.

In the end, passwords are only worthwhile if they are secure *and* easy to remember. But be smart about

**order information**

qty total

(32300A)

**Support Package**

one year of unlimited access to our experts to help you with HIPAA, and the HIPPANow! newsletter.

\$240

\_\_\_\_\_

sales tax (MN only) 6.5%

\_\_\_\_\_

**payment information**

total \_\_\_\_\_

payment type (check or credit card) \_\_\_\_\_

credit card number \_\_\_\_\_ expiration \_\_\_\_\_

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

signature \_\_\_\_\_

Fax form with credit card information to 618-566-4007.

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

Agent 77  
PO Box 19037  
Mascoutah, IL, 62258

**ship to:**

