

NewsLetter

HIPAA Now!

Edition 3, October 2002

Transaction Extension: Time's Up!

Wondering what to do if you didn't get the Transaction Extension in on time? This message from our President will let you know what you need to do now. Page 2.

Questions & Answers:

Are background checks required under HIPAA security? Do the Notice of Privacy Practices and other patient documents need to be in languages other than English? Can one family member call and schedule appointments for the entire family? These and other recently asked questions and their answers. Page 5 & 6.

On Privacy:

Final changes to the Privacy Regulations will affect patient rights, minors and acknowledgments and your waiting room. Pages 4 & 7.

Quick Tips:

All about the forms: How to use and access the forms in your HIPAA Now! workbook, and how to make them your own. Page 8.

On Security:

Shredders are now a fact of life. We give you some options, the benefits and drawbacks and the virtues of on-site versus off-site. Page 9.

President

Words From The:

Transaction Extension: Time's Up!

The deadline for filing for a transaction extension was October 15, 2002.

If you filed for the extension – congratulations! Remember, though: you need to have started testing your transactions (usually with the cooperation of your software vendor and/or clearinghouse) by no later than April 16, 2003.

On the other hand, if you didn't get the transaction extension filed in time, you don't need to panic. While CMS, the HHS department responsible for administering the transaction regulations, is gearing up for enforcement, there are a couple of things to keep in mind:

- 1 They have to catch you first. I don't say this to discourage compliance in any way, but detecting non-compliant transactions between private parties, many of which have received an extension to continue to send non-compliant transactions, is going to be hard. And, unlike the privacy or even security regulations, most patients don't know how you do your billing, so reporting is an issue.
- 2 HHS has consistently said that providers who show intent to comply with HIPAA should expect the cooperation of HHS in developing a remediation plan instead of being hit immediately with huge fines.

Your position with regard to the HIPAA transaction regulations is not unlike finding yourself going 50 in a 40 MPH speed zone. The best approach is to slow down to the appropriate speed as safely as possible.

Therefore, our recommendation is to get compliant as soon as you can. Possible strategies include:

- 1 Work with a clearinghouse to translate your non-compliant transactions to a compliant form (HIPAA allows you to transmit non-compliant transactions to a clearinghouse for reformatting). Just make sure you know where the clearinghouse is headed from a compliance standpoint.
- 2 Get compliant – ASAP. Inasmuch as there are no HIPAA police, so many providers will not be compliant by the mandatory date, and transaction compliance will be difficult to enforce during the transition period, one of the best strategies is to get compliant as fast as possible. Use your *HIPAA Now!* Guide and Workbook, and focus on getting through Section 3 as quickly as is practical. Call your software vendor, billing service and clearinghouse, and follow up the conversations in writing. With this strategy, you may still have some limited liability, but you are clearly showing the proper intent to comply.

Either way, do not delay. Get your practice into compliance with HIPAA's transactional requirements as soon as you possibly can to avoid potential fines and improve your practice.



Gordon Kuntz, President, Agent 77

Security not yet finalized

Word from Washington is that HIPAA security regulations should be finalized sometime between December 2002 and February 2003. There is every indication that these regulations will provide additional details around electronic security rather than sweeping changes from the draft regulations. Physical security measures are covered under existing privacy regulations.

HHS recently clarified that (1) it considers physical security requirements to be covered by existing privacy requirements; (2) final security regulations will primarily cover electronic security issues; and (3) these two issues are considered hand-in-hand.

For these reasons, we encourage our customers to proceed with privacy compliance with an eye toward the April 14, 2003, deadline and implement security regulations as soon as they are published. Agent 77 will provide updates as they are available.

New CDT version to take effect

CDT-4, the latest version of the version of the Code on Dental Procedures and Nomenclature, is now available from the American Dental Association. To remain compliant with HIPAA, dental practices should use the current version, CDT-3, through December 31, 2002, and start using the new CDT-4 codes as of January 1, 2003. The new codes include 52 new codes and 40 codes with revised nomenclatures/descriptors; 27 codes have been deleted.

Staff training available

Agent 77 has a staff training CD that can be used to train your entire staff, all future employees and any temporary personnel. For only \$249.95, you get a complete package on one CD-ROM: a 45-minute, self-paced training session, a self-test for your staff and a certificate of completion. Built as part of the HIPAANow! compliance system, this CD builds on your progress with the HIPAANow! Toolkit. It is the easiest way to satisfy the HIPAA requirement to train your staff on HIPAA Privacy and Security, your policies and procedures.

Call your distributor or Agent 77 today at 800.294.2556 for ordering information.

Kick-start your HIPAA compliance

Having trouble finding the time to do HIPAA compliance? Maybe what you need is a personal trainer! Agent 77's Accelerated Implementation Service provides a "personal trainer" for HIPAA compliance. Built to supplement the HIPAANow! toolkit, the Accelerated Implementation Service provides you with weekly reminders of the tasks you should be working on, helpful implementation tips and a look ahead to better plan your time.

HIPAA is much more about doing than learning. But finding the time can be hard. The Accelerated Implementation Service may be just what you need to get going. At only \$160, the Accelerated Implementation Service will help you to make sure your HIPAA compliance gets done.

Call Agent 77 today at 800.294.2556 for more information.

Contributors:

Don Kaiser
Gordon Kuntz

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

On Privacy

You may have been wondering...

Patient rights versus patient responsibilities

We are often asked about a particular situation that highlights the difference between a patient's rights under HIPAA and a patient's responsibilities in general. The situation in question involves whether a practice can deny (or withhold or delay) a patient's request for access to or copies of medical records (or any other patient rights under HIPAA) if there is an unpaid balance on the account. The reasoning goes (on the part of the practice) that the patient shouldn't be able to get a copy of the records if he still owes for the service that contributed to the creation of those records.

The answer, however, is that patients have, and are granted under HIPAA, certain explicit rights, among them the right to inspect and obtain a copy of their medical records. The language of HIPAA, without being absolutely explicit on the issue, provides an essentially unfettered right to access or obtain a copy of records. While a practice may charge appropriate, reasonable duplication charges for a copy of the record, the law does not allow a practice to withhold this right for non-payment.

What practices may do, however, is use the occasion to request payment of the balance so long as, in the process of requesting such payment, they do not interfere with the patient's HIPAA rights. (The practice might also use the opportunity to identify any issues impeding payment.) Lastly, the practice may take the maximum amount of time allowed by law (30 days) to satisfy these requests for delinquent accounts.

Minor patients and the acknowledgement

While recent privacy modifications go to great lengths to rely on state law when it comes to restricting or disclosing PHI about minor children, one other aspect of HIPAA requires a separate discussion of minor children.

Healthcare practices are required, under the recent modifications to the Privacy regulations, to provide a copy of the Notice of Privacy Practices and obtain an acknowledgement of receipt of the NPP for each patient. This right is not provided to a family, but to each patient. Therefore, a parent should receive a separate copy of the NPP and sign an acknowledgement for each child. This signed acknowledgement would then be filed in each patient's record and provide the necessary documentation under HIPAA. Practices may have the parent sign one acknowledgement listing all children, then copy this form for each child's file.

If a minor patient is seen by the practice and does not have a parent present to sign the form, the practice should continue to provide the appropriate care. The Privacy regulations require that you make your best effort to obtain the acknowledgement at the first practicable opportunity, not prior to (and certainly not as a condition of) providing care. Simply send a copy of the NPP and the unsigned acknowledgement form home with the minor. It is best to send a self-addressed envelope along as well. Be sure to note in the patient's file that you sent the form. If it returns, great – file it. If not, you have appropriate documentation that you made reasonable efforts to obtain the proper documentation. *(Continued on Page 7.)*

Question Answer

recently asked questions and their answers

Q **If someone breaks into your office and steals all the charts, and we have a security alarm, are the security people responsible or am I?**

A Most of the HIPAA regulations are about what could be reasonably be expected for privacy and security of patient information. Since you had locked doors and a security alarm protecting your records, this is all that could be reasonably expected of you for security of patient information. Thus, under HIPAA, you would not be responsible. As a non-covered entity, the security people would also not be liable under HIPAA.

Q **Will insurance companies no longer take paper claims, like Medicare?**

A The Administrative Simplification Compliance Act (ASCA) prohibits HHS from paying Medicare claims that are not submitted electronically after October 16, 2003, unless the Secretary grants a waiver from this requirement. It further provides that the Secretary must grant such a waiver if there is no method available for the submission of claims in electronic form or if the entity submitting the claim is a small provider of services or supplies. Nothing in the law prevents insurance companies from taking paper claims. That is not to say that an individual insurance company will decide not to accept paper claims or that they may add a surcharge for processing a paper claim. Each company will decide on its own how it will deal with paper claims.

Are background checks required under HIPAA security?

HIPAA states in the proposed Security Regulations that you must establish “personnel clearance procedures (a protective measure applied to determine that an individual’s access to sensitive unclassified automated information is admissible).” The proposed regulations clarify this for small offices: “The requirement for Personnel Clearance Procedures could be met in a small office with standard personal and professional reference checks.” This may change when the Security Regulations are finalized.

Do the Notice of Privacy Practices and other patient documents need to be in languages other than English?

Not necessarily. The only guidance HHS has given us is that these documents must be written in plain language. There is no provision for requiring the document to be written in a language that the patient understands. Currently, Agent 77 does not offer any of these documents in a language other than English. Feel free to translate any of our documents into other languages if you think your patients will be better served.

Can one family member call and schedule appointments for the entire family? Can we ask for personal information from one family member about another (such as a spouse’s Social Security number)?

HIPAA regulations define uses and disclosures of PHI that healthcare providers can make. There is nothing in the regulations about disclosures from patients to a provider. Thus, one family member can make appointments for the entire family, and you can request personal information at that time. What cannot happen is for you, the provider, to disclose personal information about a patient to anyone (except that patient’s legal guardian) without the patient’s express permission, unless the disclosure is for treatment, payment, your operations or the disclosure is to authorized law enforcement or government officials. This includes disclosing information to a patient’s spouse, parent or child (unless the person requesting the information is the patient’s legal guardian.)

(Continued from Page 4.)

One last consideration: who should sign for minor patients? Your state law is your best guide in this respect. You should follow the same decision path you would use to determine who may authorize treatment for a minor child. The documentation you require for treatment-related decisions will be adequate for HIPAA as well – just be sure to note who signed and their relationship to the patient.

Waiting-room etiquette

Both patients and providers will need to do some adjusting under HIPAA. You are familiar with the restrictions on oral conversations and that you should do your best to minimize incidental disclosures. However, it is sometimes hard to know exactly what to do. Here are some specific suggestions:

1. You may call patients from the waiting room by name – just keep the information to a minimum. Use their first and last name (or whatever salutation your patients expect) to call them into the examination area. Of course, don't ever use treatment-related information.
2. Allow some space to patients conversing with the receptionist. One suggestion is to put a piece of masking tape on the floor and a sign asking patients to remain behind the line. It doesn't take much room to provide the buffer needed to minimize incidental disclosures.
3. Educate your patients. You may have to ask them (in some case more than once) to stand back, keep their voice down, etc. Remind them that you are protecting their privacy and the privacy of others. In areas where neighbors are very familiar with each other's conditions, it will be a big adjustment for patients not to be able to ask how Mabel's arthritis is doing. Remember, any information willingly disclosed by one patient to another is their discourse not yours.
4. When a doctor is with a patient and is called to the phone for an urgent medical situation, simply mention this fact, in those terms. It is inappropriate to interrupt him/her with a patient in the room to say that Dr. Smith is calling about Mrs. Brown's toothache. Say, directly, that Dr. Smith is calling about an urgent situation. The doctor can politely ask to be excused; the patient, thus disturbed, should not object, and no PHI is disclosed.
5. Doctors or other healthcare practitioners may still discuss a patient's care with the patient and his or her family in the waiting room, but they should do so quietly and, to the degree possible, out of hearing of others. If that is not possible, or if the subject is especially sensitive, hold the conversation in an area further away from other patients.

HIPAA does not provide a patient an absolute right to complete secrecy regarding care. In fact, HIPAA specifically exempts incidental disclosures if (and only if) the practice makes reasonable efforts to minimize them. So take the appropriate safeguards and rest assured that you are doing the right thing.

Quick Tips

About our forms:

Colwell Systems offers many of our forms, such as the Notice of Privacy Practices, Acknowledgement and Authorization Forms, pre-printed. Talk to your Patterson salesperson or call Colwell to order these pre-printed forms.

You can print your own forms from the CD, which contains all the Workbook pages in two formats: Portable Document Format (.pdf files, read by Adobe Acrobat) and Microsoft Word format (.doc files).

If you access these documents from the screen that runs automatically when you insert the CD, the forms displayed are the .pdf version, which you can print but you cannot change. However, if you look at the directory, you will see a folder for each section that contains all forms and documents for that section. If you want to edit these, you must use the Word (.doc) version.

To access the Word version:

1. Put the HIPAANow! CD in your CD drive.
2. Start Microsoft Word (or WordPerfect, or other word-processing program).
3. Select the File menu, then select Open.
4. Use your mouse to move down the list of files until you see the listing for the HIPAANow! CD.
5. If you don't see it, you may need to click on the small plus sign (+) next to "My Computer."
6. Double-click on the HIPAANow! CD.
7. Look for a folder called "Docs," and double-click on it to open it.
8. You will now see folders for each section of the Workbook.
9. Double-click on the folder for the section that contains the document you want.
10. You will see a list of all the pages in that section.
11. Double-click on the document you would like to open, then click "open."
12. You can now add your practice's name to the document and print it out.
13. When you are done editing the file, you can close the file if you do not wish to save it, or, if you want to save the file, you can select the File menu, then select "Save As" (you can't do a "Save," as the original file is on the CD).
14. Select the location on your hard drive to save the file to, then press "Save."

To eliminate the word "Sample" written across a portion of the document:

1. Repeat steps 1 to 11 above.
2. With the document open, click on the large "SAMPLE"; you should see dots at each corner of the word.
3. Press the "Del" key on your keyboard.
4. Repeat steps 13 and 14 from above.

If you would like to copy the entire Documents folder to your hard drive for easier access:

1. Make sure the HIPAANow! CD is in your CD drive.
2. Click the Start button on the lower left part of your screen.
3. Look for the Windows Explorer program (you may need to click on All Programs; if it is not there, click on Accessories to find it).
4. Start Windows Explorer.
5. You will see a window divided into two parts. Use your mouse to move down the list of files in the left-hand part until you see the listing for the CD.
6. If you don't see it, click on the plus sign (+) next to "My Computer" in the left-hand side of the window.
7. Double-click on the CD.
8. You should see contents of the CD listed on the right-hand side, including the "Docs" folder.
9. Now, use your mouse to move to the top of the left-hand window until you see a listing for Desktop. *Do not click anything on the left-hand side.*
10. Using your mouse, drag the "Docs" folder in the right-hand side to the Desktop on the left-hand side. A window will pop up saying that the folder is being copied to the desktop.
11. You can now access any of the forms and documents directly from your desktop and, after editing them, save them back to the "Docs" folder without having to use "Save As."

On Security

Shredders

Patients expect the information they entrust to you will not be tossed out in your trash, to be easily found by anyone. HIPAA privacy and draft security regulations make it your responsibility to ensure that patient data is destroyed, not just disposed of.

To accomplish this goal, you have options:

Shred documents in your own office

In selecting a shredder for your office, there are two considerations to keep in mind:

- 1 The shredder should be a crosscut shredder to ensure maximum security. Only slightly more expensive, crosscut shredders create confetti rather than strips of waste paper.
- 2 Make sure it has adequate capacity to handle the volume of documents you need shredded. Less expensive, lighter-duty shredders may be adequate for a single-provider office; larger settings will need either multiple or heavier-duty shredders.

There are costs as well as benefits to shredding documents in your own office:

Benefits:

Flexibility – you may shred when and where you want

Low ongoing costs – once you own the equipment, you have few out-of-pocket expenses associated with shredding.

Costs/issues:

Staff time – someone has to run the shredder, feeding it documents to shred and disposing of the waste. These hidden staff costs can add up!

Noise – shredders are noisy. Especially in a small office, the noise can necessitate shredding only after hours.

Placement/space – shredders with the capacity for even a small office are floor models requiring several square feet of space. They also generate a fair amount of dust and debris from waste that misses the output bag.

Hire a shredding service

Shredding services gather documents and other items to be shredded on a regular schedule, often conducting the shredding in your parking lot in a specially equipped truck. These companies will also usually provide secure holding bins for documents waiting to be shredded. Costs will vary with company, location and service plan, so compare prices and services carefully. Any company you choose should provide documentation of the completion of their shredding activities. Ideally, they will also help you with destruction of non-paper items such as fax carbon rolls, CDs and computer diskettes.