

Newsletter

HIPAANow!

Edition 2, September 2002

The Costs and Benefits of HIPAA:

Wondering what cost benefits you can reap from becoming HIPAA compliant? This message from Agent 77's CFO may shed some light on the matter. Page 2.

Regulatory Update:

On August 14, 2002, the Department of Health and Human Services issued final changes to the HIPAA privacy regulations that will affect your HIPAANow! implementation. Pages 4 & 5.

Questions & Answers:

Recently asked questions and their answers. Page 6 & 7.

On Privacy:

This month's issues include: Media and Other Non-Family Requests, Logging Incoming Information, Multiple patients on one Acknowledgement/Authorization and Gifts. Pages 8 & 9.

Quick Tips:

Inboxes and viruses are the Quick Tip subjects for this month. Page 10.

On Security:

Patients expect the information they entrust to you will not be tossed out in your trash, to be easily found by anyone. But what do you need to know about disposal? Page 11.

CFO

Words From The:

Catering to the Customer, er... Patient — The Costs and Benefits of HIPAA

As signs across America logged the millions of McDonalds™ hamburgers consumed, it was evident that we embraced the speed and taste of fast food. It forever changed the restaurant business and waistlines of America. Fast food became a new standard, and many other chains followed. From restaurants to the dentist/doctor's office, the public ultimately determines what standards will stay or go.

Recent surveys indicate that up to 40% of the American public value their individual privacy above all else. Financial privacy has been the target of much legislation over the past five years. Bills like the Gramm-Leach-Bliley bill have forced financial institutions to treat the financial information of their customers with the importance that the public expects (as you've probably seen in a multitude of flyers and brochures from those institutions). Now, the patients of medical practitioners have spoken, and they expect the medical field to protect their private health information. Along came HIPAA with its Privacy and Security regulations.

The HIPAA regulations attempt to ensure that every record that moves from provider to intermediary to payer and back again, remains safe and secure from unauthorized access or distribution. If we're going to use electrons to pass data, we need to make sure it gets passed safely and confidentially. And, if a patient is in your office, they likely have the expectation that the visit they're making and the information it generates stays between the doctor and the patient.

So, what is the cost of meeting those expectations?

A number of potential costs are associated with implementing HIPAA within your practice. Many large medical organizations are spending hundreds of thousands of dollars on HIPAA implementation efforts. Securing your data might require locked filing cabinets or converting a closet to a file room. New software may need to be purchased. Time, thought and resources must be devoted to a new way of handling patient data, or maybe even reconfiguring your office. HIPAA does not REQUIRE any of these, specifically. HIPAA requires that each practice make an effort to safeguard its patients health information from unnecessary access as well as ensuring that it doesn't leave the premise in an unauthorized fashion. Scalability, reasonableness and "good faith efforts" are constant themes in HIPAA. But, are there any benefits?

It benefited McDonalds™ to meet the desires of customers. Sure, they profited (and mightily). But they profited because they provided something customers wanted. Patients want privacy and security for their private health information. HIPAA may not provide hard dollars to the "bottom line" of your practice, unless, of course, you don't meet your patients' expectations and they opt to use another provider. We don't anticipate that the penalties associated with non-compliance will be levied on every provider. But, for those who do get penalized, the cost will be steep. Thus, the benefit in spending the money to become compliant is similar to the benefit one has in paying for insurance, i.e., fewer sleepless nights worrying over unforeseen events. But most importantly, there is the benefit of knowing that you not only provide the care your patients expect, but you provide peace of mind — peace of mind that tells your patient, "I respect your privacy."

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!*

Electronic Transaction Extension

Time is running out. The deadline for submitting this form electronically on the World Wide Web (www.cms.gov/hipaa/hipaa2/ascaform.asp) is 10/15/02. Submissions on paper also must be postmarked by that date. The extension is free. The form is about 2 pages in length (and instructions) and takes 20-30 minutes to complete. It must be filed unless you are fully compliant with the transaction sections of HIPAA. Failure to file for the extension makes you subject to fines and penalties if you do not use compliant transactions after 10/16/02.

While the extension allows you until 10/16/03 to comply with the transaction standards under the law, your contractual obligations to various trading partners may require you to be able to transmit the new standards prior to that date.

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.

Contributors:

Jeff Abramovitz
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

Regulation **Update**

Impact of Final Changes to HIPAA Privacy Regulations

On August 14, 2002, the Department of Health and Human Services issued final changes to the HIPAA privacy regulations. Slated to take effect October 14, 2002 (following the mandated 60-day period before it becomes law after publication in the Federal Register on August 14, 2002), these rule modifications for the Standards for Privacy of Individually Identifiable Health Information make the implementation of HIPAA somewhat easier for providers. Although these are the final regulations for the enforcement deadline of April 14, 2003, additional modifications are likely in subsequent years since the law allows for each standard to change annually.

The final changes have the following impact on a practice's HIPAA implementation:

Removal of the Consent Requirement

This is the most significant change from the previous regulation. Instead of a specific Consent Form, the final regulation requires that covered entities provide patients with the Notice of Privacy Practices, and then patients are asked to acknowledge receipt of the Notice of Privacy Practices through a "good faith effort" on the part of the covered entity at the earliest possible time. Covered entities may continue to use a consent process that works for that entity but it cannot withhold patient care if a consent form is not signed by the patient. It also reinforces but simplifies the use of the Patient Authorization Form for patient data other than for TPO.

Requires Reasonable Safeguards Regarding Incidental uses and disclosure of PHI

This change reinforces the oral communication and minimum necessary rules, but it indicates that if minimum necessary rules are followed and reasonable precautions against overheard conversations or practices such as using sign-in sheets are taken, then incidental uses and disclosures are allowed.

Provides Model Business Associate Agreements

To ease the transition, HHS has provided model Business Associate Agreement language and will allow up to an additional 12 months (to 4/14/2004) for existing contracts to be changed.

Changes to the Marketing Rules

First, the Marketing definition was further defined to distinguish between types of communications that are and are not marketing and clearly states that covered entities are prohibited from selling lists of patients and enrollees to third parties or from disclosing PHI to a third party for the marketing activities of the third party without the patient's authorization. Marketing rules were clarified to require explicit approval by obtaining prior written authorization before using an individual's PHI for marketing purposes except for a face-to-face encounter or a communication involving a promotional gift of nominal value. The final regulation allows free communication by providers regarding treatment options and other health-related information.

Clarifies State Preemption Regarding Parental Access

The final regulation removes any ambiguity about the preservation of state laws and regulations regarding parental access to information.

Modification to the Accounting of Disclosures of Protected Health Information

The required Accounting of Disclosures of PHI is modified not to require tracking of those disclosures made subsequent to an authorization signed by the patient.

Clarifies the Transfer of Information for TPO

This modification allows a covered entity the ability to disclose/transfer PHI for the treatment and payment activities of another covered entity or a healthcare provider, and, with certain limitations, operations. This clarifies that it is permissible to transfer patient information in referrals and pharmacy relationships.

Accounting of Disclosures

The final Rule exempts disclosures made pursuant to an authorization from accounting requirements. Simply stated, a covered entity does not have to account separately for disclosures that are made as a result of an approved authorization. The authorization provides the adequate support for the disclosure of PHI in each instance where it has been used.

Other minor modifications

Several other minor modifications were included in the final regulation changes, mostly affecting organizational issues such as clarification of a hybrid entity, how to handle changes in ownership of a practice or those items that namely affect small providers, and then only in a limited way or in specific cases.

The *HIPAANow!* Guide and Workbook will be changed to reflect the revised rules and will be distributed to you by September 30. Be sure to complete and return your *HIPAANow!* Toolkit Registration Form and return it to Agent 77:

Fax 651.686.6528
Mail Agent 77
 PO Box 19230
 Minneapolis, MN 55419-0230

Agent 77's HIPAA Newsletter and Product Updates will keep you updated on these and future rules changes. Don't miss out — make sure your subscription is current. If you have any questions regarding the changes proposed by HHS or their implications for your practice, please contact Agent 77.

Question Answer

recently asked questions and their answers

Q Can we still send recall cards, thank yous, appointment reminders, etc.?

A Sure. However, any visible information should exclude details related to specific treatments (past or future) or financial issues. In other words, it is OK to send an appointment reminder that indicates an upcoming appointment (no description of a specific treatment). But if specific dates or treatment details need to be communicated, the reminder should be put in an outer, plain envelope that only has the provider's name and address information. It is equally inappropriate to put "2nd Notice" on the outside of a request for payment.

Q I've heard that I need to change my office design and put new walls or partitions in my open areas so patients cannot overhear other patient - doctor conversations.

A Not true. In response to a similar question, the July 2001 Guidance from HHS says, "Covered entities (providers) must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of PHI... The Department **does not consider** facility restructuring to be a requirement under this standard." This means that HHS has said that providers need to be prudent in how they conduct conversations in open areas, but they do not need to add partitions or remodel.

Can we still have sign-in sheets?

Absolutely. However, in the interest of patient privacy, it is prudent to put the absolute minimum information on them. Any additional information you might need to collect, such as reason for visit, other condition, or treatment information, could be requested on a separate form that is put in the patient's record and treated as PHI.

Someone told me we can't even call patients by name when they're waiting in line.

Not true. The July 2001 Guidance from HHS says, "Covered entities (i.e. providers) must provide reasonable safeguards to avoid prohibited disclosures. The rule does not require that all risk be eliminated to satisfy this standard." Patients may be called by name (unless they request not to be) when waiting, but again, discretion and minimum necessary considerations should be followed. In other words, while it is permissible to call a patient by name, it would be contrary to HIPAA to call the patient and the treatment they are to receive.

Is it OK to publish treatment schedules in the office?

It is permissible to publish patient directories and treatment schedules, but, as with all Protected Health Information (PHI), patients must be protected from inappropriate disclosure. What this means is that the lists should be posted in a place inaccessible to casual observers (inside a cabinet door or in a staff-only break room or other office area to which patients do not have access). Such lists should not be posted in plain view of patients.

On Privacy

Media and Other Non-Family Requests

Remember, requests for information about a patient from anyone other than those involved in their care (typically family members) require a specific authorization. That includes the media, coaches, friends or other non-family members (who don't have an appropriate form of power of attorney) who inquire as to the patient's specific diagnosis, treatment or more than an overall condition level. Even then, you can only provide the patient's name, location in the facility and general condition (e.g. stable, critical, etc.) if they ask for the person by name. For example, you should not respond with any detailed information about requests for information on the condition of "the accident victim."

Make sure you have a standard response for such requests, such as "Due to patient privacy concerns, we are not allowed to release that information without a specific authorization from the patient or their designated representative."

Logging Incoming Information

HIPAA's draft security rules require that you log receipt and transmission of PHI. The Privacy rules further require that you be able to produce a log of all PHI disclosed for a specific patient for the last 6 years (please note that significant limitations apply regarding the data you have to track in this way). There are a couple of ways that you can log patient information as it comes into or goes out of your office:

- 1 You can set up a simple computerized tracking system using Microsoft Access or Microsoft Excel to log faxes and other documents containing PHI received or sent by your office. Be sure to record whether it was received or sent, how the document was disclosed (paper copy, fax, etc.), what the document was and which patient it pertained to. You may have other information you wish to track as well (who sent it, reason for disclosure, authorization obtained, etc.).
- 2 You may be able to use a comment screen in the patient accounting system you already have to log this information as well. This provides a convenient way to track by patient; however, while sorting by patient is easy, it may be more difficult to find certain specific dates of receipt or transmission in this format. It may also be more difficult to ensure that the appropriate data is collected for every event.

Multiple patients on one Acknowledgement/Authorization

The medical record is patient-centric; it contains the records of a single patient.

The recently released final privacy regulations require that you provide a Notice of Privacy Practices to each patient and obtain their acknowledgement of receipt, and that you maintain a record of these acknowledgements. This will be most easily accomplished by placing the signed acknowledgement in each patient's medical record.

Patient Acknowledgements are designed to authorize release of a specific set of information for a specific patient to a particular recipient for a specific reason. This level of specificity in the design of the document

does not lend itself to combined authorizations. In fact, because Patient Authorizations are so specific, it is highly impractical to share them among patients.

If authorizations are required to release the records of several children in a family for various summer camps, the regulations would effectively preclude you from combining these on one form; instead, you will need to create separate Patient Authorizations for each release for each person and have the patient or (in the case of minors) their parent sign them.

Alternately, for simple requests such as immunization records for school or camp, you can provide the information to the patient (or parent) without an authorization at all, and without needing to track the disclosure. However, it remains a solid practice to document any release of information in the patient's record.

Gifts

You may give new parents or other patients gifts or other giveaways, as long as a few basic rules are kept in mind:

1 The gift should be of "nominal value." Most items given to patients would be considered of nominal value, so this shouldn't be a big problem.

2 The information gathered to provide these gifts (mailing lists) is best kept in-house. If you need to send this data out to a marketing firm to fulfill the gift order, be sure you have a business associate agreement in place with the marketing firm, that the original source (your office) is clearly indicated on the communication, and that the patient has an opportunity to opt out of future communications.

3 It is NOT permissible to sell the patient's name and/or other identifying information to a third party for marketing purposes (or, generally, for any other purpose) without a patient authorization.

4 The closer the gift relates to treatment, the better. The HIPAA definition of marketing limits it to those items related to treatment.

Quick Tips

After Hours Cleaning Services

Recent changes to HIPAA rules allow for “incidental disclosures” as long as there are adequate safeguards in place to limit disclosures to those that are truly incidental. HHS also specifically indicated that providers are not required to have business associate agreements with non-employee after-hours cleaning services, as any disclosure to them would be incidental. However, this begs the question as to what “adequate safeguards” would need to be to allow for this exception. In our opinion, practices have 2 choices: they can either secure their records with locking file cabinets or file rooms, or they can have a business associate agreement with their cleaning service.

If you choose the approach of securing your paper and electronic records, make efforts to put away as many paper records as possible, and protect electronic assets with passwords. Recognizing that a complete “clean-desk” policy is probably not practical, we recommend that you remove as many records as possible daily to a secure environment (locking cabinets or room). Even with this approach, you should educate your cleaning service on the importance of protecting patient information.

If you choose to enter into a business associate agreement with them, you should make sure you ensure that they have been properly trained on handling PHI and the prohibitions against disclosure. Conducting this training is the janitorial service’s responsibility but you are on the hook if they don’t execute properly. This is a situation where an ounce of prevention will be worth a pound of cure. Make sure they know that not only are medical records “off limits,” but so are incoming faxes, papers left on desks and in-boxes. Their training should also include a notice that reading, copying or viewing sensitive patient data can carry serious consequences for your practice, their employer and themselves.

Viruses

Computer viruses come in many forms. While many are, thankfully, not particularly damaging, some can be devastating, deleting critical files or making your computer unusable. While all are of concern to computer users across the country, a particularly troublesome one in regards to HIPAA issues is the Kleg virus (or “worm,” a term used to describe the mode of transmission and action). The Kleg virus, once it has infected your machine, will sit dormant for a period of time then look for two things: e-mail addresses, whether stored in an address book or any other file; and a file, or files, to send. The latter are chosen at random and, when the computer belongs to a healthcare provider, could certainly contain PHI. Worse yet, the e-mail received as a result of a Kleg attack may not have the correct return address, but will likely have a “spoofed” e-mail address confusing things further.

The bottom line is that viruses can compromise PHI through e-mail without your knowledge. You can protect yourself by doing the following:

Have and use up-to-date virus detection software. You must keep it up to date for it to do any good, and you should use it to screen all incoming e-mail messages and Internet traffic, as well as scanning any floppy disks or CD-ROMs used in your machine.

If possible, store PHI and sensitive documents on a central server. These are less susceptible to Kleg viruses because they are one level removed from the e-mail system. Periodic virus scans should be done of these systems as well, of course.

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 several options:

1 Shred documents in your own office

In selecting a shredder for your office, there are several characteristics to keep in mind:

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.

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 either need multiple shredders or heavier duty shredders.

If you elect to shred documents in your own office, there are costs as well as benefits. These include:

Benefits:

Flexibility – you have the flexibility to shred when and where you want

Low On-Going 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, shredder 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.

2 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.

order information

qty total

(32300A)	Support Package one year of unlimited access to our experts to help you with HIPAA	\$240	_____	_____
(32400A)	Periodic Updates keep your Guide and Workbook fully compliant	\$240	_____	_____
(32500A)	Support and Update Package combine the Support and Update Packages for complete coverage	\$360	_____	_____
(32600A)	Security Technical Bulletin bulletin filled with information covering the technical side of HIPAA	\$125	_____	_____

sales tax (MN only) 6.5% _____

total _____

payment information

payment type (check or credit card) _____

credit card number _____ expiration _____

name on card _____

signature _____

shipping information

practice name _____

address _____

city _____ state _____ zip _____

phone number _____

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

Agent 77 - PO Box 19037, Mascoutah, Il, 62258 or fax form with credit card information to 618-566-4007.