Billing
Healthcare Billing & Management Association

HBMA

January/February 2003

HIPAA Privacy Rule

SURVIVAL TIPS TO AVOID LAST-MINUTE PANIC

By Karen Collier, J.D.

Some health care providers, facilities, and other covered entities have spent the last three years planning, preparing, and implementing strategies for HIPAA Privacy compliance by April 14, 2003. They are now checking the minor details, making sure all staff is thoroughly trained on the Privacy rule, and sitting back waiting for the arrival of mid-April with the satisfaction of a job well done.

For the rest of the health care world, however, reality is a little different. Government and industry estimates show that the majority of HIPAA-covered entities are not sitting back smiling right now. They are scrambling to learn, plan, and implement HIPAA Privacy compliance programs between now and the fast-approaching deadline.

If your company falls into the latter category, then this article is for you. If you feel that your company does not have to comply with HIPAA because it is not a "covered entity," read on anyway. Enacting basic privacy measures based on HIPAA requirements for your business will likely become the *de facto* liability standard for anyone who touches health care-related information, covered entity or not.

THE BASICS TO KEEP IN MIND

Wherever you are in your HIPAA planning and implementation, there are a couple of things that should be in the forefront of your thinking at all times. First, remember that the basic premise of all these laws and regulations is that patients' privacy be respected and protected. The key here is to make sure that all your employees and others treat patient information as carefully as they would want their own information treated by others. It is easy for health care workers to become inured to the sensitivity of the data they see and touch every day, so adequate training and frequent reminders are vital.

> The goal of billing companies should be to establish a culture of privacy and confidentiality that permeates the business.

Keeping that basic premise in mind, the goal of billing companies and others who use and process protected health information should be to establish a culture of privacy and confidentiality that permeates the business. If you can accomplish the goal of a privacy-oriented culture in your business, you will greatly lessen the risk of major liability for unauthorized or unintentional disclosure of protected health information. You will also make things easier in the long run for you, your employees, your clients, and your business.

A privacy-oriented business culture means that whenever policies are enacted, actions are taken or decisions are made, the issue of patient privacy is always considered. If you are successful in developing and nourishing this type of corporate culture, then privacy compliance becomes second nature, not an additional burden. Each member of

(continued on page 5)

INSIDE...

(continued from page 1)

your team, every aspect of your systems, even the layout of your offices, should have patient privacy concerns embedded in them. Achieving this mindset is what HIPAA privacy compliance is all about.

GETTING STARTED

Okay, mindset and culture are good, but how do you get there? How do you make sure that you're not caught holding the bag, HIPAA-wise, when the deadline rolls around? There are several practical steps you should be taking now to make HIPAA compliance happen.

- Take it seriously. It's time that we all get through the stages of coming to terms with HIPAA—anger, denial, bargaining, etc. These emotional responses are luxuries you can't afford at this late date.

- Make sure you've got a point person to lead the way. In many billing and practice management companies, this means the boss. Whether it's a one-person shop or a larger organization, your privacy official (that's the HIPAA term) needs to be someone who can get the job done. Having someone in charge of getting everybody on board, who has the authority and drive to accomplish it, is essential.

- Perform an assessment of the flow of patient health information through your business, and conduct a gap analysis of that flow compared to the HIPAA regulations. In layman's terms, you should think about patient health information (PHI) and how you interact with it. These questions should be answered, thoroughly and completely, during this "thinking" process:

  A. How does patient information come into my office?
  B. How is it used, accessed and stored while it's here?
  C. How is it transferred or disclosed to others?

- Brainstorm. Have everybody participate. The answers to these questions should provide the framework for building the appropriate policies and procedures you will need, and for constructing your overall HIPAA compliance plan.

> Make sure that all employees and others treat patient information as carefully as they would want their own information treated.

Once you have completed your assessment/analysis—and often during any HIPAA-related activities—you and/or your HIPAA privacy official should do the following: close your eyes, take a deep breath, and repeat the unofficial HIPAA mantra: *Reasonable Safeguards*. When you feel panic setting in, this phrase can work wonders. HIPAA privacy compliance is possible, and it doesn't have to consume all your time and resources to get there. A well-thought-out plan, some serious effort, and frequent mantra-chanting can be key.

Primary Policies and Procedures

Developing written policies and procedures covering patient health information is the next step toward HIPAA privacy compliance. The primary consideration should be a basic policy covering the use and disclosure of such information:

1. What is required (release to patient or as required by law)
2. What is permitted (e.g., release for treatment, payment and operations or disclosure to business associates)
3. What is not permitted (unauthorized, against policy, etc.) in dealing with protected health information.

There should be clear direction to staff and employees, and there should be disciplinary consequences for failure to follow the policy.

Remember that practically any element of data that can potentially identify patients or something to do with their health care status or treatment is protected, not just the whole patient record. Billing and financial information is considered protected health information under HIPAA, too. Personnel should be aware that more than names and Social Security numbers are considered part of the patient's protected information, which includes such things as addresses, phone numbers, dates of birth, insurance policy numbers, and even ZIP codes.

The next area that your policies must address is the minimum necessary standard. The minimum necessary standard requires entities to limit unnecessary or inappropriate access to and disclosure of protected health information. In other words, only the minimum amount of information necessary to do the job should be utilized, even when such use is allowed by HIPAA.

This standard may have a far-reaching effect on the health care billing and payment industry. According to most interpretations, gone are the days when a payor can request the whole patient chart in order to determine whether a particular claim should be paid. These types of requests, and billing companies' responses to them, should be considered carefully after April 14th.

Every HBMA member company should have a written policy stating clearly that only the minimum amount of patient information necessary to accomplish the intended purpose is allowed. Real-life examples and situations should be discussed with staff, employees, contractors, etc. Disclosures to the patients themselves, or ones that have been authorized by the patient, in writing, do not have to meet this standard.

Security and access to information should be covered in the company's policies and procedures. This could be a formal security and technological access plan, or it could be as simple as directives that all patient files are to be covered up when a worker leaves a desk, and all computer screens must use a password-protected screen saver.

If there are different departments, or different job functions that require different levels of access, think these through and write them into the policies. Physical security measures such as vendor access, the use of pass codes, key cards, locked file cabinets and office doors, etc., should included.

Although at the time of this writing CMS had not yet finalized the HIPAA Security regulations, being aware of what they contain will help in the decisions as to what your *reasonable safeguards* should be.

FIVE ESSENTIAL HIPAA PRIVACY SURVIVAL TIPS

1. Remember the Golden Rule–treat patient information as you would want yours treated by others, and foster a **corporate culture of privacy** and confidentiality
2. Have a point person–someone who keeps up on HIPAA matters and makes sure the business is doing what it is supposed to **(Privacy official)**
3. Think through all aspects of patient information flow **(assessment/analysis)** and write down your conclusions about how it should be handled in compliance with HIPAA **(policies and procedures)**
4. Make sure everybody knows what to do, what not to do, and what is expected of them **(training and enforcement)**
5. Repeat often, as necessary, the HIPAA mantra: ***reasonable safeguards***

Communication media and verification of identity are important aspects of a HIPAA privacy policy, and will impact day-to-day behavior in every office. Fax machines, e-mail, and telephone procedures need to be thought through carefully and written into HIPAA compliance plans and policies.

For example, a privacy policy should make it mandatory that any piece of protected health information that is sent via e-mail must be encrypted. Tell your employees that sending information by e-mail is a lot like sending an electronic postcard—anybody along the way can intercept and read it. It will not be considered a reasonable safeguard of information to use unencrypted, public, Internet e-mail, even occasionally.

Fax machine usage is another daily activity that should be included in HIPAA privacy policies. Checking and verifying numbers, using pre-programmed "speed dial" when possible, and verifying receipt of faxes are all sound policies. In most cases, limiting overall use of fax machines for transmission of patient health information is wise.

For those companies who take patient or payor calls on behalf of their clients, verifying a caller's identity before discussing a patient account is necessary to ensure that unauthorized or inadvertent disclosure of information doesn't take place. Banks, credit card companies and other financial institutions have dealt with this issue for years, and the use of PINs, account verification questions (What is your mother's maiden name?), call backs, and other methods are customary. For billing companies, these or other ways to reasonably safeguard information on the telephone must be developed. Outbound telephone calls to insurers, employers, or for collection purposes, etc., should be covered in the policy as well.

OTHER REQUIREMENTS

Every business should have a policy that any and all privacy errors (unauthorized or inadvertent disclosures) must be reported to management or the HIPAA privacy *(continued on page 10)*

- Ask your insurance agent to also read the fine print.
- Purchase your own coverage if in doubt.
- Consider a recovery program offered by the system vendors.

Using a Courier Service

- Ask for a certificate of insurance for workers' compensation, general liability, and business auto coverage prior to contracting for services.
- Require a new certificate before the expiration date on the original certificate(s).
- Suspend your contractual arrangement should your courier service allow its coverage to lapse.

Using a Business Record Archiving Service

- Require a contractual agreement and review for insurance coverage description; the industry standard is $1.00 per box.
- Confirm that you have valuable papers insurance in an amount sufficient to cover the cost to reconstruct.

Employees Use of Personal Vehicle for Business

- Require a current copy of the employees' driver licenses.
- Require a current copy of the employees' auto insurance verification documentation.
- Remember employees' auto insurance protects the employee only.
- Your company's Hired Auto and Non-Ownership coverage within your commercial package policy protects the company only.

Using Independent Contractors

- The company will be charged a higher rate under its general liability policy when subcontractors are used if they do not provide their own coverage.
- Workers' compensation in most states allows the company to cover the individual and charge the cost back to the contractor. An alternative might be for the contractor to sign a waiver with the state and pay a nominal fee.
- For travel to and from your company, the contractor will need to provide you with proof of insurance for his personal automobile and the company will need to have Hired Car and Non-Ownership coverage to cover the company's liability.
- For errors and omissions insurance, the billing company can cover the contractor under its errors and omissions insurance policy and charge back any additional cost to the contractor.
- For valuable papers coverage for any financial data and/or billing source documents being transported or housed in the contractors' homes or automobiles, the cost, which will be based on the cost to reconstruct, can be charged back to the contractor.

As owners and managers, we can come up with other situations that exist within our company's operations that have exposure. There is no better time than now to review your existing insurance programs to identify any gaps in coverage and identify the coverage terms that should be defended at all costs as opposed to those that could be sacrificed if necessary. ◆

Susan J. Gregg, CMPE, is Chief Executive Officer at Shared Management Services, Inc. in Oklahoma City, OK. She can be reached at 405/858-2350 or by e-mail at sgregg@smsokc.com.

(HIPAA continued from page 6)

official. Like any compliance program, good communication of what's going on is key to fixing mistakes, improving processes, and ensuring compliance.

Destruction of any media containing protected health information should be included in HIPAA planning. Shredding documents, erasing and properly disposing of electronic media, disks, tapes, recordings, etc. are important things to consider. How are surplus computers or other equipment "cleaned" before disposing of them?

All the thinking and planning and writing of policies and procedures should be thoroughly explained to your employees and anyone else involved in your day-to-day business. Training on your HIPAA policies can be formal or informal, but it must be documented as to who received it, what was covered, and when it was completed. The HIPAA regulations say that staff training must be completed by the April 14, 2003 deadline.

While this doesn't cover absolutely everything HIPAA says you must do, it goes a long way towards achieving HIPAA privacy compliance. For more guidance, check out the new Privacy Guidance published by DHHS on the web at www.hhs.gov/ocr/hipaa/privacy.html. In the next HBMA newsletter, crafting appropriate business associate agreements and dealing with patient rights under HIPAA will be explored. ◆

Karen Collier is Corporate Compliance Officer and Privacy Officer for Emergency Physicians Billing Services in Oklahoma City, OK. She can be reached at collierk@epbs.com