Maintaining ***Patient Confidentiality***

HIPAA Compliance

by Teri Junge, CST, CFA, FAST, BS

A HIPAA compliance program is necessary in a medical setting to protect the patient's personal, medical and financial information. It will be necessary to share patient information with other entities, and that must be done legally. This article addresses planning, implementation and evaluation of a HIPAA compliance program.

The acronym HIPAA represents the term Health Insurance Portability and Accountability Act, which became federal law in 1996. Implementation and enforcement of HIPAA is the responsibility of the Office for Civil Rights, which is part of the US Department of Health and Human Services.[1] A HIPAA compliance program is necessary to ensure delivery of quality health care to the general public and to protect the patient's personal, medical and financial information. The two main goals of the HIPAA program are portability and accountability.[2]

The portability portion of HIPAA was set up to broaden the health care options available to an individual by increasing his or her ability to obtain and maintain health coverage, even when changing jobs, or by allowing individuals to purchase health insurance if group coverage is not an option. HIPAA also limits exclusions from health insurance coverage due to preexisting and current conditions.[3] The portability portion of HIPAA pertains primarily to health plans, and the focus of this article is on the accountability portion of HIPAA as it pertains to health care providers and health care clearinghouses. Therefore, additional information concerning portability will not be provided.

LEARNING OBJECTIVES

- Evaluate your workplace for potential HIPAA trouble spots
- Assess your own personal practices as they relate to HIPAA requirements
- Examine the potential consequences for noncompliance
- Compare and contrast the different methods of notifying patients of the privacy policy
- Examine the intricacies of business associate agreements

The accountability portion of HIPAA was set up to protect patient privacy in relation to health care. This type of information is called protected health information, and there are three types of health organizations that are required to follow the HIPAA privacy rules. These organizations are called covered entities and include health plans, health care providers, and health care clearing houses.[4]

PROTECTED HEALTH INFORMATION

Protected health information (PHI) is defined as any health information that is created or maintained by a covered entity in any form. Forms of information include handwritten or printed documents, electronic documents, and the spoken word. Protected health information consists of anything that is individually identifiable including the patient's physical or mental status (past, present or future), care that he or she has received, is receiving, or will receive, and the method of payment for that care.[2]

Protected health information may be released in limited situations. The HIPAA Privacy Rule allows protected health information to be released as permitted by the rule or at the written request of the patient or the patient's legal representative. Additionally, information must be released to the US Department of Health and Human Services if requested during an investigation of an alleged HIPAA violation or as required by state or federal law.[5]

PERMITTED USES OF PROTECTED HEALTH INFORMATION

Under the HIPAA privacy rule, the two main reasons for release of protected health information without written authorization or notification are to the individual and to business associates who are directly or indirectly involved with treatment, maintenance of treatment records or payment for treatment. Additionally, protected health information may be released in facility directories and to family and friends involved with the patient's care. Incidental release of information is also allowed, as is release of information for the sake of public interest. Limited information may be released for research purposes.[6]

POLICIES AND PROCEDURES

Each covered entity must appoint an individual as the privacy officer. This person is responsible for creation and maintenance of a HIPAA policy manual that describes all policies and procedures relating to a patient's protected health information. The policy manual must contain information concerning the covered entity's business associates and the working agreements that are in place to protect patient information handled by those associates. The manual also includes information notifying the patient about how his or her confidential information is used by the covered entity. This is done via a document called a notice of privacy practices. The patient signs an acknowledgment that he or she has received the notice, and that acknowledgment is kept on file. Should the patient choose to have his or her protected health information released, an authorization form must be available for the patient, or his or her representative, to sign prior to that information being released. The privacy officer is also responsible for updating the policy manual as needed, ensuring that all staff receives HIPAA training and that the training is documented in the employee's file. Additionally, the privacy officer is to handle all patient questions or complaints concerning the covered entity's privacy practices.[2]

The accountability portion of HIPAA was set up to protect patient privacy in relation to health care. This type of information is called protected health information...

TABLE 1[7,8]

Component	Rationale
Name, address and telephone number of covered entity	Identifiable information.
Name, address and telephone number of business associate	Identifiable information.
Brief explanation of HIPAA	Raise awareness of the business associate.
Definition of related terms	To eliminate misunderstanding of contractual contents (examples include covered entity, business associate, individual, protected health information, etc.).
List of responsibilities of the business associate	List the exact terms of the contract including specifics concerning how the privacy rule is to be followed, timelines for completion of work.
List of permitted activities of the business associate	Description of exactly how the protected health information is to be used. Also contains a provision to extend the agreement to any subcontractors hired by the business associate. Lists reporting requirements and limitations.
Procedures to follow should a breach of security occur	Covered entity must be notified.
List of consequences for noncompliance	Includes civil monetary penalties and federal criminal (monetary and incarceration) penalties.
Disclosure	Covers any possible errors or omissions in the contract and states that HIPAA regulations will prevail.
Liability insurance requirement	May be optional (according to state law).
Signatures and date of signing	Validation of the contract.
Notarization	If desired or required by state law.

BUSINESS ASSOCIATES

A business associate is typically not a covered entity, but is an individual or a business that provides services to a covered entity and has access to a patient's protected health information. Examples of business associates include (but are not limited to) transcription services, billing services, insurance claims processing services, answering service personnel, accountants, consultants (such as quality assurance or utilization review teams), members of a legal team, etc.[7]

BUSINESS ASSOCIATE AGREEMENT

All business associates of a covered entity who have access to a patient's protected health information must have a signed business associate agreement in place.[7] According to Hinkley, *et al*, the required contractual provisions include:

- Ensuring that PHI will not be used or disclosed except in accordance with the business associate contract;
- Ensuring that appropriate safeguards are in place to protect the confidentiality of PHI;
- Requiring business associates to report breaches to the covered entity;
- Requiring agents and subcontractors to comply with the same requirements that apply to business associates;
- Making PHI available to satisfy patients' rights;
- Making PHI available to satisfy HHS's right to investigate and enforce HIPAA; and
- Returning or destroying all PHI upon termination of the agreement, if feasible.[7]

An overview listing the main components of a business associate agreement and the rationale for each entry is provided in Table 1.

NOTICE OF PRIVACY PRACTICES

The notice of privacy practices must be given to the patient and a signed acknowledgment of receipt must be obtained prior to the first interaction unless an emergency situation exists. In the case of treatment necessitated by an emergency, the notice must be provided as soon as is feasible following the emergency and a signed receipt is not necessary. As the notice of privacy practices is updated, the information

need only be available to the patient. This may take place by making written brochures available, by posting the information in the reception area, or by posting the updated information on the covered entity's Web site. As the notice of privacy practices is updated, it is not necessary to obtain an updated, signed acknowledgment of receipt from each patient as long as the necessary updates are available upon request. The document must not use legal or medical terminology, but must be written in terms that most patients can easily understand.[9]

An overview listing the main components of a notice of privacy practices and the rationale for each entry is provided in Table 2.

TABLE 2[9, 10]

Component	Rationale
Name, address, and telephone number of covered entity.	Identifiable information.
Brief explanation of HIPAA and definitions for any terms that the patient may not understand.	Patient education.
Disclose how private health information is used, stored, and protected.	Raise awareness of the patient.
Explain how changes in the notice of privacy practices are handled.	General patient information.
Patient's rights and responsibilities are explained.	Inform patient of his or her rights and responsibilities.
Describe the mechanism by which a patient may make a complaint regarding HIPAA.	General patient information.
Explain the legal duties of the covered entity.	General patient information.
List the name and contact information of the privacy officer.	Raise level of patient confidence.

PATIENT AUTHORIZATION

A covered entity must secure that patient's permission in writing prior to releasing any protected health information that does not fall under permitted usage or is not covered by a business associate agreement. The patient (or the patient's legal proxy) must sign and date an authorization form that states exactly what information is to be released, to whom and for what purpose. The date or date range for which the authorization is effective is noted, and the method for revocation of the authorization is also included.[9] A log should be kept in each patient's chart documenting any release of information.[11]

OPERATING PROCEDURES

When developing the policies and procedures for protecting the patient's health information, the two main concerns for consideration are privacy and security of information that is to be exchanged between the covered entity and other covered entities, the patient, and business associates, as it applies to written or printed information, electronic information, and spoken information.[12]

Written or printed information is anything that is on paper, including faxes.[13] Some methods of protecting written or printed information include using patient sign-in sheets that contain minimal protected information, placing treatment sheets and staff assignments away from areas where they may be viewed by non-employees, ensuring that patient charts are secure, such as in a locked cabinet or storage room, or by restricting access to the storage location, and placing fax machines where they are not visible to non-employees.[14]

Electronic information is anything that is stored in a computer or that is transmitted electronically (excluding faxes). Some methods of protecting electronic information include restricting physical access to computers, including placing computer monitors in locations where they cannot be viewed by non-employees, restricting access to computer files and e-mail accounts, use of firewalls to protect computer files, use of passwords to access computer files and e-mail accounts, and remembering to log off when the computer is not in use. Also, maintenance of computer software and routine backup of computer files is necessary. Laptop computers and personal digital assistant (PDA) devices must be stored in a secure location. Any type of file sharing between covered entities and their business associates, as well as file sharing with patients (for example, access to laboratory results), must be secure.[14]

Spoken or verbal information is anything that is said about the patient. Some methods of protecting spoken information include conducting telephone and face-to-face conversations with patients or about patients in private areas so that the conversation is not overheard by non-employees. Employees must also use caution when communicating with the patient by telephone that information is not inadvertently given to someone other than the patient. For example, messages concerning appointments and lab results should not be left on an answering machine without the consent of the patient because someone else could intercept the message or overhear the message being played back.[14]

STAFF TRAINING

One of the responsibilities of the privacy officer is to ensure that the staff has been trained according to the HIPAA policy and procedure manual of the covered entity as part of his or her initial orientation and annually thereafter. Documentation of the training must be maintained in the employee's file. Training should include an overview of the policies and procedures and a review of the patient's rights. The consequences for violation of the policies and procedures as set forth in the manual are also made known to the employee, who may be legally held personally responsible for any violation that may occur.[11]

CONSEQUENCES OF NONCOMPLIANCE

Employees of covered entities who do not comply with the HIPAA Privacy Rule by disclosing or improperly using a patient's protected health information could face civil and federal charges. "Improper use or disclosure of PHI could result in civil monetary penalties of $100 per incident, or as much as $25,000 per person, per year, per standard. Because certain criminal violations qualify as a felony, criminal penalties can range from $50,000 to $250,000 and up to 10 years in prison."[2] All employees of a covered entity should be aware of the severity of the criminal penalties and take compliance with all HIPAA regulations in all aspects of the organization seriously.

EVALUATION OF THE HIPAA COMPLIANCE PROGRAM

Most instances of failure to comply with the HIPAA compliance program are inadvertent and, unfortunately, some are purposeful. In order to maintain compliance and reduce the risk of suffering the penalties of noncompliance with the HIPAA regulations, ongoing audits or self-evaluations should occur on a regular basis. Typically, the responsibility for evaluation of the HIPAA compliance program falls to the privacy officer. The evaluations may also be conducted by the risk manager or by an outside consultant. First, the contents of all documents that relate to HIPAA should be compared to the actual regulation to ensure accuracy and thoroughness. Then, actual compliance with the prescribed policies and procedures should be assessed and any corrective action taken. Physical inspections of the facility may also turn up unexpected policy violations. A task as simple as sitting in a reception area while watching the activities and listening to any

In order to maintain compliance and reduce the risk of suffering the penalties of noncompliance with the HIPAA regulations, ongoing audits or self-evaluations should occur on a regular basis.

verbal interactions that involve protected patient information may prove useful in identifying any problem areas. If a violation is suspected, immediate corrective action (that may actually be very easy to implement) must be taken to avoid a possible patient complaint. A potential government-initiated investigation will be time consuming and will take personnel away from his or her normal duties and may result in punitive action.[15]

Numerous tool kits for self-evaluation of HIPAA compliance programs are available online or for purchase.

CONCLUSION

Each facility must maintain a HIPAA policy manual that describes all policies and procedures relating to a patient's protected health information. Business associate agreements are needed between the covered entity and any organizations that are contracted to provide service to the covered entity that involve protected health information. Additionally, a notice of privacy practices informing the patient of his or her rights concerning protected health information and how his or her protected health information will be used by the covered entity must be developed and provided to each patient. The notice must be provided to the patient and a signed acknowledgment of receipt must be obtained and retained by the covered entity. The patient must authorize in writing any release of protected health information that does not fall under permitted usage or is not covered by a business associate agreement. All staff members must receive and have documentation of HIPAA compliance training upon hire and annually thereafter. The consequences for violation of HIPAA regulations are harsh and may involve fines of up to $250,000 and 10 years in prison for the most severe offenses.

ABOUT THE AUTHOR

Teri Junge, CST, CFA, FAST, BS, is the surgical technology program director at San Joaquin Valley College in Fresno, California. She also serves as AST's editorial review consultant. Ms. Junge recently finished her bachelor's degree in health services administration.

REFERENCES

1. Frimpong, J., Rivers, P. (2006). *Health insurance portability and accountability act: blessing or curse?* Journal of Health Care Finance. New York: Fall 2006. Vol. 33, Iss. 1; pg. 31,9pgs. Retrieved on December 6, 2008, from ***http://proquest.umi.com/pqdweb?did=1152143131&Fmt=3&clientId=4684&RQT=309&VName=PQD***
2. Ziel, S. (2002). *Get on board with HIPAA privacy regulations*. Nursing Management. Chicago: Oct 2002. Vol. 33, Iss. 10; pg. 28, 3 pgs. Retrieved on December 7, 2008, from ***http://proquest.umi.com/pqdweb?did=223140251&Fmt=3&clientId=4684&RQT=309&VName=PQD***
3. Gruber, J., Madrian, B. (1994). *Health insurance and job mobility: the effects of public policy on job-lock*. Industrial & Labor Relations Review, Vol. 48, 1994. Retrieved on December 6, 2008, from ***http://www.questia.com/googleScholar.qst;jsessionid=J7yTpmRQnGpGcYlhjm7nlnNPJ5tsY1Qy3fvdKW1bJK0l8Dk63yCv!515286004?docId=98939193***
4. Davino, M. (2004). *Covered entities*. Medical Economics. Nov 3, 2004 v81 i21 p25 (1). Retrieved on December 6, 2008, from ***http://wf2dnvr6.webfeat.org/***
5. United States Department of Health and Human Services. (2008). *HIPAA medical privacy—national standards to protect the privacy of personal health information*. Retrieved on November 23, 2008, from ***http://www.hhs.gov/ocr/hipaa***
6. Guthrie, J. (2003). *Time is running out--the burdens and challenges of HIPAA compliance: a look at preemption analysis, the "minimum necessary" standard, and the notice of privacy practices*. Annals of Health Law Pub.**:** 2003**,** Volume: 12**,** Issue**:** 1**,** Pages: 143-77, V retrieved on December 7, 2008, from ***http://www.ncbi.nlm.nih.gov/pubmed/12705207?ordinalpos=1&itool=EntrezSystem2.PEntrez.Pubmed.Pubmed_ResultsPanel.Pubmed_DefaultReportPanel.Pubmed_RVDocSum***
7. Hinkley, G., Glitz, R., & Hirsch, W. (2003). *Do you know your business associates?* Healthcare Financial Management. Westchester: Jan 2003. Vol. 57, Iss. 1; pg. 54, 6 pgs. Retrieved on December 7, 2008, from ***http://proquest.umi.com/pqdweb?did=276608411&Fmt=4&clientId=4684&RQT=309&VName=PQD***
8. United States Department of Health and Human Services Department of Human Rights. (2006). *Medical privacy—national standards to protect the privacy of personal health information sample business associate contract provisions*. Retrieved on December 8, 2008, from ***http://www.hhs.gov/ocr/hipaa/contractprov.html***
9. Sarraille, W., Spencer, A. (2003). *Assembling the HIPAA privacy puzzle*. Healthcare Financial Management 57 no1 46-52 Ja 2003. Retrieved on December 9, 2008.
10. United States Department of Health and Human Services Office of the Assistant Secretary for Planning and Evaluation. (2008). *Section 164.512 notice of privacy practices; rights and procedures*. Retrieved on December 9, 2008 from ***http://aspe.os.dhhs.gov/admnsimp/nprm/pvcnprm3.txt***
11. Caplin, R. (2003). HIPAA: *Health insurance portability and accountability act of 1996*. Dental Assistant. Chicago: Mar/Apr 2003. Vol. 72, Iss. 2; pg. 6, 2 pgs. Retrieved on December 9, 2008, from ***http://proquest.umi.com/pqdweb?did=324849131&Fmt=4&clientId=4684&RQT=309&VName=PQD***
12. McNealy, T. (2008). *HIPAA compliance training*. POWERPoint accessible to San Joaquin Valley College faculty.
13. Dodek, D., Dodek, A. (1997). *From Hippocrates to facsimile. Protecting patient confidentiality is more difficult and more important than ever before*. Canadian Medical Association. Journal. Ottawa: Mar 15, 1997. Vol. 156, Iss. 6; pg. 847. Retrieved on December 10, 2008, from ***http://proquest.umi.com/pqdweb?did=418342341&Fmt=3&clientId=4684&RQT=309&VName=PQD***
14. Pabrai, U., (2003). *Getting started with HIPAA (1st ed)*. United States: Course Technology PTR.
15. Ross, L., Friedman, M. (2006). *HIPAA privacy audit tool*. Healthcare Financial Management. Westchester: Feb 2006. Vol. 60, Iss. 2; pg. 133, 4 pgs. Retrieved on December 9, 2008, from ***http://proquest.umi.com/pqdweb?did=989047281&Fmt=4&clientId=4684&RQT=309&VName=PQD***

SURVEY RESULTS

Prior to researching information for this article, the author conducted a qualitative survey of 10 covered entities. Ten survey questions were asked of the individual or group of individuals responsible for setting up the HIPAA compliance program at their facility (Please refer to Appendix 1).

Of the 10 facilities surveyed, a single person was responsible for the program at half of the facilities. There were also teams of two at three facilities, one team of three, and one team of four.

Of the 10 facilities surveyed, five facilities put the HIPAA compliance program together from scratch, two facilities hired consultants, and three facilities purchased planning kits. Of the two facilities that hired consultants, both were very satisfied with the consultant's work. Of the three facilities that purchased planning kits, only one was satisfied with the contents of the kit. The most challenging part of program implementation was reported as time constraints by six of the respondents, one reported that choosing a consultant was the most challenging, one reported problems with the print shop, and two reported no challenges.

Eight out of 10 facilities reported compliance problems with the physical layout of the facility and nine out of 10 facilities reported problems with personnel not following the regulations. None of the facilities reported performing regular comprehensive evaluations of the HIPAA program and three are not doing any type of evaluation at all. Of the 10 facilities surveyed, only one reported a relevant patient question about HIPAA. Ninety percent of the facilities reported that they had no HIPAA violations that resulted in citations.

APPENDIX 1 – SURVEY QUESTIONS AND RESPONSES

Please explain who was responsible for setting up the HIPAA compliance program at your facility.	1. I did it myself. 2. I was the only one responsible for setting up the HIPAA compliance program. 3. Two of us were assigned to the task. 4. The owner and I worked together on the program. 5. Just me. 6. It started out as a committee of four, but I ended up doing all of the work without any input from the other three. 7. I was. 8. Me, by myself. 9. Me and one other person. 10. Three of us worked on the assignment together.
Would you please describe the planning and implementation process for the HIPAA compliance program at your facility?	1. I did the research online and set up the program. 2. I hired a consultant. 3. We did quite a bit of research and then decided to purchase a prepackaged program. 4. Neither one of us had much time, so we decided to buy a program from the internet. 5. I did everything. 6. When the committee fell apart, I got permission from the boss to hire a consultant. 7. I started out thinking that I would do everything myself, but it was too much so I bought a kit and worked from there. 8. I researched the options and because of cost constraints I put the program together on my own. 9. We did it all. 10. We divided up the work at the start of the project and then put the finishing touches on together.
If a proprietary service (such as a consultant or document center) was used to provide assistance with planning and implementing the program, please describe the amount of the work that was accomplished by the service?	1. N/A. 2. The consultant did about 95% of the work. 3. About half. Even with the purchase of a program, we still did quite a bit of work on the project. 4. The program was good, but we had to tailor it to our facility, so I would say about 75%. 5. Does not apply. 6. The consultant did most of the work, I'd say about 90%. I just had to approve the final documents and train the staff. 7. The kit provided about half of what I actually needed. It was a bare bones kit. I should have done more research before deciding. 8. Did not use. 9. We did not use a service. 10. N/A.

APPENDIX 1 – SURVEY QUESTIONS AND RESPONSES

If you relied solely on a proprietary service to provide everything necessary for implementation of the program, what did you like or dislike about their work?	. N/A. . I was very pleased with the consultant's work - she took care of everything. . We were not pleased. The program was basically an outline and we had to fill in all of the information. . The program that we bought met our expectations and was satisfactory. . Does not apply. . Yes, I really liked the consultant. He did absolutely everything! . I really disliked the fact that after spending all that money I still had to do a lot of the work myself. . Does not apply. . We did not use a service. 10. N/A.
Please describe what was the most challenging part of planning and implementing the program.	1. Finding the time to do it. 2. Interviewing the three consultants and deciding who would be the best fit. 3. Realizing how much work that the owner and I still had to do after purchasing a prepackaged program. 4. Working with the people at the print shop to make sure that all of the documents were ready by the time we needed them. 5. I wasn't able to train the staff all at the same time, so I had to repeat the class four times. 6. The consultant pretty much took care of everything. If there were challenges, I was not aware of them. 7. Thinking that I could do everything myself and then caving in a buying a kit. 8. I wish there had been money to hire a consultant because it took me almost a month of working full time (+) to get the HIPAA program together. 9. We didn't really have any problems. 10. Finding time for the three of us to meet to review and finalize the program.
What concerns do you have about maintenance of the program that relate to the physical layout of your facility?	1. The FAX machine had to be moved because it was too visible. 2. We should have planned for a private consultation room. 3. Now that we have redirected traffic to the restroom, we can put the patient's charts outside of the exam rooms again. 4. I am concerned about security of the patient's charts because they are not locked up. 5. The walls between the exam rooms are not soundproof. 6. So far, no concerns have arisen. 7. The scale is in a busy hallway. 8. People in the waiting room may be able to overhear telephone conversations. 9. The sign in sheet at the front desk was visible to all and asked for lots of private information, so we simply stopped using it. 10. None yet.
What concerns do you have about maintenance of the program that relate to the personnel at your facility?	1. One employee shared her computer password to another employee. 2. There is no place to hold a private conversation, so we have to really concentrate on keeping our voices low and watching to make sure that nobody hears who shouldn't. 3. No personnel problems so far (that I know of). 4. The patients are a bigger problem than the personnel because this is a small community and they all know each other. 5. We have a large staff and ensuring that the training is up to date is huge. I try to do all of the training annually, but every time we get a new employee they are off the schedule. Then to get them on track with everyone else, sometimes they take the training twice on one year, so that they are in sync with everyone else. 6. The hardest thing is getting the employees to tell me when we start running low on the printed material so that I can order more before we run out. 7. One employee is constantly leaving charts, lab reports, etc. scattered around the office where they could be seen by other patients and their family members. 8. We had an employee tell her mother that another family member came in for treatment and provided details of the visit. This was reported to HIPAA as a violation and is currently under investigation. This is the only personnel problem that we have had. 9. One employee was using the phone in the reception area to call in prescriptions to the pharmacy. People in the waiting room could hear the conversation. This actually came to our attention because someone in the waiting room reported it to the office manager. 10. We need to set up a formal training program for the employees. So far, we have been doing it from the top of our heads without a checklist. Three of us share the responsibility for training and I think that we each focus on different aspects

APPENDIX 1 – SURVEY QUESTIONS AND RESPONSES	
What types of evaluations are carried out to ensure effectiveness of the program?	1. Requests for information are tracked to be sure that written releases are obtained before the requested information is sent out. 2. All employees are trained and the training is documented in his or her personnel file. 3. We conducted one patient satisfaction survey, but very few patients responded and I don't think that many of the ones that did actually understood what we were asking. 4. None yet. We just opened about a month ago. 5. I guess the fact that the patients are complaining about having to sign a release to get information released to a family member is a good indicator that we are doing something right! 6. We have a HIPAA binder with all of the regulations and documents in it, but I don't think that anyone is making sure that we follow the instructions. 7. Are we supposed to be doing evaluations? Like what? 8. We don't have time to do evaluations. 9. When I have time, I randomly audit patient charts to see if the front office staff is getting them to sign the receipt for the Notice of Privacy Practices. 10. About twice a year I make sure that the Business Associate Agreements are up to date.
What types of questions, if any, do the patients ask about the program?	1. None, most are familiar with the privacy policies from dealing with other facilities. 2. None. 3. I can't recall anyone asking, but I could check with the receptionist if you need more information. 4. They just sign the receipt without asking. 5. Some people ask why they have to sign the HIPAA document at every facility, but that's it. 6. None. 7. They don't ask. 8. We had one patient ask if the privacy policies would prevent her ex-husband from getting information about her health because she was still on his insurance. 9. We stopped using a sign-in sheet at the front desk and the patients quite often ask about that. 10. I can't remember anyone asking questions about HIPPA. They are more concerned about how long they might have to wait.
Please list any citations that your facility has received for HIPAA violations and the describe consequences.	1. None. 2. No citations. 3. One patient threatened to report us for a violation, but once we explained to her that we were allowed to release information to her insurance company in order to receive payment, she understood and did not file a complaint. 4. N/A. 5. None, so far. 6. None. 7. N/A. 8. One complaint has been filed, but it doesn't look like the facility will be cited. The (former) employee who violated the policy will be held responsible and will most likely pay a significant fine however the investigation is ongoing. 9. N/A. 10. None.