

HIPAA - Privacy And Security Audit For Provider Practices

THIS IS A MODEL AUDIT. IT WILL NEED TO BE CHANGED TO MEET THE PARTICULAR NEEDS AND CIRCUMSTANCES OF ANY TRUSTED SOURCES DEVELOPING AN AUDIT.

The health care industry must come into compliance with the new privacy and security requirements of the Health Insurance Portability and Accountability Act (HIPAA). These requirements apply to payors, institutions, and healthcare professionals and providers, from the largest multi-state integrated delivery networks to solo practice professionals.

All individuals involved in the health care delivery system must start now to prepare for HIPAA.

Actually, HIPAA does ***not*** apply to all health care providers. Rather, it only applies to those who engage in “standardized electronic transactions,” as defined by the federal government. For example, if you submit claims or perform eligibility checks electronically, either directly or through a third party, e.g., a billing service, then you are subject to the HIPAA privacy and security requirements. In addition, if you perform any transactions electronically, the information in both your ***electronic and paper*** records are covered by HIPAA.

This audit is intended to be a starting point for solo and small practice professionals. This includes physicians, dentists, physical and occupational therapists, psychologists, social workers, and all other health care professionals. This audit provides professionals with a list of 20 considerations. Each of these considerations is presented in the form of a statement. Depending on how you respond to these considerations, you can determine how much you will have to do to prepare for HIPAA. To assist you in thinking about the changes you may have to make in your office, a series of suggestions are presented under each consideration regarding how to ensure your practice meets the HIPAA privacy and security requirements.

This audit is a preliminary step. It is not intended to be comprehensive and it is not intended to provide a comprehensive guide to meeting the HIPAA privacy and security requirements. Further information will be developed by WEDI/SNIP over the next several months. These documents will help you to prepare for HIPAA. In the meantime, it is important that you become aware of, and get a start toward, meeting the HIPAA requirements.

The following 20 considerations are intended to help you audit your practice and to determine if you will need to make any changes to meet the privacy and security requirements of the Health Insurance Portability and Accountability Act (HIPAA).

If you answer any of the following statements “False” you may need to change office procedures.

1. My office does not use a patient sign in sheet that includes confidential patient information.

True False

A sign-in sheet will allow patients who come into your office later to learn the identity of other patients who came to your office earlier. This is acceptable, so long as the sign-in sheet does not contain confidential patient information such as reason for the visit. In some cases this information seems very innocent. However, some physicians specialize in patients with sensitive issues or conditions, e.g., cancer, psychological problems, or pregnancy, and simply disclosing that an individual has had an appointment with you for a specific purpose may be a breach of patient confidentiality. At a minimum, the sign-in sheet should be changed periodically during the day.

2. My office does not place patient schedules in any places that may be seen by patients or other non-staff individuals.

True False

Some practices print out the schedule for the day and post it for the professional staff. Often the schedule is posted where it may be seen by a patient – either in an examination room, in a corridor, or on a door. This may result in the unauthorized disclosure of patient information. As with consideration 1. above, disclosing information about a patient may be a breach of patient confidentiality.

3. In my office, all confidential conversations take place to the maximum extent possible in areas that cannot be overheard by other patients or non-staff individuals.

True False

Conversations may be easily overheard in many settings. For example, a receptionist may schedule appointments or provide results over the telephone. This requires taking and verifying the name of the caller, as well as discussion of medical information, e.g., the reason for the appointment or the results of the tests. If patients and others are sitting in the waiting room, they may hear this exchange of confidential information, and this could represent an unauthorized disclosure of patient information. The same is true of conversations between staff members in the hallway and if a professional takes a call from a patient in the presence of another patient, e.g., in an exam room or if a professional dictates notes to a recording device. (Providers must use their best professional judgment to reduce the risk of such information being shared, but do not have to guarantee it can never occur.)

4. In my office patients and non-staff individuals cannot gain access to our computers or fax machines and cannot view our computer screens.

True False

Offices use computers for a variety of reasons, including billing, accounts receivable, scheduling, and medical records. Usually computers and fax machines are placed only in the reception area, although sometimes they are throughout the office, including in patient exam rooms. It is important that only staff members can gain access to the fax machines and computers. This access includes restricted physical access as well as restricted viewing access. In addition, computers should have screen savers so that unauthorized people cannot read the information if they happen to wander into a restricted area, and computers should be password protected. When the staff person steps away from their computer for a period of time, the staff person should be required to re-enter his or her password.

5. Each computer user in my office has a personal computer password, these passwords change on a regular basis, and passwords of terminated employees get deleted immediately.

True False

It is important to ensure that each person in your office has access only to the computer(s) and information to which they are entitled. Toward that end, each user needs to have his or her own password. In addition, passwords need to be kept confidential (i.e., not shared with anyone else) and need to be changed on a regular basis to ensure security. Passwords must *never* be left on “Post-it” notes next to the computer.

6. In my office patients and other non-staff individuals do not have any opportunity to access patient medical records, laboratory reports, and faxes.

True False

Paper medical records are located in a number of places around the office, including the receptionist area, bins in the exam rooms, on the professional's desk, and at check out. It is vital that no patient or non-staff individual have access to any medical records at any place in the office. For most offices, this will require a change in the manner in which medical records are handled and stored.

7. My office has formal documented procedures to ensure patient confidentiality when transferring to other offices paper files, orders, images, and specimens.

True False

It is very important that every office have formal policies for the transfer of confidential patient information outside its office. Your office staff must understand these policies. You must make sure that only appropriate information is transferred and that it is transferred to the proper individuals. (You may need specific authorization from a patient to transfer information.) If you use e-mail, you must ensure that the e-mail is secure. If you use couriers, you must ensure that they will keep the information confidential in transit and will deliver it only to authorized individuals. If you use a transcription service, you must ensure that the transcription service can keep your information confidential in compliance with the HIPAA requirements. Even if you currently have such policies, they will have to be reviewed to ensure that they meet the HIPAA requirements, and you may have to change your agreements with your business associates to ensure that they comply with the HIPAA requirements.

8. My office has formal documented procedures for the acceptance of confidential patient information from outside of our office.

True False

As with records you send offsite, you will need to have formal policies for accepting confidential patient information from outside your office and keeping it confidential, including e-mail. Your office staff must understand these policies. Even if you have such policies in place, they will have to be reviewed to ensure that they meet the HIPAA requirements.

9. My office has confidentiality statements in place and we make patients aware of our confidentiality policies.

True False

HIPAA requires each health care professional to have confidentiality statements. These statements must be posted in a prominent place in your office. In addition, patients must sign a consent form allowing you to release their confidential information for billing and other purposes. Even if you have confidentiality policies in place and make patients aware of your policies, they will have to be reviewed to ensure they meet the HIPAA requirements.

NPRM - Consent is no longer needed under the NPRM for the use and disclosure of confidential patient information; however, each health care professional still needs to give Notice to his or her direct care patients and document that the notice has been given or that a good faith effort was made to provide the notice.

10. My office has formal privacy and security procedures regarding access to confidential information, access to computer information, and access to areas of the office that may contain confidential information.

True False

Unauthorized personnel must never have access to confidential information. Your office must have formal policies and procedures to ensure that only appropriate staff and other individuals gain access to confidential information. This may mean limiting access to certain parts of your office, to certain computers, or to certain programs or files in your computers. (For example, if you have separate accounting staff, they do not need to see patient encounter notes, just the billing form prepared by the treating healthcare professional, while the cleaning staff should not be able to see any confidential information.)

11. My office requires the return of all keys and other items that allow access to the office and to computer files when a person no longer is authorized to access information.

True False

Unauthorized personnel must never have access to confidential information. This includes all staff and other individuals who may have, at one time, be authorized to have such access. Your office must have formal policies and procedures to ensure the return of all keys and other items that allow access to information, both physical access and computer access.

12. My office has formal privacy and security policies for all office personnel, training for all office personnel, and the training of each individual is documented.

True False

All office personnel must receive training about your privacy and security policies and records must be kept of the training. The policies must detail which personnel have access to different kinds of confidential information in different circumstances, personnel clearance procedures, procedures to be followed when a member of the office staff is terminated, and procedures for identifying and correcting potential problems. The training requirements should be included in your human resources policy manual or booklet. In addition, you must have a formal policy manual that details all of your privacy and security procedures. Even if you have a policy manual in place, it will have to be reviewed to ensure that they meet the HIPAA requirements.

13. If my office uses laptops or other portable equipment that holds confidential patient information, this equipment is secure and can only be accessed by authorized personnel.

True False NA

Many offices use portable equipment, including laptops, calendars, and “personal assistants.” All of these devices may contain confidential information that must be kept secure in an appropriate fashion. Your office must have policies and procedures regarding the setup, use, security and disposal of this equipment.

14. My office has policies and procedures in place to ensure patient confidentiality by off-site contractors, such as billing and accounting services.

True False

You are responsible for ensuring your confidential information remains confidential, even when it is sent off-site. This is not a concern when you send information to another health care provider or a health insurance company – they also are required to comply with the privacy rule and protect the information they receive. In addition, most billing services will be covered by the rules, although you need to double check with them. However, many businesses are not covered by the rules, e.g., auditors and software vendors. You need to have agreements with these businesses to ensure the confidentiality of any patient information they will see or transfer.

15. My office has a comprehensive survey of all of our computer systems, including all software.

True False

The security rules require you to keep a complete listing of your computer systems, including all software. This will help you manage your systems and help to detect any problems that might lead to a breach of patient confidentiality. Remember: Confidential information is contained in billing and accounting records and in letters to patients and other health care providers, as well as in the medical records.

6. My office has a disaster plan to protect patient information, contingency plans in the event of a computer systems failure, perform regular virus checks, and corrects any identified problems.

True False

You must ensure that you can access confidential information, even in the case of a disaster. For computer records, this can be fairly simple – backup the computer files on a daily basis and store the backup offsite. For paper records, this can be more difficult. In addition, you must ensure your confidential information is safe and cannot be seen or altered without your permission. Electronic information – including billing records and correspondence – is subject to attack if it is not protected from computer viruses and unauthorized intruders (hackers).

17. All confidential information – paper and electronic – is stored with appropriate safeguards.

True False

You must ensure that all confidential information is protected from inappropriate access. This includes both electronic and paper records. For electronic records, you need to use passwords and other methods to ensure that only authorized people have access to information. For paper records, you will need to ensure your records are stored and locked in a secure manner.

18. Internet transmissions, including e-mail, and telephone conversations are secure.

True False

You must be sure that internet and telephone conversations are secure. In the case of the internet – most commonly e-mail – you must ensure communications are “encrypted.” In the case of telephone conversations, you must make reasonable efforts to ensure that others are not listening in, e.g., on a second telephone. In most cases, the staff needs to have some assurance of the identity of the person with whom they are communicating.

19. My office has patients sign a consent form. True False

Patients must sign a consent form allowing you to release their confidential information for treatment, billing and other purposes. Even if you have such a form in place, you need to review it to ensure that it meets the HIPAA requirements.

NPRM - Consent is no longer needed under the NPRM for the use and disclosure of confidential patient information; however, each health care professional still needs to give Notice to his or her direct care patients and document that the notice has been given or that a good faith effort was made to provide the notice. Professionals may want to have patients sign a form acknowledging that they received the Notice and then place that form in the medical record.

20. My office has confidentiality statements on all faxes and e-mail sent by the office staff.

True False

All faxes and e-mail should state the confidential nature of the contents and have instructions should the fax or email be misdirected.

This audit is a preliminary step. It is not intended to be comprehensive and it is not intended to provide a comprehensive guide to meeting the HIPAA privacy and security requirements. Further information will be developed over the next several months. These documents will help you to prepare for HIPAA. In the meantime, it is important that you become aware of and get a start toward meeting the HIPAA requirements.

Document provided by 2002 WEDI – SNIP, visit the website, <http://snip.wedi.org/>, for up-to-date information.