

Chapter 5

Security and privacy

A critical issue

It is essential for medical practices to maintain the privacy and confidentiality of their charts and records. Compromised medical records can cause people to lose their jobs and destroy lives. This is why the Federal Health Insurance Portability and Accountability Act (HIPAA) mandates several penalties for failing to protect medical information.

By the same token, good health care rests on a physician's ability to access critical information quickly and share it with other professionals who need to know. People can die if essential information is missing, or not immediately shared with the right person. If the data are stored on paper, they can be lost in a fire or a natural disaster, as we know from Hurricane Katrina that destroyed many medical practices.

Good security begins with education

Everybody in your practice or clinic, from janitors to surgeons, needs to understand the importance of security. They all need to know what is vulnerable—the threats and risks—and what measures they need to take if they see a potential breach. The threats are many. You can put up firewalls and other measures to thwart hackers bent on stealing data or installing viruses and worms on your software. A disgruntled employee might decide to take out his or her revenge on your records. That's not to mention the possibility of embezzlement or stealing financial records.

Some security starters

One thing you need to do is work with your staff to develop a comprehensive data security policy. You'll need to identify what you need to protect, how it's best protected, and who on your staff is responsible for security.

Of course, you'll want to protect everything on your system, but the reality is that you have to set priorities. Some data are more important than others are. You will wind up spending the greatest amount of resources protecting the most critical data.

Some security issues are simple and free. Your employees should memorize their passwords. No writing them down and stashing them somewhere handy. Each staff member should take care of his or her own computer, making sure their anti-virus software is kept up to date and running it and anti-spyware before they leave for the day.

Many EMR vendors are now adding biometric security to their system, that is, fingerprint recognition. Gone are the days of using passwords to log in or log off. You simply flash one of your digits and it's done.

Software to stop viruses, worms and spyware

You need to buy and install anti-virus and anti-spyware/adware software. A good one is AVG which updates regularly and doesn't use as much computing power as many other systems. Whatever system you buy, it should update itself automatically every day.

The dangers of a system failure or electrical blackout

Banks and other financial systems, initially wary of storing their data on computers, now zap billions in multiple currencies around the planet each day, landing accurately in accounts on all continents. If money managers and financial officers were at first disconcerted by the use of computers, they have learned to relax. Around the world banks have established back-up and other system fail-safes to ensure the security of their data. If they tried to run their business on paper, they'd go out of business.

In the end, the benefits of EMR over storing your medical data on paper are so overwhelming as to dwarf any worst-case security nightmare. While you can install EMR with confidence that your charts and other data will be safe, you of course shouldn't take security for granted; too many people can get hurt if records are lost. There are possible legal problems if data get scrambled, rewritten, or lost.

How to make sure an EMR system is secure

If you have EMR software installed on your computers, you'll have to periodically check the backup tapes and even store them in a second location. You can hire local techies to come in and back up the data. You need to be diligent about this. You shouldn't forget about it because the system appears to work just fine and you begin to relax over time.

When you close for the day, someone has the chore of backing up the data. Set up a simple system. Assign a dependable member or members of your staff and make sure his or her responsibility is clear. It should be a part of their daily routine. Not a big deal. Most reputable vendors can arrange for you to store your back-up data on their computers. If you do that, you should make sure that their computers are located in a safe, secure environment.

It's a good idea to have both a local backup and a remote backup. If you lose data due to a power outage, you can quickly restore your system from your local back up. If you lose data because your building burns down, you go to your remote backup. If your system is hosted on a server's computer, make sure you're satisfied with the care and security of your data.

If you rely on your vendor for safety, don't rely on the word of a charming salesman. Yeah, cool, dude, your records will be safe. No problem. Yadda, yadda, yadda. Just sign here and all your problems are over. Make them put the backup arrangements in writing. Make them spell out just how it is that your data will be safe. What kind of computer system are they using? Where is it located? Is it protected against fire and other calamities? Against hackers? Do they have a generator? Do they have a duplicate backup in another location? You need to make sure that both your responsibilities and those of the vendor are made clear.

Who has access

You need to make sure that if you have multiple users on your system that each person is given only permissions that he or she needs.

Secure transmissions

You need to make sure that you have proper encryption if you transmit medical data over the web via email or instant messaging.

A hacker's tactic

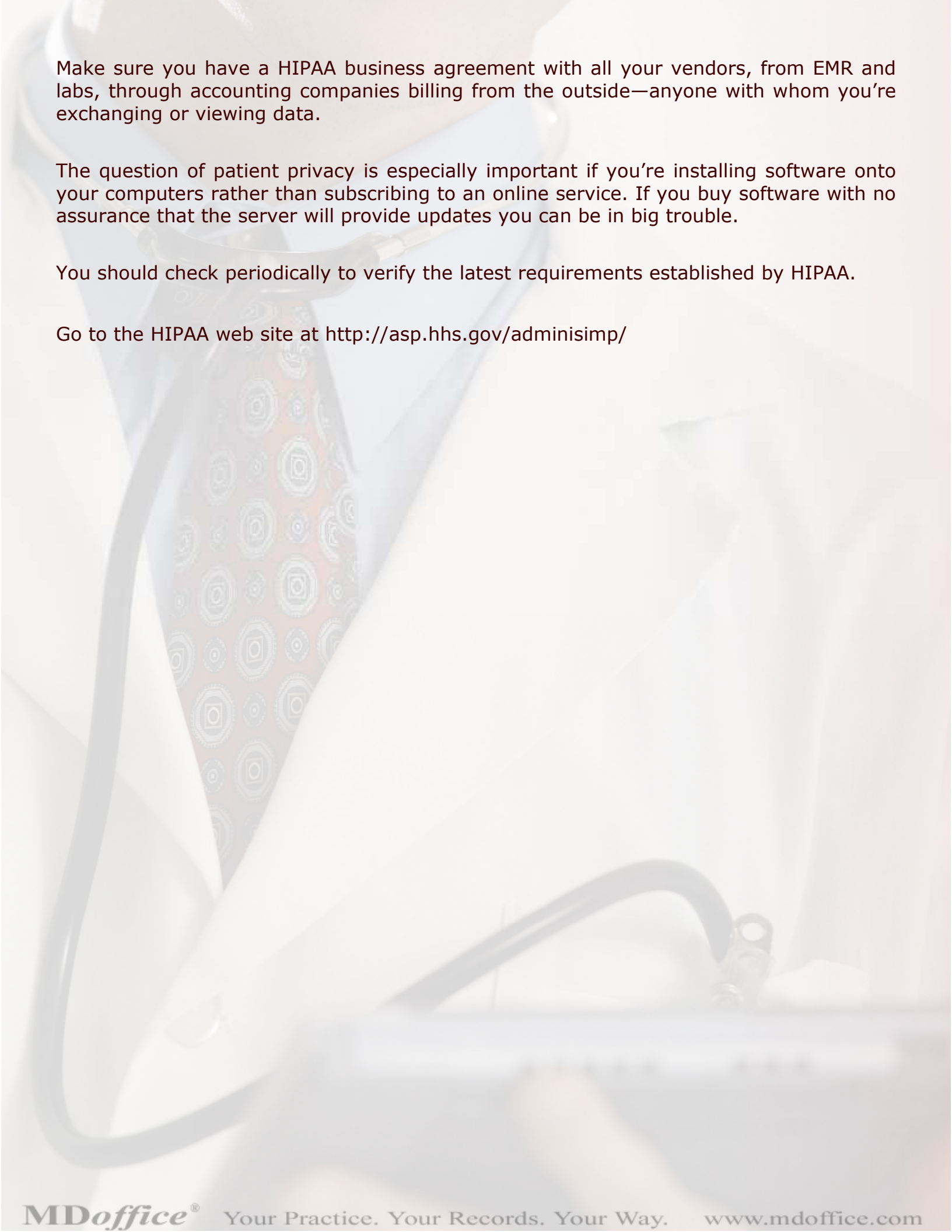
Pay attention here. Anytime you enter data into your EMR system, your software has to process it. A tactic hackers use to attack websites is to find a form and stuff too much data on it, creating a buffer overflow. The company providing your EMR needs to have data input checks to thwart this gambit. Also useful in frustrating hackers is the installation of a "sonic wall" a form of secure linked hub to separate older computers from newer work stations.

How to ensure the privacy of patients with EMR charts and files

Look for a vendor that meets the industry standards for privacy and security set by the federal Health Insurance Portability and Accountability Act (HIPAA) of 1996. HIPAA defines acceptable transaction and codes sets. Standards are pending on health plan and individual IDs, claim attachments and enforcements.

You and the doctors, nurses and members of your staff each should have a username and personal password to access data on the system. You should be able to specify which users have access to what data. That's basic to any system that you would want to use.

Additionally, your vendor should monitor new HIPAA regulations and work them into their product updates to insure that you're always in compliance. EMR systems cost money. You will want to make sure your system complies with federal standards six months or a year or two years from now. Once again, this is something your vendor should be willing to spell out in writing. It is good to have a company that's been around awhile and isn't likely to go out of business.



Make sure you have a HIPAA business agreement with all your vendors, from EMR and labs, through accounting companies billing from the outside—anyone with whom you're exchanging or viewing data.

The question of patient privacy is especially important if you're installing software onto your computers rather than subscribing to an online service. If you buy software with no assurance that the server will provide updates you can be in big trouble.

You should check periodically to verify the latest requirements established by HIPAA.

Go to the HIPAA web site at <http://asp.hhs.gov/adminisimp/>