My mother always said, “Don’t sweat the small stuff. In the long run, it doesn’t matter, and it’ll drive you crazy the quickest.” Once again, it appears my mama was correct.

As far as dentistry is concerned, the HIPAA Security Rule that goes into effect April 21, 2005, is “small stuff.” Not because you can’t get in trouble if you’re not careful; on the contrary, if personal health information is not protected according to the requirements under the Security Rule, civil penalties can be from $100, up to $25,000 per year per violation. Criminal penalties can be anywhere from $50,000 in fines and one year in prison up to $250,000 in fines and 10 years in prison. Is that likely to happen in a dental office? No, not if you take reasonable precautions to protect patients’ electronic health information.

The reason the Security Rule is “small stuff” is because we’ve really already done most of what’s required under this rule. We’ve already analyzed our practices to determine potential problem areas, so the additional requirements under the Security Rule are fairly minimal. You still have to go through all the same steps again, but it’s much easier since you’re already familiar with the general requirements.

Generally, according to the regulations, the Security Rule deals with “administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of electronic protected health information.” The major goal is to ensure that all protected health data is protected as much as possible from inappropriate use, access, modification, or destruction.

Unfortunately, computers and electronic data are vulnerable to hackers, computer viruses, and worms, as well as physical destruction, so it’s important to take steps to make sure your patients’ private health information is protected as much as possible. Dental facilities are also required to enter into business associate agreements with any companies that have access to their patients’ private health information, and are also required to ensure that their employees comply with the regulations.

Although it deals with many of the same considerations as the Privacy Rule, the Security Rule is concerned only with private health information in its electronic form, not written or spoken. Also, as with the Privacy Rule, the Security Rule only applies to health care providers that either maintain or transmit private health information electronically. However, as with the Privacy Rule, even if you don’t deal with electronic claims, or even if you don’t verify benefits electronically, the standard of care will probably require these same precautions, so it’s better to go ahead and make sure your security plan is in compliance with the HIPAA rules.

Some of the considerations outlined in the Security Rule are “required,” and some are “addressable.” The required measures must be adopted, and the “addressable” measures must be considered and then adopted if it is “reasonable and appropriate” to do so. If it is not “reasonable and appropriate” to do so, then you must document why it’s not and provide an “equivalent alternative measure.”

The good news is that the Rule clearly states that the size, type, and complexity of each facility should be considered when determining which security measures should be used. For example, a huge dental corporation with multiple offices and a large, complex computer network has different security needs than a small office with one computer at the front desk. The Rule also allows providers to consider the cost of various security measures against the risks of inappropriate use, access, or disclosure. That doesn’t mean you can say, “it’s all too expensive” and choose to do nothing. You must analyze the situation and if a security measure is reasonable and appropriate, and is not ridiculously costly for the degree of protection it offers, you need to do it.

Administrative Safeguards
According to this section of the Security Rule, administrative safeguards focus on policies and procedures in the workplace that help prevent, detect, contain, and correct security violations. The Rule requires that the office conduct a risk analysis to determine potential vulnerabilities and then adopt security measures “sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.” One employee must be designated as the Security officer. In most dental offices, the Security officer should be the same person as the Privacy officer because the requirements are so similar. This individual is responsible for recordkeeping and for establishing and maintaining the Security Rule policies and procedures.

Business associate agreements must be entered into with any outside business who, as part of their duties, has access to your patients’ data. Existing agreements under the Privacy Rule can be edited to add that the business associate must notify the dentist in the event of a known security incident, and that the business associate must “appropriately safeguard the information in accordance with [the Security Rule].” In the event a business associate fails to safeguard the information or fails to correct a problem that results in a security incident, business dealings with that associate should be terminated.

It’s important to ensure that only those employees who need access to patients’ protected health information actually have access. For example, if an employee’s only job is to process instruments, there is no reason for that employee to have access to private patient information. In the event an employee violates these administrative safeguards, the employer must establish and maintain sanctions against that employee.

To further ensure that only authorized users are accessing the system, records of system activity, such as audit logs and access reports, should be regularly reviewed. In the event a security incident is discovered, steps must be taken to fix the problem, mitigate any damages as much as possible, and document the event and its outcome.

Security incidents can also include “any occurrence that damages systems
that contain electronic protected health information,” which can include events such as a computer crash, natural disasters, fires, or acts of terrorism. The Rule requires that every office have a data backup plan, a disaster recovery plan, and an emergency mode operation plan in place so that lost data can be quickly accessed and restored in the event of a catastrophic event.

Think about this: If your office was destroyed today by a fire or a hurricane, how long would it take you to be back in operation? If you have electronic patient records and have a current, complete backup, you could be up and running in the amount of time it takes you to get a new computer. You may not have all your x-rays or some of your oldest written records, but you have enough to get going. If you don’t have these things, you don’t have anything...you don’t have your patients’ names or phone numbers, you don’t know when they’re coming in, you don’t know what needs to be done, and you don’t know what they owe you. Now, you’ve got a problem.

Back up your computer every day. Think how many transactions are completed on your computer every day...payments are entered, appointment dates are changed, patient notes are entered. If you don’t back it up, you lose a huge amount of information that may be impossible to reconstruct completely.

Also, at some point, make sure that your backup is working properly. A local dentist had his computer server crash. He took his current backup disk, inserted it in the new computer, and found there was no data. Apparently, when he thought he had been backing up his data, it was actually copying his dental software instead. He had to send his server to a data recovery company and, $7,000 later, he retrieved most of his data. If he’d had a fire, he would have been completely out of luck. It’s worth the cost of getting your computer repair person to visit your office to check and make sure that when you click on “Backup,” it’s actually writing the correct information onto the disk.

This section also requires that certain other related topics must be addressed and adopted if it’s “reasonable and appropriate” to do so. Most of these sections should be implemented, but different facilities will need different levels of compliance, so these sections are considered to be addressable, rather than required. For example, a security awareness and training program should be implemented in every facility; this may require a full-time trainer in a large corporate facility, or it may require a fact sheet and a five minute discussion in an office consisting of a dentist and his spouse.

Password protection, determining which employees have what level of access to electronic information, establishing how to end computer access in the event an employee is terminated, and determining how often the security program should be updated, must all be considered. Firewalls and anti-viral software should be installed that are adequate for the type of system and the size of the network.

Physical Safeguards
Physical safeguards are defined as “security measures to protect a covered entity’s

Continued on page 24
HIPAA SECURITY RULE
Continued from page 23

electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.” Dentists are required to establish policies and procedures that ensure that physical access to electronic data is limited only to those who are authorized to use it. The policies should also discuss workstation security and physical safeguards for each workstation and all disks, CDs, magnetic tape, and any other media that may contain private patient information.

For example, make sure that computer terminals and data disks or tape are not accessible to patients or visitors. Those that are accessible should be password protected and disks should be locked away. Lock your office when you’re not there to protect your equipment from “unauthorized physical access, tampering, and theft.” If you are in a building with other occupants, evaluate building security to ensure that access to your office is properly limited. If you are replacing your computers, make sure that all patient information is removed from the hard drive and any disks before disposal. If a computer is being removed for repair, record the name of the repair person and log in the date of removal and when it is returned. Back up any data before the computer is removed from the facility, if possible. Also, have that individual sign a business associate agreement if there is any patient data on that terminal.

Technical Safeguards
Dentists are required to implement policies that allow access “only to those persons or software programs that have been granted access rights” under the Security Rule. In other words, you need to establish protections to ensure that no one else can hack into your systems and mess with your data. You don’t want a computer savvy patient who owes you a couple thousand dollars to be able to sneak in and adjust off the balance. Also, with identity theft becoming such a huge issue, a dental office with Social Security numbers, birthdays, and addresses would be a gold mine for a criminal, so you don’t want to put you or your patients at risk.

Assign a unique name and/or number to make sure that only authorized users are accessing the system. Make sure that your emergency plan includes procedures that allow rapid access to health information in the event of a catastrophic event, including power failures. Install technical systems to ensure that the network is as secure as possible while transmitting data. Establish procedures to ensure that information cannot be accessed, edited, or destroyed without authorization. Set up hardware and software systems to ensure that any such unauthorized activity will be recorded, and establish schedules to examine the resulting audit logs in order to reveal any unauthorized access.

Consider using automatic logoffs if the system is inactive for a specific time in order to ensure that a computer is not left on inadvertently, thereby allowing unauthorized access. The Rule also suggests considering “encrypting” information so that unauthorized users would be unable to decipher any information. The problem with encrypting information is that, unless you have compatible “decrypting” software, the information is not usable. This would be a problem when sending information to another provider or a patient who may not have the software. Also, the type of information we generally send outside our facilities is mostly things like insurance claim forms and patient e-mails, which rarely contain sensitive information. For example, on your average claim form, now that insurance companies have generally stopped using Social Security numbers as identifiers, the information the hacker may receive is name, birthdate, address, and the fact that a filling was done on tooth number 31. Big deal. They can get name, address, and birthdate from public records, and the type of health information that we generally transmit on an insurance form is not particularly damaging. As a result, encryption software is probably more protection than we need and is likely to cause more problems than it solves.

That’s pretty much the basics. Keep all records relating to the Security Rule for at least six years from the date the records were created, and make sure your policies are in place by April 21, 2005. If you change your policies, review your procedures, or update your computer systems, make sure you update your documentation, as well. Happy HIPAA.