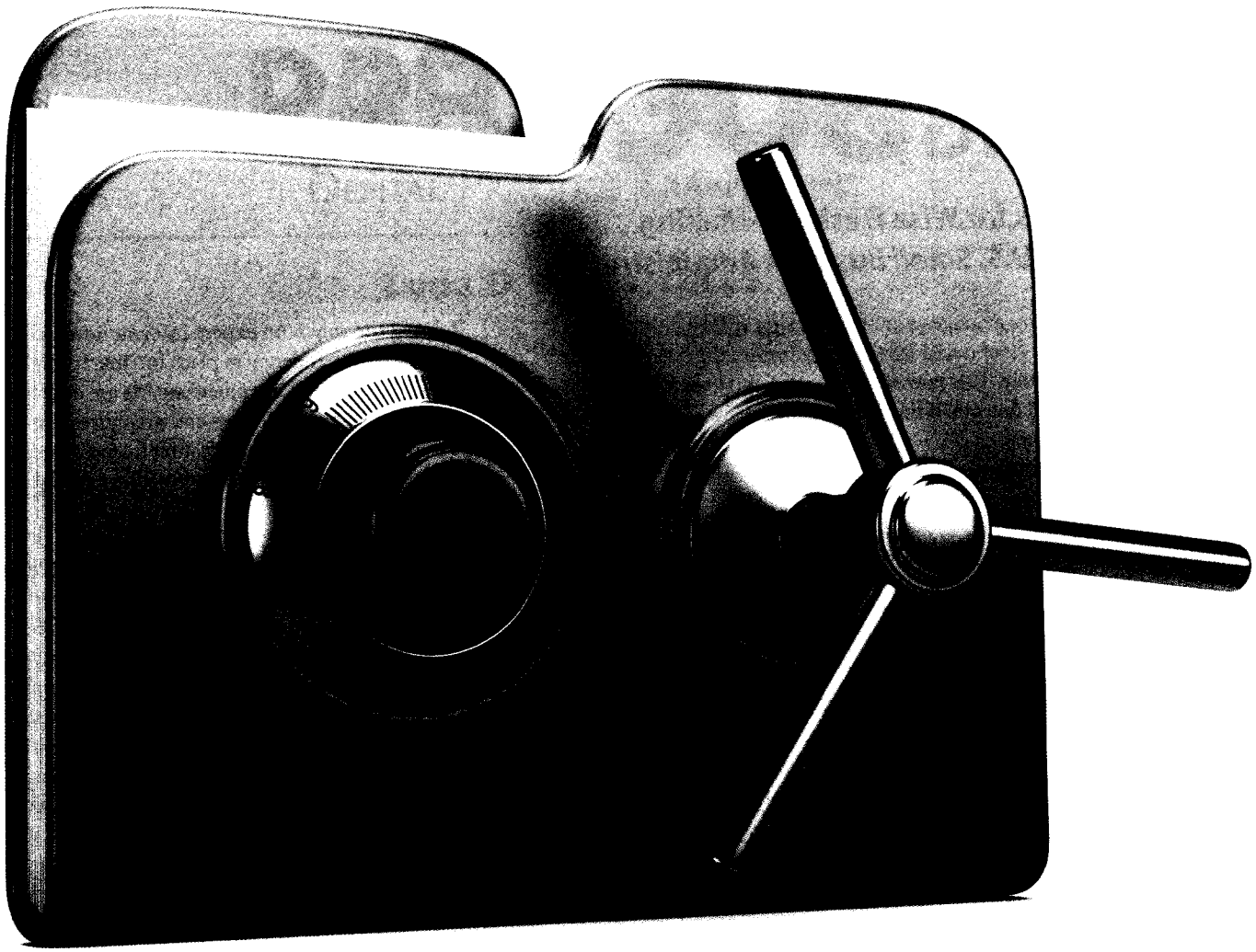

HIPAA Alert: We're From the Government ... And We're Here to Help!

By Laney Kay, JD, MPH

I've got a problem with the Health Insurance Portability and Accountability Act (HIPAA). I know … stand in line, right?

As someone who has dealt with regulatory compliance in dentistry since the late 1980s, I've dealt with regulation after regulation, and never have I seen one with the potential complications that can be caused by a HIPAA violation. Since the newest rules were passed in January 2013, the maximum penalty that can be levied is as much as $1.5 million per incidence.

Everyone agrees that there is need for some form of patient privacy. As patients, all of us have an expectation that our personal, private information will be protected and kept from being misused and improperly disclosed. However, when electronic records were pushed as the savior of modern health care, there were several unintended consequences that soon became obvious. Yes, electronic records can help make health care records more accessible to patients and their doctors. Yes, electronic records are easy to transfer and are easier to read, which is a huge benefit considering the real problems caused by many doctors' illegible handwriting. For example, in hospitals and pharmacies, electronic medical records have shown a significant benefit in reducing the frequency of medication errors. However, there are problems, as well.

Electronic recordkeeping requires multiple checkmarks and reading and dismissing those areas of documentation that aren't relevant to that specific patient's care. The result is that the time required to complete paperwork has increased so much that many doctors feel that patient care has been significantly impacted; they often spend more time on documentation than on actual patient care. The other problem, and in my opinion the main problem, is that once information is online, it's accessible to others.

The HIPAA folks don't seem to get that sometimes. We all need to understand that, by putting records online, we have traded some security for convenience. Regardless of how many precautions you take, every office can be hacked. Hackers have accessed the CIA and NSA databases; ironically, Health

and Human Services' own Healthcare.gov website has been a frequent victim of hacking attacks. With all the taxpayer money they have available to protect their databases and websites, they are still unable to completely protect private information. What are the chances that a small dental office can avoid a focused data breach attempt?

In my opinion, so long as you are taking reasonable precautions to protect electronic information, and so long as your security is sufficient for your system and is regularly maintained and updated, you shouldn't have to worry about being fined and penalized if your information is compromised. To be fair, there are a significant number of cases where offices don't receive fines or corrective actions in spite of a complaint. For example, I know of an instance where paper records were stolen, resulting in a large breach. The practice did what they were supposed to do, and HIPAA didn't fine or penalize the office.

I also agree that HIPAA considers how much of an effort is being put into protecting patient information. The offices that seem to get into the most trouble are those that haven't conducted proper risk analyses of situations and have not taken what HIPAA considers to be reasonable precautions. They haven't identified issues. If they did identify them, they didn't fix them. They haven't regularly maintained their HIPAA program, or they haven't encrypted their electronic devices. My biggest concerns are that the situations can be arbitrary, and the potential size of the fines could be fatal.

I mentioned that to one gentleman in the Department of Health and Human Services' Office for Civil Rights (OCR), the group responsible for HIPAA enforcement, and expressed my concerns. I told him that a $1.5 million fine would shut down any small business and that I was concerned that they really didn't have a feel for how much damage a fine could do to a practice that has already spent considerable time and effort trying to protect patients' health information. He stated that the government understands that, and that, so long as you are making an effort to comply, you don't start on the high end of the penalty scale. However, even a penalty on the "low" end of the scale would put many of us out of business. That's a huge problem to a small business owner.

For example, Anchorage Community Mental Health Services (ACMHS) recently agreed to settle potential violations of HIPAA with OCR and pay a $150,000 fine. OCR opened an investigation after receiving notification from ACMHS regarding a breach of unsecured electronic protected health information affecting 2,743 individuals due to malware compromising the security of its information technology resources. **OCR's investigation revealed that ACMHS had adopted sample Security Rule policies and procedures in 2005, but these were not followed. Moreover, the security incident was the direct result of ACMHS failing to identify and address basic risks, such as not regularly updating their IT resources with available patches and running outdated, unsupported software.**

In addition to the $150,000 settlement amount, the agreement includes a corrective action plan and requires ACMHS to report on the state of its compliance to OCR for a two-year period.

I recently had a meeting with some dental supply representatives. They told me they've run across many dental practices still using Windows XP, which is software that is no longer supported by Microsoft and, therefore, susceptible to security breaches. In fact, just like our ACMHS friends in Alaska who were fined $150,000, they are "running outdated, unsupported software."

If you have not reviewed your HIPAA compliance program yet in 2016, make it a resolution to follow these steps to help protect your practice from a HIPAA violation and a potentially devastating fine, whether it is $150,000 or $1.5 million.

First, make sure your staff members are well trained in HIPAA requirements and understand that they can be fired, fined, and/or prosecuted if these rules are violated. There are training manuals out there, and even if they are technical and many pages long, an office must make the effort to conduct staff training and adhere to the regulations. Staff cannot talk about patients' private health information, they must be careful how patient information is used and disclosed, and they should always disclose the minimum amount necessary. Electronic and paper information must be protected using a combination of administrative, technical, and physical safeguards. Computer security must be regularly updated and maintained. Properly encrypt your hard drive and electronic devices. You must have appropriate agreements in place with business associates. Your written HIPAA compliance program must be up to date and regularly maintained. Risk assessments must be performed on a regular basis to ensure that patient information is protected as much as possible.

Unfortunately, this may still not be enough. You can take all of these precautions and still end up with a computer breach that can potentially result in a significant cost to your practice, in time if not in actual fines. Experts have estimated that, by the time you factor in potential penalties, the costs of mitigation (such as offering credit monitoring), and the actual costs of notification, a large breach may cost as much as $200 per patient. Once you consider how many patients you actually have in your computer, you can see how that could potentially put any of us out of business.

I have been asked if there are additional steps a dental office could take in addition to staff training. A lot of it depends on your level of risk aversion. The truth is, few dentists have sustained large HIPAA fines. However, stolen medical records are now worth more than credit card records to an identity thief; as a result, small dental and medical practices are now considered favorite targets of identity theft hackers. (*"Your medical record is worth more to hackers than your credit card," Reuters, September 24, 2014.*) The reality is that this problem with probably become more significant in the future, so we need to start making decisions on the best way to protect ourselves. Here are two options to consider:

• Some dental business owners' policies include what is often called cyber coverage, but that coverage might just cover instances of fraudulent statements made online, or online copyright infringement. However, some insurers may offer optional breach coverage you can add to a current policy. Breach coverage is intended to help cover costs associated with a data breach, such as patient notification, and sometimes insurers offer resources on complying with regulations should a breach occur. This may

HELP

Continued on page 26

THE PRACTICE

Continued from page 13

offices are at a higher risk because of the quantity and type of sensitive information that is handled or stored.

Secure Email Solutions

The GDA is now working with iMedicor to assist you in complying with HIPAA regulations through providing you a secure messaging solution. Although iMedicor will assume the liability if there is a breach in transporting data through their system they are not liable if the breach occurs outside of that.

We at GDIS want to provide our members with the knowledge to best protect themselves and their businesses. We are happy to discuss your current polices and ensure that you have adequate coverage so that you may protect what you have worked so hard to build. Contact GDIS at (404) 636-7553, (800) 432-4357, or support@gadental.org.

HELP

Continued from page 17

be an option for dental practices, especially since we now know that we may be likely targets for identity thieves and a breach could be devastating.

• Some practices, especially larger practices, seek outside help with HIPAA compliance. There are companies that will come into your practice, set up a compliance program, train your employees, maintain the program, ensure that your computer system is adequately protected then randomly test its security, and provide all documentation. From what I understand, they also provide some level of liability protection in the event of a HIPAA issue. For some offices, this outsourced approach may be worth the investment. However, you can continue to do HIPAA training and compliance in-house. Since common sense policies and procedures prevent most HIPAA problems in dental offices, the odds are in your favor that, barring a large computer breach, you probably wouldn't have a significant issue.

The bottom line is that HIPAA compliance must be taken seriously. Figure out what works for you and do what you need to do to make sure you're in compliance and your patients' information is protected from improper use and disclosure. As with all regulations, the most important thing is to get your systems in place and regularly maintain them so it's as easy as possible and doesn't drive you crazy. Good luck and Happy HIPAA!

Laney Kay, JD, of Entertaining Training, LLC, has been writing and speaking on regulatory topics since 1989, and she managed her husband's dental practice for 18 years. Her article is offered for information only, and any guidance offered is the opinion of the author and should not be construed as advice, legal or otherwise. Any specific questions, circumstances, or situations you are concerned about in your particular office should be addressed by your own attorney.