New HIPAA Rules Increase Penalties for Patient Information Breaches
As if the previous thousands of pages of Health Insurance Portability and Accountability Act (HIPAA) regulations weren’t enough, the long delayed HIPAA Omnibus rule, all 563 pages of it, was issued at the end of January. The new rule makes significant changes to the existing rules and requires us to change our procedures once more, all in an effort to keep patient information safer.

Unfortunately, as with most government regulations, the end effect to those who are governed by the rule is that we have much more cost and liability. At the end of the day, who knows whether patient information will be any safer than it was before? Regardless, dentists must comply with the new HIPAA rules by September 23, 2013. And it is my opinion that we are all going to have to make some changes in the way we practice dentistry to comply.

**Penalties for Violations Will Increase Dramatically**

Under these new rules, the penalty structure has changed significantly; in fact, a fine can now be as much as $1.5 million per violation. These fines are partially based on how much of an effort you’ve made to get your office into compliance and what actions you’ve taken to ensure that your patients’ information is safe. If you have not made a significant effort to take adequate precautions to protect your patients’ information, this can be construed as “willful neglect.” This means that you knew (or should have known) that you had a problem and failed to take steps to correct it. The more neglect, the bigger the fine, so making a significant effort is incredibly important.

Regular risk assessments and regular, well-documented training demonstrates effort on your part and shows that you are serious about complying with the rules. These actions would hopefully minimize any potential HIPAA fines.

**HIPAA Breaches and Malpractice Coverage**

Most dental malpractice insurance carriers will pay for certain HIPAA violations, but there are exceptions. Check with your carrier to see how much coverage you have and what the terms are in the event of an issue. Additional HIPAA coverage can be acquired; however, be aware that if a violation is considered to be a result of willful neglect, oftentimes, your malpractice carrier will refuse to pay because it is considered to be an intentional act on your part, and therefore, is not covered by insurance.

**Set Up and Maintain a HIPAA Program**

If you are not already doing so, now is the time to set up a HIPAA program in your practice and maintain the program regularly. Get a manual, choose a security officer in your office to oversee the HIPAA program, and then fill out the manual so you have written policies and procedures. The American Dental Association sells “The Practical Guide to HIPAA Training” for $202.50 as one possible option. You can also find information about policies and procedures at www.hhs.gov/ocr/privacy.

Perform regular employee training on HIPAA issues, as needed, and document the training. Most importantly, you need to perform regular risk analyses and assessments to evaluate potential issues in your office regarding patient information, take action to fix any problems you find, and then document your actions. You can’t do this once and then say you’re done. The risk assessments must be done whenever necessary, and at least on a regularly scheduled basis. The schedule needs to be documented in your materials.

**Posting of Policies and Patient Acknowledgements**

The new rules require us to make changes to our existing privacy policies. You do NOT have to distribute the new policies to current patients or have them sign a new acknowledgement of receipt. However, you would have to post the new policies, have copies available for those patients who request them, and distribute these new policies to new patients and have them sign an acknowledgement.

If a practice has a web site or social media presence, such as a Facebook page, and posts privacy notices there, common sense would dictate replacing all current notices with the new information. Including a statement that the practice has changed its privacy practices, and that patients should read the new information could show a good faith effort to ensure patients are aware of the updated practices.

The new policies must state that a patient’s information cannot be sold or used for marketing or fundraising purposes without previous signed authorization by the patient, and that a patient will be informed if there are any financial conflicts of interest with the dentist and any products or services utilized within the practice or as part of treatment. The patient must also acknowledge this conflict of interest statement in writing. The policies must state that a patient will be notified of any breaches of information in a timely manner.

The new rules also state that if a patient personally pays for a procedure and asks that information about that procedure NOT be disclosed to their insurance company, so long as the patient pays in full for the procedure in a timely manner, the practice cannot make the disclosure.

If you use electronic health records, and patients want an electronic copy of their records, they should be able to get an electronic copy, if possible. If patient information is not maintained in an electronic format, then the information must be provided in a mutually agreed upon format. The rule specifically states that a health care provider doesn’t have to buy new software or change a current computer system in order to comply with this
requirement. If a patient requests, in writing, that a copy of his record be sent to a specific third party, the record must be sent, as directed.

**Big Changes Coming in Business Associate Disclosures**

Some of the biggest changes we will see involve business associates. According to a presentation made in June 2012 by an attorney with the Department of Health and Human Services, more than 20% of all large breaches of private health information are caused by business associates.(1) With that sort of track record, business associates came under fierce scrutiny by federal regulators. The result is that under the new regulations business associates are now regulated by the HIPAA rules. They are subject to the same liability and the same fines and penalties, and they must adhere to the same policies and procedures and comply with all of the HIPAA requirements.

Many of your business associates may not be aware of these new rules, so before you renew any contracts with them, let them know that they will be subject to all HIPAA requirements and what that means. This is especially important if you deal with someone who, for example, shreds secure patient information as a side business, or performs work for your practice as a favor. If there is a breach and the HIPAA agencies start investigating all involved parties, the ramifications to both of you may be huge.

I imagine that there are some companies that are going to stop working with health care providers altogether because they don’t consider it worth the hassle of dealing with HIPAA.

In case you do not recall or know, a business associate is a business entity that requires access to your patients’ private health information on a routine basis as part of performing tasks. If the business creates, receives, maintains, or transmits data on your behalf, that entity is a business associate. Here are some examples of business associates in dentistry:

- Anyone who stores your patients’ information or converts, or transmits it, or transcribes it;
- Anyone who works on your computer system and has access to your patients’ information;
- A consultant, lawyer, or accountant with access to patients’ personal health information;
- A clearing house that prepares electronic claims for filing with insurance companies;
- A shredding company that takes patient charts offsite for disposal;
- Your dental software company if they have remote access to your system;

HIPAA
Continued on page 14

---

**ATLANTA DENTAL IMAGING**

[Website link: www.atlantadentalimaging.com]

CBCT Scans for Dentists, Dental Specialists, and ENT’s. We service your imaging needs at an affordable price for you and your patients.

Cost for full Scan: $99.00

- Surgical suite available for your Surgical needs at only $250.00 per hr. (Free Scan if Surgery Suite is reserved for 2hrs. or above)
- Secure file transfer

Please Call for more information (678) 399 1919
• Billing services, collection agencies, and any other entity that accesses your patients' financial information.

Please note that dental labs, insurance companies, other doctors, and pharmacies are not business associates and do not require an agreement.

Does the liability of our business associates relieve us of our liability if they screw up? Of course not. The government is now allowed to fine everyone, but ultimately, we are still responsible for the acts of our business associates and anyone working for them on our behalf, and are responsible for ensuring that patients are properly notified and protected in the event of a breach.

So how can we protect ourselves? The most important thing is to make sure that we have written agreements with our business associates that clearly designate each party's responsibilities. The agreements need to have indemnification agreements that acknowledge that, in the event of a breach caused by the business associate, it will be responsible for all announcements and notifications, and will pay for any actions needed to mitigate damages, such as credit protection services.

If your business associate has subcontractors, you do not have to have personal agreements with the subcontractors; that is your business associate’s responsibility. However, make sure that your contract includes a section that says that the business associate is also responsible for indemnification of any damages caused by subcontractors. Since you are still ultimately liable for the acts of your business associates and any subcontractors they hire, these agreements are very important to protect your interests in the event of a breach.

Big Changes on Way in Breach Definition and Reporting

The new rules will also bring us significant changes in the definition and reporting of breaches. Basically, a breach is a use or disclosure of protected health information which compromises the security or privacy of a patient’s protected health information. What are examples of a breach? The most common example is when a computer gets hacked or gets a virus, but can also include situations in which a computer, smart phone, or backup device such as a thumb drive or external hard drive containing patient information is lost or stolen.

It is also a breach if you mail or email one patient’s bill to another patient or you fax a patient’s information to the wrong fax number.

Under the old rules, if a breach occurred, the business would need to evaluate the situation to see if the breach could result in a risk of significant risk of
harm to the person; if so, notification would have to be performed. **Under the new law, if any situation occurs that could compromise patient information, it is presumed that a breach has occurred and notification is necessary unless a risk assessment shows that it is not likely that the information has been compromised.**

You can't just say 'it's not a breach' if an incident occurs. You must perform a risk assessment to determine if a breach occurred. Since the presumption is that a breach has occurred, unless you can demonstrate a low probability that the information was compromised, an assessment must be performed to see whether you need to go any further. **Every risk assessment must be done thoroughly, completely, and in good faith and the conclusions have to be reasonable.**

A proper risk assessment considers four factors, and all four of these factors must be considered together in order to make a reasonable assessment of the situation.

1) **First**, evaluate what type of information was potentially compromised and how much was actually disclosed. If you have a situation where only patients' names were disclosed, but no other information, that is much less of a problem than if the patients' Social Security numbers and dates of birth were disclosed.

2) **Second**, consider who received the information. For example, consider a situation where you accidently faxed the wrong patient's information to a specialist. They called and told your office that you sent the information to the wrong doctor but that they destroyed it as soon as they realized the mistake. Because they are a doctor you are familiar with and they are also a health care provider who is under HIPAA constraints, it is unlikely the information would be used improperly. In this case, it is likely that a completed risk assessment would show little likelihood that the information was compromised, so no breach notification would be necessary. In that case, you would finish the risk assessment, document your findings, and place a document in your HIPAA manual to show you properly evaluated the situation.

On the other hand, if you accidently fax a patient's medical record to his employer, that's an entirely different situation and it is likely that notification would be necessary.

3) **Next**, determine whether the information was actually acquired or viewed or if there was only the potential for those scenarios. For example, if you had a laptop stolen and the cops caught the guy coming out the back door before he had a chance to do anything with the machine, it is unlikely that a risk assessment would show that to be a reportable breach. If an EOB was mailed to the wrong patient, and it was returned to you unopened, a risk assessment would...
show that the information had not been compromised. If the patient received a document mailed to them in error, opened it, and called you to tell you they got the wrong bill, patient information has been compromised.

4) Finally, consider the extent to which the risk to the information has been mitigated. In some situations, it is possible to determine that there is little risk that the compromised information will be used improperly. For example, if the wrong type of patient information is sent to a business associate or practice employee and they assure you the information was immediately destroyed and will not be used, the likelihood that the information will be disclosed is minimal. Or, if information is sent to an unauthorized person, and they sign a confidentiality agreement assuring that the information will not be used or disclosed, depending on the situation that may be sufficient activity to prevent improper usage of the information.

Once you determine a breach has occurred, the method of notification required by the HITECH rules are still in effect. (The Health Information Technology for Economic and Clinical Health Act was created in 2009 to promote widespread adoption of health information technology and forced the modification of HIPAA privacy, security, and enforcement rules.)

First, whenever a patient’s information is breached, the patient has to be notified. If the breach involves fewer than 500 people in a single geographic area, then the breach has to be logged and reported to the U.S. Department of Health & Human Services (HHS) at “the end of the year in which the breach was discovered,” and patients have to be notified as soon as possible.

If the breach involves more than 500 people in a single geographic area, you must notify HHS and your patients immediately, and absolutely within 60 days of the breach. You must then notify the local media. This could involve calling the local television station, or sending a press release for publication to a newspaper that serves the affected area. The media notification has to contain the same information as the information given to the patients, which is generally:

- A brief description of what happened;
- Description of the type of information involved;
- The steps involved individuals should take to prevent further harm;
- Information on what your office is doing to investigate, mitigate harm, and prevent future breaches; and
- Phone numbers and addresses (including a toll free number) that patients can use to contact the office with any questions.

You also have to try to mitigate the situation as much as possible. When BlueCross BlueShield suffered a breach, they offered credit monitoring to 2.5 million patients for a year. Credit monitoring costs at least $10 a month per patient. Do the math. Add in notification costs, negative publicity costs, the hassle and stress of HIPAA coming in your office to investigate the breach, AND possible fines, and you are looking at an unbelievably expensive problem.

Some Exceptions to the Breach Rule
There are specific exceptions to the breach rule that do not necessitate notification or evaluation. If a person who is supposed to have access to patient information accidentally accesses information that she should not have access to, but no further disclosure happens, that’s not a breach. This isn’t usually relevant in dental facilities, but an example would be if an insurance processor in a large dental practice accidently goes into the clinical record and that is not the information she’s normally supposed to access. Another exception would be a situation in which a disclosure is made to an unauthorized person, but the unauthorized person couldn’t access or retain the information. Examples of this situation would be if you mailed a bill to the wrong patient, but the mail was returned unopened meaning the information wasn’t viewed, or your front desk person hands the wrong EOB to a patient but immediately realizes it and retrieves it before the person has a chance to look at the information.

How Dental Offices Can Avoid a Breach
The HHS HIPAA website www.hhs.gov/ocr/privacy lists of all the entities that have suffered breaches involving 500 or more patients. If you look at all of the small health care providers on the list, almost every single breach was related to a stolen device, either a computer or an unencrypted smart phone with full access to patient information. Occasionally, the list notes that a computer was hacked or a backup was lost, but most of the incidents were related to stolen or compromised technological devices.

The best way to deal with a breach is to avoid a breach. What is the single most important thing we can do to protect our patients’ information and avoid potential breaches? Encrypt your hard drive.

There are only two methods of making patients’ information unusable: shredding it, or encrypting it. If the information on your hard drive is encrypted and the hard drive is stolen, or lost, or someone hacks into it, the information is not usable. If the information isn’t usable, a risk assessment will show that a breach has not occurred and the breach notification process is avoided. As we’ve discussed, that’s a huge deal.

Talk to your computer support person about encryption. There can be problems, especially if you have an older system. Encryption can slow down a computer to the point that it’s almost unusable. In that case, you may have to weigh the costs and benefits of upgrading your system versus risking a breach. My personal opinion is that it’s cheaper to upgrade your system than deal with a breach, so consider your decision carefully.

Some computer experts have argued that using encrypted passwords is sufficient and will comply with all of HIPAA’s requirements of how to protect information from unauthorized access. That is absolutely true. Encrypted passwords are perfectly adequate
protection from someone being able to easily access your equipment and will absolutely satisfy what is required by HIPAA. However, if someone breaks into your office and steals your computers, or takes your snazzy smart phone that has access to your system, or hacks into your system, that is a breach. If they can get past the passwords, the information is fully accessible to them because it’s not encrypted and is therefore usable. That’s a breach, and notification is necessary. If it’s encrypted, a risk assessment will show there’s no breach. That’s an enormous difference.

**What Do We Need To Do Now?**

Bottom line, here are four of the most important things you can do to protect yourself and your patients’ information under this new rule:

1. Set up a HIPAA program and maintain it regularly;
2. Encrypt your hard drive to protect your patients’ information;
3. Understand the concept of business associates and the related liability issues and make sure you have business associate agreements that protect you and your patients’ information;
4. Always disclose the minimum amount of information necessary when dealing with patients’ information.

There is plenty of information out there to help you get your office into compliance. Good luck!

---

**References**


Laney Kay, JD, of Entertaining Training, LLC, has been writing and speaking on technical and regulatory topics and women’s issues since 1989. Her expertise is in taking very complex and / or incredibly boring topics and making them fun and informative. She has written many articles for state and national journals and has taught courses at multiple Hinman Dental Society and American Dental Association meetings as well as at many other national, state, and district meetings, study clubs, and individual offices all over the country.

---

**"I never thought I could be this happy with dentures. The drive was well worth it."**

Whether you have that hard-to-fit patient or simply don’t enjoy dentures, our specialty practice is limited to denture and implant care. Our professional team is passionate about restoring your patient’s confidence and smile.

---

**Georgia Denture & Implant Specialists**

Our on-site lab is home to two of Georgia’s most dedicated and gifted artistic technicians.

---

Georgia Denture and Implant Specialists, LLC
Private Prosthodontic Specialty Practice
**WARREN G. BERNE, DMD**

203 Woodpark Place
Suite B-102
Woodstock, GA 30188

770-926-0021
DrBerne@GaDentures.com

---

**GDA ACTION**
MARCH 2013