Where Dentistry Stands with the Affordable Care Act
Because We Love You: 30 Things You Can Do to Stay in Compliance with HIPAA

Laney Kay, JD

GDA Members! A guide to the new HIPAA guidelines was published in the March 2013 GDA Action. Read that article at www.gadental.org. Click the green For Members button, then click the GDA Action Journal link.

Since the new HIPAA regulations went into effect in 2013, we’ve seen a lot of incorrect and scary information about what dentists are required to do in order to comply. Here are some lists I have a compiled that hit the big areas we need to cover in order to be compliant with both the HIPAA Privacy and Security regulations.

The most important key when it comes to HIPAA compliance is to make sure you establish a program and then regularly maintain it. That means you can’t just fill out the manual and forget about it. You need to regularly evaluate patient information safety, provide regular risk assessments, have regular training sessions, and document all of it. Possible penalties of up to $1.5 million per information breach incident are at least partially based on the office’s effort to effectively maintain the program, so the effort is a worthwhile investment apart from being required.

HIPAA DOES NOT REQUIRE YOU TO DO THIS

Despite what you may have heard in webinars, conferences, or via sales solicitations, HIPAA regulations do not require you to do any of the following:

• Build glass partitions at your front desk to prevent patients from overhearing other patients’ information, or completely reconfigure your office if you have an open bay system.

• Take down pictures of child or adult patients from your office hallways or bulletin boards. As part of the original paperwork patients complete with your office, have patients sign an authorization if they will allow the use of their images or the images of their children to be used in your office or online (your web site, your Facebook page, etc.) At that point, if a parent doesn’t want their kids’ images used, or want their image used, they will let you know.

• Get other doctors and specialists to sign a Business Associate agreement. You also don’t have to have complete a Business Associate agreement with insurance companies, dental labs, or pharmacies. (A Business Associate is an entity that requires access to your patients’ private health information on a routine basis as part of performing tasks apart from the above, such as consultants, lawyers, accountants, shredding companies, dental software companies, and billing services.)

• Be paperless. Unless a significant portion of your practice consists of caring for Medicaid or Medicare patients, you are not required to be paperless. If you do participate at all in Medicaid or Medicare, contact officials with these entities to ensure you are in compliance with their paperless requirements. Otherwise, you may see a yearly reduction in reimbursement.

HIPAA DOES REQUIRE YOU TO DO THIS

These checklists are not comprehensive, but do cover most of the big areas we have to worry about in dentistry. We hope you find these checklists helpful and that they take some of the mystery out of compliance.

10 HIPAA Program Things to Do

1) Assign a HIPAA Privacy and Security officer to oversee the program.

2) Order a compliance manual, open it, and fill it out. The manual is not helpful if it’s wrapped in cellophane and never used! The manual that you select should have forms and policies you can configure for use in your office. (Editor’s note: The American Dental Association sells a “Complete HIPAA Compliance Kit” (J598) at www.ADACatalog.com that includes a manual, training CD-ROM, and a three-year update service.)

3) Develop privacy policies and a Notice of Privacy Practices. Post these in your office and make copies to hand out to patients.

4) Make sure all employees receive HIPAA training at the time of initial employment and at regular intervals as needed in your office. Document all training and place it in your manual.

5) One method to help avoid the largest penalties is to consistently maintain your program. Perform regular risk assessments and audits, have regular training meetings, and document your efforts. The more you can demonstrate that you are constantly trying to maintain the privacy of patient information, the less severe the consequences may be in the event of a problem.

6) Make sure employees understand the idea of disclosing only the “minimum amount necessary” when discussing or disclosing private health information. DO NOT talk about patients’ private health information outside the office! Make sure employees also understand that improper use of patient private health information can lead to dismissal, as well as potential fines and criminal prosecution under HIPAA regulations.

Continued on page 18
7) Perform regular risk assessments to evaluate how patients' private health information is used, stored, and transmitted in the office. Take precautions to ensure that patients' information is protected in the office as much as possible. These precautions can include shredding documents containing private health information, limiting patient physical access to information, locking doors, and using an office alarm.

8) Ensure you have policies and procedures in place in the event of a breach. Depending on the type of breach, notification must be provided to patients, the HIPAA folks, and in some cases, the local media. You need to be able to act fast to reduce any damages and mitigate any harm that may be caused by the breach, so policies and procedures are very important.

9) Make sure a plan is in place to ensure that patients' information can be retrieved in the event of a disaster or emergency.

10) If an employee is terminated, ensure policies and procedures are in place to make sure that the locks are changed and access codes and passwords are changed to prevent future access to patients' private health information.

8 HIPAA Privacy Program
Things to Remember

1) Have patients sign an Acknowledgement of Receipt of Privacy Policies that show they received a copy of the policies and place the signed acknowledgement in the patients' chart. (If the Privacy Policies are changed in the future, you are not required to have current patients sign a new acknowledgement; just post the new policies with the new changes and issue the new policy to all new patients.)

2) Set up authorizations for release of protected health information, as needed.

This can include releases for the use of patient photos, or disclosure of information for financial purposes, or disclosures to certain family members, or disclosures if information is used for marketing purposes.

3) Patients have a right to limit the use of their information. For instance, if a patient asks you to place an appointment postcard in an envelope when sending them mail, or asks your office not to call them at work, those are reasonable requests to limit information.

4) Patients have a right to obtain a copy of their record, even if they owe you money. If they request a copy of their record from you, in writing, you must provide a copy within 30 days. Doctors holding on to patient records is one of the most common reasons that patients file HIPAA complaints. (Editor's note: This requirement to provide a copy of a record to a patient is also codified in Georgia law. A patient must make the request in writing. A dental office must provide a complete copy of the record. The office may charge a reasonable fee for the copy of the record, within certain limitations. The dentist is required to maintain the original patient record and only provide the patient with a copy.)

5) Patients have a right to an accounting of disclosures for any disclosures not for treatment, payment, or regular health care operations. If you disclose information to a public health official, for example, you don't have to get permission from the patient, but you do have to document that the disclosure was made, and the patient has a right to see a log of those disclosures.

6) You must have complaint procedures in place in the event a patient has a complaint.

7) Make sure all Business Associates are identified and a Business Associate agreement is in place. The agreement should specifically require a certain level of protection of patient information and should specify each party's obligations in the event of a breach. Indemnification and notification (patients, the media, and HIPAA) must be addressed.

8) If you use social media, such as Facebook, or have an office web site, never mention private health information in a public forum. If a patient asks a personal question on social media, only answer privately. Also, make sure that patients have given written permission to post photos, videos, x-rays, etc. before you post them.

12 Security Program
Things to Deal with NOW

1) Our most important goals are to prevent a breach a) because we want to and must protect our patients' information and b) we want to and must protect our businesses because the penalties can be so harsh financially. Avoiding a breach is VERY important to us. Consider this:

- 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.

- 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.
2) In my opinion, the most important thing you can do to prevent a significant breach of patient information is to encrypt your hard drive. Most breaches in dental offices and other small health care environments occur when a computer is stolen, or a smartphone with access to patient information is lost or stolen, or a portable device is lost or stolen. If such an event happens and the hard drive of the device is not encrypted, that incident becomes a reportable breach. Although encrypted passwords, protective firewalls and software, and other protections may be sufficient to provide protection under normal circumstances, they are NOT sufficient to prevent a breach if a computer is stolen. Bottom line, if the hard drive is encrypted, it’s not a reportable breach. If it’s not encrypted, it’s a reportable breach.

3) Computers must be protected with software to guard against malware and viruses as well as firewalls, passwords, and whatever other protective methods are necessary in your office to protect private health information. All hard drives should be encrypted (see above) in order to prevent a breach in the event of theft or loss of an electronic device.

4) Physical access to computer workstations should be limited to only those who should have access. If computer workstations are accessible to patients or others who should not have access, additional precautions must be taken to ensure that private health information cannot be accessed. For example, a computer in a consultation room must have limited access to private health information and monitors should be placed so that displayed information is not easily viewed by others.

5) If you offer wi-fi in the office for patient use, make sure it is on a different router than the one used for patient information. Password protect both wi-fi routers.

6) Assign employees and Business Associates with unique passwords that they must use when accessing patient information on practice computers.

7) You must develop policies and procedures for the use of portable devices, including smartphones, tablets, and backup devices, to ensure they are not lost or improperly accessed.

8) Policies and procedures must be developed for any electronic information that is backed up. Can you address how electronic information is accessed and stored? Where the data is kept? How many devices there are? How the data is secured?

9) You must address how computer hardware is used, stored, and destroyed in the office.

10) Schedule regular audits and review access reports to ensure the safety of your patient information and to ensure that data hasn’t been improperly accessed. Any security incidents should be logged whether they resulted in improper access or not.

11) Private health information must be transmitted securely. E-mails should be encrypted or properly protected if you are transmitting private health information.

12) Any changes or updates in your computer system should be documented and the documentation placed in your HIPAA manual. Consider requiring your information technology vendor to document all work done on a dedicated form that you date and place in your manual. This shows that your system is being maintained and protected on a regular basis.

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 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.

---

**Do your patients suffer from any of these symptoms?**

- **Head Pain**
  - Forehead + Temples
  - Migraine-type
  - Sinus-type
- **Eyes**
  - Pain behind eye
  - Blood-shot eyes
  - Sensitive to light
- **Teeth**
  - Clenching/grinding at night
  - Toothaches
  - Soreness of back teeth
- **Ear**
  - Ear pain + ringing in ear
  - Dizziness + Vertigo
- **Jaw**
  - Clicking, popping jaw joints
  - Pain in cheek + Limited opening
- **Neck**
  - Lack of mobility/stiffness
  - Neck pain + Tired/more muscles
  - Arm/finger numbness

Visit us online at www.tmdatlanta.com to download a referral form and learn more about our services!

Manoj Maggan

**Center for TMJ Therapy**

- DDS, DABSM, DABCPR, DAAPM, FICCMO, FAACP
- 8590 Old Milton Parkway, Alpharetta, GA 30005
- Phone: 770.521.9978 • Fax: 770.521.9930
- Web: www.tmdatlanta.com • Office@tmdatlanta.com

---

**TMJ Therapy**

Our dedicated team of professionals have years of training and are happy to assist you in the diagnosis and treatment of possible craniomandibular/ temporomandibular disorders.