The following questions and answers were raised during the May 1, 2013 AAOMS Webinar on, “HIPAA Review and Update for OMS Practices.” This Webinar educated OMS administrators, staff and providers about the general applicability and impact of the Health Insurance Portability and Accountability Act (HIPAA) of 1996; the recently released Omnibus Final Rule; Privacy and Security Rules and Breach Notification; Business Associates rules, regulations and Business Associate Agreement documentation; compliance mandates and best practices for Notice of Privacy Policies and Authorizations.

Q. If a patient is referred to our office and we take a panoramic image, do we need to have a signed HIPAA release to send a referral without the panoramic image back to the doctor?

No, you would not need an authorization, as this scenario falls within the treatment exception under HIPAA.

Q. Can we receive X-rays and notes on patients via e-mail or fax from general dentists?

Yes, you may receive Protected Health Information (PHI) from other providers via e-mail or fax; however, it would be best if e-mails were encrypted to protect against potential breaches.

Q. Are there any guidelines for charging patients for copies of their CT scan data (even if the CT scan is performed free-of-charge)?

While HIPAA allows for the imposition of a “reasonable, cost-based fee,” you should check your state’s laws on the matter, as they may limit what you can charge a patient for such records.
Q. Is our shredding company a Business Associate?

Most likely, if individually identifiable health information is part of the information provided for shredding.

Q. Our attorney will not sign a Business Agreement, stating PHI becomes public record when it goes to legal collection.

If your attorney requires access to PHI to perform his or her function, then they most certainly are a Business Associate. As such, your practice must enter into a written agreement with the attorney.

Q. Can we throw away documents after we shred them?

Yes, so long as the shredding renders the PHI essentially unreadable, indecipherable, and otherwise incapable of being reconstructed. You might also want to consider using trash bags or containers that are not clear or see-through to further protect the shredded data.

Q. Do our appointment reminder service and computer tech support fall under the category of Business Associates? What about NEA Fast Attach and our practice management vendor?

Generally speaking, all of these third parties seem to be performing activities where they are required to access the PHI of your practice, and as such, they would be considered Business Associates and require written agreements.

Q. Has there ever been a HIPAA violation, ePHI breach, etc. litigated against a dentist? If so, what judgment was made?

Yes. The dollar amount of monetary penalties, fines and other administrative sanctions is dependent upon the severity of breach and underlying actions that led to the breach.

Q. Where can we find the omnibus rule?

You can find the Final Rule online at the following link: http://www.hhs.gov/news/press/2013pres/01/20130117b.html
Q. Are we required to provide employees with specific HIPAA training, or must they fill out any type of compliance form upon hiring?

HIPAA doesn’t really provide specific requirements, but instead simply hiring requires that you provide your employees with training that is necessary and appropriate for the members of your workforce to carry out their functions in a manner that safeguards PHI. You must train your staff on the policies and procedures adopted by your practice, as required by HIPAA, to safeguard PHI. We would suggest that you provide your staff with a copy of your HIPAA compliance plan along with a certification form, on which the employee certifies that they received, read and had the opportunity to ask questions and have such questions answered by the practice’s Privacy Officer.

Q. What does the Business Associate Agreement form need to include?

HIPAA requires that Business Associate Agreements must (1) establish the permitted and required uses and disclosures of protected health information by the business associate; (2) provide that the business associate will not use or further disclose the information other than as permitted or required by the contract or as required by law; (3) required the business associate to implement appropriate safeguards to prevent unauthorized use or disclosure of the information, including implementing requirements of the HIPAA Security Rule with regard to electronic protected health information; (4) require the business associate to report to the covered entity any use or disclosure of the information not provided for by its contract, including incidents that constitute breaches of unsecured protected health information; (5) require the business associate to disclose protected health information as specified in its contract to satisfy a covered entity’s obligation with respect to individuals’ requests for copies of their protected health information, as well as make available protected health information for amendments (and incorporate any amendments, if required) and accountings; (6) to the extent the business associate is to carry out a covered entity’s obligation under the Privacy Rule, require the business associate to comply with the requirements applicable to the obligation; (7) require the business associate to make available to HHS its internal practices, books and records relating to the use and disclosure of protected health information received from, or created or received by the business associate on behalf of, the covered entity for purposes of HHS determining the covered entity’s compliance with the HIPAA Privacy Rule; (8) at termination of the contract, if feasible, require the business associate to return or destroy all protected health information received from, or created or received by the business associate on behalf of, the covered entity; (9) require the business associate to ensure that any subcontractors it may engage on its behalf that will have access to protected health information agree to the same restrictions and conditions that apply to the business associate with respect to such information; and (10) authorize termination of the contract by the covered entity if the business associate violates a material term of the contract. Contracts between business associates and subcontractors that are their business associates are subject to these same
Q. Does AAOMS have sample manuals and forms to enable us to update our existing policies?

Yes, AAOMS sells a HIPAA Compliance Plan and Guide, which contains templates of all of the documents required by HIPAA.

Q. Is it allowable to send letters that mention patients’ names to our referring doctors when following up on patients?

Yes, there is nothing in HIPAA that bars this.

Q. Are referring doctors considered Business Associates?

Not typically.

Q. We e-mail X-rays between our referring offices. Do we need any type of authorization from patients to do that?

No, this falls under the treatment exception. We would encourage you to employ encryption technology to guard against a breach if you are going to use e-mail.

Q. Do open-bay operatories in offices and dental schools violate HIPAA or privacy rules?

We do not see why they would. Of course, care should be taken to prevent nothing more than incidental disclosures of PHI from occurring.

The AAOMS frequently posts information related to HIPAA and other topics relevant to OMS practices on the AAOMS website at www.aaoms.org. The AAOMS will also release news or announcements as they become available in the AAOMS Today, AAOMS Advocacy E-Newsletter, and OMS Staff Communiqué.