HIPAA 101 for Cosmetic Orthodontic Dentists

by Jody Erdfarb, Esq.

You've undoubtedly heard about HIPAA. Read why compliance is important to dentists providing Clear Aligner Treatment.

Most dentists have heard HIPAA mentioned in dental school, during residency training, or in continuing education courses. Yet, unfortunately, not all dentists take HIPAA compliance seriously, relegating it to the bottom of their ever-expanding and never-completed to-do lists. This article briefly summarizes HIPAA's applicability to dentists practicing cosmetic orthodontics and explains why HIPAA compliance should be prioritized.

Jody Erdfarb, J.D. is an associate in the Health Care Department at the law firm of Wiggin and Dana LLP and is based in Stamford, Connecticut. Jody's practice involves advising health care providers nationwide on a broad range of issues including compliance, fraud and abuse, HIPAA, patient care, and regulatory and corporate matters. Jody regularly advises clients on developing HIPAA privacy and data security policies and procedures, and assists clients in preventing and responding to data breaches and managing federal and state investigations and settlements. Jody can be reached via email at **jerdfarb@wiggin.com** or by phone at **203.363.7608**.

What is HIPAA?

The federal Health Insurance Portability and Accountability Act of 1996 and its implementing regulations (HIPAA) established national standards for the protection of certain health information. HIPAA addresses the use, disclosure, and security of "protected health information," and also provides patients with certain rights regarding that information.

"Protected health information" includes all individually identifiable health information, in any form or media, whether electronic, paper, or oral. Individually identifiable health information is defined broadly and includes any information that relates to

- the individual's past, present, or future physical or mental health or condition,
- the provision of health care to the individual, or
- the past, present, or future payment for the provision of health care to the individual,

and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security number), but also can include a photo or other identifiable image.

HIPAA governs "covered entities" and certain of the covered entities' service providers. There are three types of covered entities: (1) health plans, (2) health care clearinghouses, and (3) health care providers who conduct certain transactions in electronic form. A dentist who transmits claims for payment electronically to health care insurance companies is a covered entity. Size is irrelevant when it comes to determining HIPAA's applicability; a large multi-dentist practice and a solo practitioner are bound by the same rules so long as they both qualify as covered entities.

What does HIPAA compliance entail?

The HIPAA rules are too complex and extensive to detail in this article. They not only address how protected health information is used and disclosed by a covered entity, but also require that covered entities comply with certain administrative requirements. These requirements include establishing written policies and procedures, entering into written contracts with certain service providers, designating a Privacy and Security Officer, distributing Notices of Privacy Practice to patients, training staff, and retaining documentation of compliance. HIPAA also requires that covered entities perform a security risk analysis of electronic protected health information and adhere to standards designed to safeguard protected health information from improper use and disclosure. Moreover, HIPAA requires covered entities to notify affected patients, the federal government, and even the media of certain privacy breaches.

Merely purchasing a binder or CD of prefabricated policies and procedures, even those designed specifically for dentists, is not going to pass muster with federal regulatory agencies. Compliance with HIPAA requires active participation from the health care provider to ensure that the rules are followed and that a culture of compliance is prevalent at the practice.

How does HIPAA apply to my practice?

HIPAA requires that covered entities use and disclose protected health information only as permitted by the HIPAA regulations. The HIPAA regulations are extremely detailed and their application is very fact-specific. While general use and disclosure rules apply to all practices that are covered entities, the operational context of a particular practice must be carefully analyzed to ensure compliance in the application of the general rules.

For example, dentists providing Clear Aligner Treatment often take before-and-after pictures documenting the patient's outcome, which then are shown to other patients, or used in articles, lectures, or advertisements. HIPAA applies to

protected health information, defined in part as "individually identifiable health information." A full-face photograph is clearly individually identifiable and therefore would require a HIPAA-compliant authorization from the patient before use or disclosure. A photograph showing only the patient's teeth, on the other hand, may or may not be individually identifiable. If the patient has particularly recognizable teeth, then the photograph would qualify as individually identifiable. This same analysis would apply to using and/or disclosing a patient's x-rays, plaster dental models, or aligners.

Common sense should be employed here as well. Even if you determine that a photograph of teeth does not contain individually identifiable information, one could imagine that patients might not be thrilled to see their before-and-after pictures plastered on large billboards alongside I-95 without their consent. It goes without saying that if the pictures had some other data that could reasonably identify the patient, such as a name or address, then HIPAA's protection would apply. Dentists should be careful about displaying x-ray images with patient names on them or aligner sets with the patient's name labeled on the box unless the patient has signed a HIPAA-compliant authorization permitting the disclosure.

Note that while HIPAA generally requires authorization to use or disclose protected health information, there are exceptions to this rule. For example, no patient authorization is necessary for the dentist to submit the patient's protected health information to an insurance company for payment purposes. Also, no patient authorization is required for the dentist to share the patient's protected health information with another dentist in order to get advice on the best course of treatment.

Also, the standards regarding safeguarding protected health information must be specifically tailored to the dentist's practice. For example, a practice that routinely leaves appointment reminders on patients' voice mail should implement a policy limiting the amount of information disclosed in the voice message. The federal government recommends leaving only the covered entity's name and number and other information necessary to confirm the appointment, or asking the individual to call back.

Why should I take HIPAA seriously?

For many years, HIPAA was not assertively enforced and fines were rarely imposed for noncompliance. Federal HIPAA investigations were largely complaint driven and settled informally through resolution agreements in which providers voluntarily agreed to adopt corrective actions. Some covered entities sarcastically referred to those who worried about HIPAA as "HIPAA-chondriacs."

However, the game has changed. Over the last several years, HIPAA enforcement has aggressively been on the rise. The federal agency responsible for HIPAA enforcement, the United States Department of Health and Human Services' Office for Civil Rights (OCR), has been armed with more staff, a larger budget, and greater enforcement authority, including the ability to impose multimillion-dollar fines for HIPAA violations.

OCR has steadily increased both the number of settlements and the monetary amounts paid in these settlements. From 2008 through 2010, there were only 4 settlements; in the 3+ years since, there have been 17 more. From 2008 through 2011, there was only one settlement for over a million dollars; in the 2+ years since, there have been over a dozen more. HIPAA settlements used to be sporadic, but a steady flow of settlements is becoming the new reality. In fact, OCR announced 5 new settlements in the last 5 months alone, totaling over $7.5 million, and the largest monetary settlement to date, for $4.8 million, was recently announced on May 7, 2014.

Lest you think that your practice is too small or nondescript to be noticed by a large federal agency, OCR has been very clear that it intends to pursue smaller providers as well. In December 2013, OCR entered into a settlement for $150,000 with Adult & Pediatric Dermatology, P.C., a 12-physician private practice that delivers dermatology services in Massachusetts and New Hampshire. The practice also agreed, as part of the settlement, to implement a corrective action plan, including submitting periodic reports on its HIPAA compliance to OCR.

The events leading up to this settlement could easily have occurred in a dental practice. On October 7, 2011, the dermatology practice filed a required report with OCR regarding an unencrypted thumb drive, containing the electronic protected health information of

approximately 2,200 individuals, that was stolen from a vehicle of one of its staff members. The drive was never recovered. After conducting a 2-year investigation, OCR concluded that although the report was appropriately made, the practice still violated HIPAA by (1) not initially conducting an accurate and thorough analysis of the potential vulnerabilities and risks to the confidentiality of protected health information as part of its security management process, and (2) not having written policies and procedures and training members of its workforce regarding HIPAA's breach notification requirements.

In this case, OCR's investigation was spurred by the practice's self-report, but investigations are very often triggered by complaints submitted by individuals. Do not underestimate your disgruntled employees or patients. With a simple letter or phone call to OCR, they can cause great financial damage, reputation damage, and inordinate amounts of aggravation.

Even if you manage to escape scrutiny from OCR, state attorneys general are also authorized to enforce HIPAA, and the Federal Trade Commission has recently displayed a burgeoning interest in investigating data security cases involving HIPAA violations as well. Moreover, since 2010 OCR has been required to audit covered entities to ensure HIPAA compliance. OCR audited 115 covered entities in late 2011 and throughout 2012 as a pilot program and is currently planning further audits. As these audits happen more often, they will surely lead to increased investigations and settlements as well.

What should I do now?

If you are subject to HIPAA, it will take significant time and effort to become compliant, and you should take steps as soon as possible to comply. Although you may need to invest considerable amounts of time, effort, and financial resources, HIPAA compliance is legally required, and these expenditures may be relatively small in comparison to the potential penalties that OCR may impose for noncompliance. We live in a new era of aggressive HIPAA enforcement, and you need to be confident about your level of HIPAA compliance, be prepared for the possibility of an OCR audit or complaint investigation, and be able to defend your policies, procedures, and practices. ■

…dentists providing Clear Aligner Treatment often take before-and-after pictures documenting the patient's outcome, which then are shown to other patients, or used in articles, lectures, or advertisements. HIPAA applies to protected health information, defined in part as "individually identifiable health information." A full-face photograph is clearly individually identifiable and therefore would require a HIPAA-compliant authorization from the patient before use or disclosure. A photograph showing only the patient's teeth, on the other hand, may or may not be individually identifiable. If the patient has particularly recognizable teeth, then the photograph would qualify as individually identifiable. This same analysis would apply to using and/or disclosing a patient's x-rays, plaster dental models, or aligners.