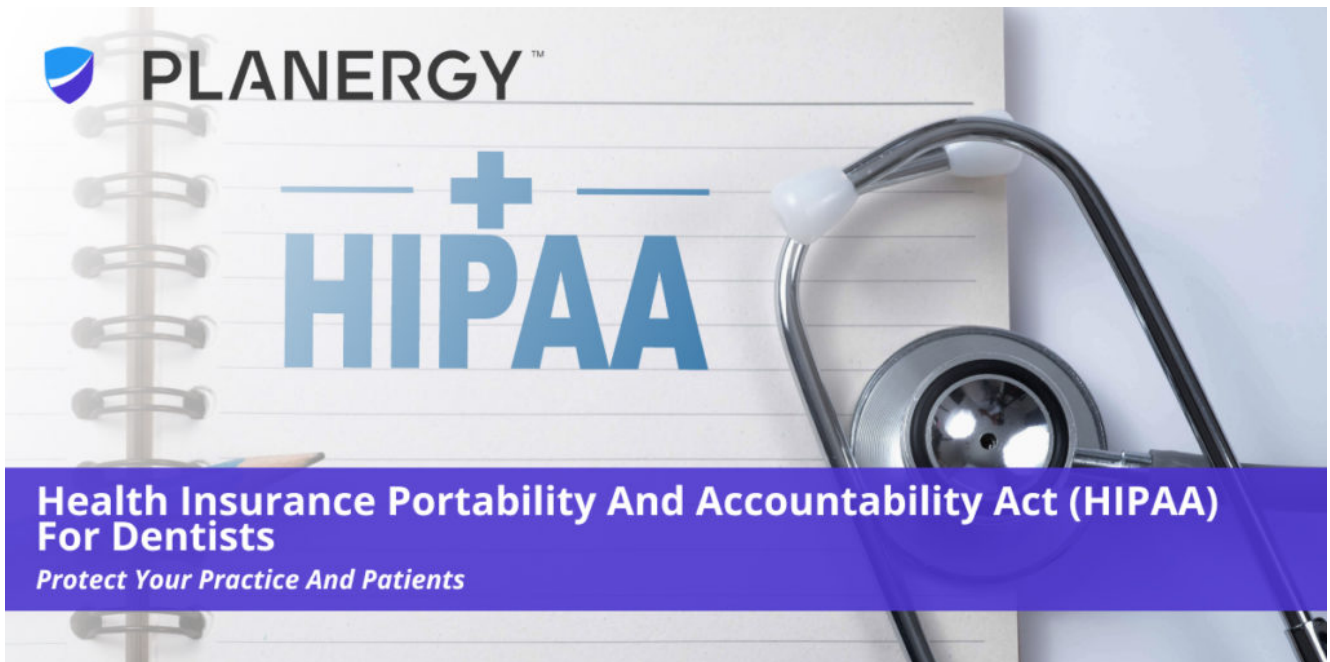


Health Insurance Portability and Accountability Act (HIPAA) For Dentists



Like other healthcare providers, dentists building a successful practice in today's marketplace need to be aware of not just the latest techniques and treatments, but how to navigate the information-driven economy. Protecting patient information is essential to complying with industry and legal requirements, and a proactive approach to meeting the standards set by the Health Insurance Portability and Accountability Act (HIPAA) safeguards a dental practice's (or dental chain's) hard-won reputation with clients.

By understanding what HIPAA is and how best to comply with its requirements, dental professionals can perform effective risk assessments, improve cybersecurity to guard patient information against data breaches, and avoid

costly HIPAA violations.

HIPAA for Dentists: An Overview

Since the dawn of the information age, big data and digital transformation have played an increasingly important role in every area of life. Healthcare is no exception; protecting medical records and other patient information against unauthorized access has always been a high priority for medical professionals, including dentists, but it has new urgency in a world where cyberattacks and data breaches can devastate lives.

Since the passage of the Health Insurance Portability and Accountability Act in 1996, dentists working in private practices, partnership-based dental offices, and dental chains across the United States have operated under additional privacy and security rules designed to safeguard patient data.

HIPAA sets forth baseline protocols to ensure:

- Patients have reliable and timely access to their protected health information (PHI), including medical records, social security numbers, phone numbers, etc. This also applies to the digital version, referred to as electronic protected health information, or ePHI.
- Medical professionals store, secure, and disclose patient information appropriately, with a sliding scale of financial penalties imposed for violations.

Since 2009, when the HITECH Act was passed, the U.S. Department of Health and Human Services (HHS) has relied on a division known as the Office for Civil Rights (OCR) to enforce HIPAA laws.

HIPAA regulations require the OCR to monitor four core rules for medical professionals and their business associates.

1. **The HIPAA Privacy Rule:** All patients have the legal right to control their PHI, and healthcare providers and businesses (along with their employees as individuals) are legally responsible for preventing unauthorized access to patient data in all forms whether written, digitally stored, or spoken.
2. **The HIPAA Security Rule:** All covered entities—including dental offices, chains, practices, and individual professionals, as well as their business associates—must, under penalty of law, secure patient information from unauthorized access when transporting or storing said information.
3. **The HIPAA Breach Notification Rule:** All covered entities and their associates must notify all affected parties when a data breach or other unauthorized access to protected patient data has occurred.
4. **The HIPAA Patient Safety Rule:** This rule defines the data security protocols for how, when, and by whom PHI may be analyzed to produce results used to improve patient safety.

Protecting medical records and other patient information against unauthorized access has always been a high priority for medical professionals, including dentists, but it has new urgency in a world where cyberattacks and data breaches can devastate lives.

Common Dental HIPAA Violations to Avoid

For savvy dentists who want to stay HIPAA compliant, it's *always* a good idea to minimize the risk of a HIPAA violation.

HIPAA compliance takes time and care, but its benefits certainly outweigh the negatives that come with HIPAA violations. The OCR issues fines (known as Civil Money Penalties, or CMPs), and both its investigations and their results are

publicly available under the Freedom of Information Act, providing a permanent record of noncompliance that can haunt dental professionals for years.

From human error to external data breaches perpetrated by hackers, dental practices across the country have certainly felt the pain that comes with HIPAA violations. Fines can range from a minimum of \$100 for inadvertent violations to a maximum of \$50,000 for willful neglect that isn't corrected within 30 days. Repeat violators can rack up fines totaling as much as \$1.5 million each year, *per violation category*.

In addition, when HIPAA violations also violate state law, the Attorneys General for those states can get involved, imposing their own financial penalties. And once state law has been violated, affected parties in some states can pursue legal action of their own, potentially leading to massive financial damages that make the OCR's yearly max look like pocket change.

Some of the most common violations to watch out for include:

- **Improperly disposing of patient records.**

Joseph Beck, a dentist in Kokomo, Indiana was already in hot water when he violated HIPAA compliance rules in 2013. He had his license revoked in 2011 and incurred fees in excess of \$31,000 for committing fraud, failing to maintain adequate patient records, and not keeping up with current professional practices and theory.

He ran afoul of HIPAA in 2013 not through his own fraudulent practices, but because the company he hired to dispose of old patient records failed to do so securely.

- **Loss or theft of devices containing patient information.**

- **Failing to restrict access to patient data.**

- **Disclosing patient data in an unapproved or unsecured fashion.**

Seth Lookhart gained much more than YouTube notoriety when he recorded and then shared video of a dental extraction performed while he

was on a hoverboard—without the patient’s knowledge or consent. The Alaska dentist had a bevy of other charges leveled against him (including fraud, embezzlement, and unlawful dental acts), but his HIPAA violation led to a patient lawsuit, heavy fines and restitution charges, and no doubt contributed to the twelve-year prison sentence he eventually received.

- **Failing to provide a “Right to Revoke” clause in your HIPAA forms.** Patients must have a method for revoking the access to their PHI they’ve granted you and your business associates. Make sure your right to revoke includes any data that might have been accessible via business associate agreements, too.

- **Cyberattacks perpetrated by, and on, third parties.**

Advantage Dental suffered a three-day hack on its systems in 2015, resulting in PHI exposure for more than 150,000 patients. The hacker had used malware to gain access to the system.

In another case, Complete Technology Solutions, an IT services provider, was hit with a devastating ransomware attack in 2019 that exposed sensitive patient data for more than 100 dental practices who were CTS customers.

The company opted not to give in to the hacker’s ransom demands, leaving the affected dental practices to try to recover their lost data on their own. Some had their own independent backups and emerged relatively unscathed, while others had their information held hostage by the hackers, who continued to demand more money to unlock files even after the initial ransom was paid.

Protecting Your Patients and Practice from HIPAA Violations

The American Dental Association (ADA) provides its own guidelines and HIPAA FAQ, but you can help improve your overall HIPAA compliance by taking a few

preventative steps of your own.

Ensure Your Staff is Properly Trained in HIPAA Compliance—and Digital Literacy

From avoiding patient information in water cooler gossip to not using day-glo stickers to mark patient files with sensitive health information to following effective cybersecurity practices, it's imperative everyone in your dental office has the best available HIPAA training.

To protect your patients' information and your business, they need to be aware of potential threats, their own accountability with regard to securing, accessing, disclosing, and discarding patient information, as well as best practices for avoiding bad actors.

A digital literacy policy that includes cybersecurity awareness and proper training for avoiding malware, phishing attempts, and other hacker's tricks will provide another layer of protection between would-be thieves and your patients' PHI.

Perform Regular Risk Assessments

Regular and thorough risk analysis of your internal controls and workflows for potential HIPAA violations will help you identify vulnerabilities *before* they can be exploited by bad actors or create inadvertent violations due to human error, ignorance, or neglect.

These risk assessments should include your suppliers as well as your internal processes.

Invest in Software Tools

Beefing up your cybersecurity directly with IT investments in firewalls and other security software is one obvious way to help secure your patients' information.

But you can take a lot of the stress and risk out of information management by investing in a centralized, cloud-based procure-to-pay solution like Planergy.

How? Like any other business competing in today's economy, you need tools that can help you take control of the vast rivers of information flowing through your office. Bedside manner aside, your patients are your customers—and having a centralized data management solution in place, supported by process optimization, artificial intelligence (including machine learning), advanced analytics, and best-in-class cybersecurity makes it much easier to process and protect their precious information.

With a purpose-built P2P solution in place, you can develop and implement internal controls to automatically limit access to sensitive information while still providing useful business intelligence. You can also automate authorizations and integrate your systems with your preferred suppliers without exposing your patients to needless risk of data breaches, thanks to advanced supplier management capabilities that help you keep your supply chain as secure as it is resilient and flexible.

HIPAA Compliance Protects You as Well as Your Patients

HIPAA violations can cost you so much more than money. The stigma and loss of trust that come from such violations can derail or end even the most promising dentistry career. Take a proactive approach to HIPAA compliance. Invest in the software tools you need to ensure patient information is as secure as possible, optimize your workflows for efficiency, accuracy, and compliance, and make sure your team is well-trained to avoid accidental as well as intentional violations. Your patients will enjoy greater peace of mind, and you'll be free to focus on building a successful and secure dental practice.

What's your goal today?

1. Use PLANERGY to manage purchasing and accounts payable

We've helped save billions of dollars for our clients through better spend management, process automation in purchasing and finance, and reducing financial risks. To discover how we can help grow your business:

- Read our case studies, client success stories, and testimonials.
- Visit our "Solutions" page to see the areas of your business we can help improve to see if we're a good fit for each other.
- Learn about us, and our long history of helping companies just like yours.

Book a Live Demo

2. Download our guide "Preparing Your AP Department For The Future"

Download a free copy of our guide to future proofing your accounts payable department. You'll also be subscribed to our email newsletter and notified about new articles or if have something interesting to share.

download a free copy of our guide

3. Learn best practices for purchasing, finance, and more

Browse hundreds of articles, containing an amazing number of useful tools, techniques, and best practices. Many readers tell us they would have paid consultants for the advice in these articles.

Related Posts