Root Cause

Cyber Security Awareness Month

IN THIS CASE: In a matter brought before the United States District Court for The Southern District of Indiana Indianapolis Division against Westend Dental LLC, the state alleged that the dental practice committed extensive HIPAA violations. The state sought injunctive relief, statutory damages, civil penalties, attorney fees, costs, and other equitable relief.

Fall 2025 **dentistcare.com** **800.492.0119**

Allegations

The investigation stemmed from a consumer complaint by a Westend Dental patient who alleged that their request for a copy of their dental records (specifically X-rays) went unfulfilled. Westend Dental alleged to the patient that they could no longer access the X-rays because their system had been hacked.

Relevant Facts

During the State's investigation by the office of the attorney general (OAG), it was learned that Westend Dental had, in fact, experienced a ransomware attack on or about October 20, 2020, which exposed their patients' personal information and protected health information (PHI) to hackers. Westend Dental became aware of the breach in October 2020 and wholly understood the ransomware attack was why they could not provide the records as requested. However, they didn't submit a "required" data breach notification form to the OAG until October 28, 2022, at which point they denied that the breach ever occurred.

In March 2023, the OAG issued a "civil investigative demand." And in April 2023, Westend Dental responded, under penalty of perjury, again stating that no systems had been compromised.

After numerous opportunities to reveal the truth about this incident under oath, the practice's ownership finally admitted to the ransomware attack in January 2024. They had attempted to cover up the breach, denying it had happened until an employee admitted it under sworn testimony. Although Westend Dental was legally obligated to report the breach to the OAG, it knowingly did not, and it was only discovered after an investigation of the consumer complaint on the heels of a patient's unfulfilled request for records.

The state's investigation of the ransomware attack prompted a broader investigation of Westend Dental's general compliance with HIPAA. The investigation revealed that Westend Dental routinely and repeatedly disclosed PHI in public replies to online patient reviews and made public posts on Facebook, revealing PHI without the proper patient authorization and violating HIPAA Privacy Regulations.

DentistCare
A ProAssurance Program

The Outcome

Westend Dental accepted a "consent order" with the Indiana OAG and will pay a penalty of $350,000. It also committed to implementing significant measures to ensure complete compliance with HIPAA Privacy Regulations. Westend Dental must notify all patients individually about the breach. While the consent order addresses the violations of HIPAA and various state laws with the Indiana OAG, it does not prevent further action or potential substantial financial penalties imposed by HHS.

Risk Management Pointers

This case reminds us of the following:

- **Train staff regularly on HIPAA compliance.** Include guidance on handling PHI in digital communications and social media. Establish clear policies for patient record requests to ensure timely and secure fulfillment of all patient data access requests. Failing to provide requested medical records violates HIPAA and can trigger investigations.

- **Keep all public communications HIPAA-compliant and be careful not to violate privacy regulations.** Responding to online reviews or posting on social media should never include PHI. Even if a patient shares personal information online, such as in a negative review, a dentist is generally prohibited from disclosing that information without the patient's written consent when responding. Do not share patient information on social media sites without authorization. Violations may incur severe penalties.

- **If a malicious actor compromises your confidential patient information, seek immediate assistance from the appropriate specialists, such as consultants and attorneys.** Attempting to conceal a data breach can lead to severe legal consequences, so ensure you provide accurate and truthful descriptions of the incident and facts in all your responses. HIPAA and state laws require prompt notification of data breaches to authorities and affected individuals. Document and report breaches immediately by submitting required forms to regulatory bodies without delay.

- **Protect your practice and your patient data from ransomware and other cyber threats.** Maintain secure backups and access controls. Audit and monitor systems proactively. Regularly assess vulnerabilities and compliance with privacy regulations. Implement a robust incident response plan and ensure all staff know how to respond to data breaches, including reporting protocols.

DentistCare
A ProAssurance Program