Cybersecurity for Dental Practices in 2026: What Owners Need to Know

William S. Barrett, CEO, Mandelbaum Barrett PC, and Co-Author Steven W. Teppler, Partner & Chair

Bill Barrett is the CEO of the full-service law firm Mandelbaum Barrett PC, co-chair of the firm's National Dental Law Group, and dental dealmaker who has successfully closed hundreds of transactions nationwide. He has co-authored two best-selling books on dental industry transactions, showcasing his expertise. Bill is also a nationally recognized speaker at industry events across the country. Mandelbaum Barrett PC is a Corporate Friend of NYCDS.

Steven W. Teppler, CDPSE, is a Partner and Chair of the firm's Cybersecurity & Data Privacy Practice Group and serves as Chief Cybersecurity Legal Officer. He advises businesses on cybersecurity risk management, data privacy compliance, and incident response, and regularly lectures and writes on cybersecurity and data privacy issues.

Running a dental practice today requires more than providing excellent patient care. Dental practices increasingly rely on digital systems to manage scheduling, billing, imaging, and patient records, all of which contain sensitive information. As a result, cybersecurity has become an important operational and legal consideration for dental practice owners.

Recent cybersecurity incidents involving dental organizations serve as a reminder that no practice is too small to be impacted. Unauthorized access to patient information can expose protected health information (PHI) and personally identifiable information (PII), creating significant challenges for both the practice and its patients.

For example, in January 2026, a dental organization publicly disclosed that an unauthorized individual gained access to its network, potentially impacting more than 11,000 individuals and exposing both PHI and PII. Incidents like this often trigger regulatory reporting obligations, forensic investigations, patient notification requirements, and significant operational disruption. Even well-run practices can face serious consequences when cybersecurity safeguards are insufficient or outdated.

Large-scale healthcare breaches also demonstrate how third-party disruptions can cripple providers even when their own networks are not directly compromised. In 2024, a ransomware attack on a major healthcare technology and payment processing company disrupted claims and reimbursement systems nationwide, ultimately impacting nearly 200 million individuals. Many healthcare providers experienced delayed payments and operational strain, underscoring how dependent practices are on clearinghouses, billing platforms, and other vendors — and how vendor failures can quickly become your crisis.

Why Dental Practices Are Vulnerable

Dental practices are attractive targets for cybercriminals because they maintain valuable patient data and often rely on third-party vendors for practice management software, billing, and cloud storage. Many practices operate with lean administrative teams and may not have dedicated IT or cybersecurity personnel, which can increase risk if safeguards are not regularly reviewed and updated.

Common causes of cybersecurity incidents include phishing emails, compromised passwords, ransomware attacks, and vulnerabilities in third-party software. Once access is gained, unauthorized individuals may be able to view or extract patient records without the practice's knowledge.

Legal and Business Risks of a Cyber Incident

A cybersecurity incident can create serious legal and business consequences. Dental practices may be required to comply with HIPAA and applicable state data breach notification laws, which can include notifying affected patients, reporting the incident to regulators, and implementing corrective actions.

In addition to compliance obligations, a cyber incident may result in:

- Disruption to day-to-day operations
- Costs related to forensic investigations and remediation
- Increased scrutiny from insurers and regulators
- Reputational harm that may impact patient trust

Enforcement actions also reflect heightened expectations. In 2025, an Indiana dental practice agreed to pay a $350,000 penalty following a ransomware incident and alleged HIPAA compliance failures, including delayed breach notification and inadequate safeguards. Cases like this demonstrate that preparation and response are just as important as prevention.

Steps Dental Practice Owners Should Consider

While it is impossible to eliminate cybersecurity risk entirely, dental practice owners can take practical steps to reduce exposure, including:

- **Conduct a Risk Assessment** – Practices should understand where patient data is stored, how it is accessed, and who has access. A risk assessment can help identify vulnerabilities in systems, software, and workflows.
- **Limit Access and Strengthen Security Controls** – Access to systems containing patient information should be limited based on job responsibilities. Multi-factor authentication and strong password policies can significantly reduce the risk of unauthorized access.
- **Evaluate Third-Party Vendors** – Many cybersecurity incidents originate with third-party vendors. Contracts should clearly address data security obligations, breach notification requirements, and responsibility for remediation. Practices should confirm that vendors maintain appropriate safeguards.
- **Train Staff** – Staff training is a critical component of cybersecurity. Employees should be trained to recognize phishing emails, suspicious links, and other common threats. Regular training helps reduce the risk of human error.
- **Prepare an Incident Response Plan** – Having a written incident response plan allows a practice to act quickly and efficiently if a cybersecurity incident occurs. The plan should identify internal contacts, outside advisors, and required notification steps.

Planning Ahead

Cybersecurity should be treated as an ongoing responsibility, not a one-time project. As technology and threats continue to evolve, dental practices should periodically review their systems, policies, and vendor relationships.

Working closely with a law firm that has dedicated cybersecurity attorneys is an essential part of managing this risk. Experienced counsel can assist with developing response plans, reviewing vendor agreements, advising on regulatory compliance, and helping mitigate exposure before and after an incident occurs. Taking these proactive steps helps protect your patient data, your brand, and your professional reputation.

Mandelbaum Barrett, PC, is pleased to offer NYCDS members a 30-minute complimentary consultation and 10% off their regular legal services hourly rates, as well as access to their continuing education content and recent industry publications. You can view the full suite of services offered by the firm at www.mblawfirm.com.