



Brooklyn Dental Collective HIPAA Privacy and Security Policy

This document establishes the HIPAA Privacy and Security Compliance Framework for Brooklyn Dental Collective. It defines how protected health information (PHI) is gathered, utilized, stored, and shared, ensuring full alignment with federal regulations.¹ Notice of Privacy Practices (NPP).

We provide every patient with a written Notice of Privacy Practices at their first point of service.

- **Patient Rights:** Patients maintain the right to inspect, copy, and request amendments to their dental and financial records.
- **Accounting of Disclosures:** Patients can request a log of specific disclosures made without their direct authorization.
- **Prominent Display:** The NPP must be posted clearly in the reception area and maintained on the practice website.

2. Minimum Necessary Standard **Practice staff may only access, discuss, or disclose the minimum amount of PHI necessary** to complete a specific task.

- **Clinical Operations:** Dental assistants and hygienists access treatment charts strictly for the patients they are treating.
- **Billing Operations:** Administrative staff access financial and insurance fields only to process claims and payments.
- **Peer Reviews:** Case discussions among providers must omit direct patient identifiers unless required for continuity of care.

3. Administrative Safeguards **The practice designates a Security and Privacy Officer** to oversee compliance training and policy enforcement.

- **Workforce Training:** All employees must complete HIPAA training upon hire and undergo annual refresher courses.
- **Risk Assessments:** The practice performs an annual Risk Analysis to identify potential vulnerabilities in electronic systems.
- **Sanction Policy:** Employees who violate privacy rules face disciplinary actions up to and including immediate termination.

4. Physical Safeguards **Physical access to the facility and hardware containing PHI is restricted** to authorized personnel only.

- **Workstation Security:** Operatory computers and reception screens must be positioned out of view from patients and visitors.
- **Device Control:** Server closets, physical paper files, and backup drives must remain locked when not in use.
- **Media Disposal:** All paper records and printed schedules containing PHI must be destroyed using a cross-cut shredder.

5. Technical Safeguards **Electronic Protected Health Information (ePHI) must be secured** using access controls and encryption standards.

- **Unique User Credentials:** Every staff member must log into the dental practice management software using their own unique username and strong password.
- **Automatic Logoff:** Workstations must automatically lock or log out after 5 minutes of inactivity.
- **Transmission Security:** All emails containing patient data, digital X-rays, or referral notes must be sent via end-to-end encrypted email channels.

6. Breach Notification Rule **The practice must document and report any unauthorized acquisition, access, use, or disclosure** of unencrypted PHI.

- **Risk Assessment:** The Privacy Officer will assess the probability that PHI has been compromised following any security incident.
- **Individual Notification:** Affected individuals must be notified via first-class mail within 60 days of breach discovery.
- **HHS Notification:** Breaches affecting fewer than 500 individuals must be logged and reported to the Department of Health and Human Services (HHS) annually. Breaches affecting 500 or more individuals require immediate HHS and media notification.

7. Business Associate Agreements (BAAs) **The practice will not share PHI with third-party vendors** without an executed Business Associate Agreement.

- **Applicability:** This applies to IT providers, cloud-based dental software, billing agencies, and digital chart storage solutions.
- **Compliance Assurance:** The BAA legally binds the vendor to protect patient data under the same HIPAA standards that apply to Brooklyn Dental Collective.