HIPAA compliance checklist for dental offices

complyday.com

Office: Privacy and security official: Reviewed by:

Date:

Privacy Rule (45 CFR 164 Subpart E)

☐	Privacy official named in writing	164.530(a)(1)(i)
☐	Contact person or office for complaints named in writing	164.530(a)(1)(ii)
☐	Written privacy policies and procedures, kept current with changes in law	164.530(i)
☐	All staff trained on the policies; new staff within a reasonable time; training documented	164.530(b)
☐	Administrative, technical and physical safeguards for patient information, including paper	164.530(c)
☐	Complaint process in place; complaints and outcomes documented	164.530(d)
☐	Sanctions for staff who break the policies, applied and documented	164.530(e)
☐	Harmful effects of a wrongful use or disclosure mitigated where practicable	164.530(f)
☐	No retaliation for complaints; patients not asked to waive their rights	164.530(g), (h)
☐	Notice of Privacy Practices given no later than the first visit	164.520(c)(2)(i)
☐	Good faith effort to get a written acknowledgment; reason recorded if not obtained	164.520(c)(2)(ii)
☐	Notice posted in a clear and prominent place in the office, with copies to take	164.520(c)(2)(iii)
☐	Notice posted prominently on the office website, if there is one	164.520(c)(3)(i)
☐	Uses and disclosures limited to the minimum necessary (not required for treatment)	164.502(b), 164.514(d)
☐	Written authorization obtained when required, including for marketing	164.508
☐	Patient record requests acted on within 30 days (one 30-day extension, in writing)	164.524(b)(2)
☐	Copy fees reasonable and cost-based only	164.524(c)(4)
☐	Amendment requests acted on within 60 days	164.526(b)(2)
☐	Accounting of disclosures provided within 60 days of a request	164.528(c)
☐	Reasonable requests for confidential communications accommodated	164.522(b)
☐	Restriction honored when a patient pays in full and asks that the health plan not be told	164.522(a)(1)(vi)
☐	Written business associate agreement with every vendor that handles patient information	164.502(e), 164.504(e)

Security Rule (45 CFR 164 Subpart C)

R = Required. A = Addressable: put it in place if reasonable and appropriate, or document why not and use an equivalent measure if reasonable (164.306(d)(3)).

☐	Security official named in writing	164.308(a)(2)
☐	Risk analysis: accurate and thorough, written	164.308(a)(1)(ii)(A), R
☐	Risk management: measures in place to reduce risks to a reasonable level	164.308(a)(1)(ii)(B), R
☐	Sanction policy for security violations	164.308(a)(1)(ii)(C), R
☐	Regular review of audit logs, access reports and incident reports	164.308(a)(1)(ii)(D), R
☐	Staff access authorized, supervised and removed when employment ends	164.308(a)(3), A
☐	Access granted by job and reviewed when it changes	164.308(a)(4), A

☐	Security awareness and training for all staff, including management	164.308(a)(5)
☐	Security reminders, malware protection, log-in monitoring, password rules	164.308(a)(5)(ii), A
☐	Security incidents identified, responded to, mitigated and documented	164.308(a)(6), R
☐	Data backup plan with retrievable exact copies	164.308(a)(7)(ii)(A), R
☐	Disaster recovery plan and emergency mode operation plan	164.308(a)(7)(ii)(B), (C), R
☐	Contingency plan testing and criticality of systems assessed	164.308(a)(7)(ii)(D), (E), A
☐	Periodic technical and nontechnical evaluation	164.308(a)(8)
☐	Business associate agreements include the Security Rule terms	164.308(b)(3), 164.314(a), R
☐	Facility access controls and a facility security plan	164.310(a), A
☐	Workstation use rules and physical security for workstations	164.310(b), (c)
☐	Old drives and devices wiped or destroyed before disposal or reuse	164.310(d)(2)(i), (ii), R
☐	Record of hardware and media moved in and out	164.310(d)(2)(iii), A
☐	Unique login for every user	164.312(a)(2)(i), R
☐	Emergency access procedure	164.312(a)(2)(ii), R
☐	Automatic logoff	164.312(a)(2)(iii), A
☐	Encryption of stored patient information, or documented alternative	164.312(a)(2)(iv), A
☐	Audit controls that record activity in systems with patient information	164.312(b)
☐	Protection against improper alteration or destruction	164.312(c)
☐	Person or entity authentication	164.312(d)
☐	Transmission security; encryption when sending, or documented alternative	164.312(e), A
☐	Security policies written; reviewed periodically and updated after changes	164.316(a), (b)(2)(iii), R

Breach Notification Rule (45 CFR 164 Subpart D)

☐	Written steps for a suspected breach, and who decides on notification	164.530(i), 164.414
☐	Risk assessment of the 4 factors documented when deciding a breach is low probability	164.402
☐	Patients notified without unreasonable delay, no later than 60 calendar days after discovery	164.404(b)
☐	Notice has the 5 required elements, in plain language, by first-class mail or agreed email	164.404(c), (d)
☐	Media notified if more than 500 residents of a state or jurisdiction are affected	164.406
☐	HHS notified at the same time as patients for 500 or more people	164.408(b)
☐	Log of breaches under 500 people; HHS notified within 60 days after the end of the year	164.408(c)
☐	Business associates required to report breaches to the office	164.410, 164.504(e)(2)(ii)(C)

Records

☐	Policies, risk analyses, training records, acknowledgments, agreements and breach records kept 6 years from creation or last in effect	164.316(b)(2)(i), 164.530(j)(2)

Federal HIPAA rules as they read on ecfr.gov. A state law that is more protective of health information privacy still applies (45 CFR 160.203(b)). Proposed changes to the Security Rule (January 2025) are not requirements and are not on this list. Do not write patient information on this checklist.