TransDontics
A DENTAL BILLING COMPANY

Checklist: What Dental Practices Should Verify Before and While Outsourcing Billing to an RCM Vendor (Fillable)

Informed by the September 2026 DireWolf ransomware listing of eAssist Dental Solutions

	Category	Checklist Item	What to Look For / Ask	Priority
☐	Vendor Vetting (Pre-Contract)	**Security Certifications**	Request a current SOC 2 Type II report or equivalent independent audit, not a self-attestation	High
☐	Vendor Vetting (Pre-Contract)	**Breach and incident history**	Ask directly whether the vendor has had any prior security incidents, how they were handled, and how clients were notified	High
☐	Vendor Vetting (Pre-Contract)	**Data storage and access architecture**	Confirm where patient data is hosted, whether it's encrypted at rest and in transit, and who internally has access	High
☐	Vendor Vetting (Pre-Contract)	**Subcontractor disclosure**	Identify any third parties (clearinghouses, cloud hosts, collections agencies) that will also touch your data	Medium
☐	Vendor Vetting (Pre-Contract)	**Staff access controls**	Ask whether the vendor enforces role-based access and individual (not shared) logins internally	High
☐	Contract and BAA Review	**Signed Business Associate Agreement**	Confirm a current, signed BAA exists before any data is shared, not after onboarding begins	High
☐	Contract and BAA Review	**Breach notification timeline**	Specify the maximum number of days the vendor has to notify your practice after discovering an incident	High
☐	Contract and BAA Review	**Notification Responsibility clause**	Clarify in writing whether the vendor or your practice is responsible for notifying affected patients	High
☐	Contract and BAA Review	**Liability and cost-sharing terms**	Review who bears the cost of breach response, credit monitoring, and potential regulatory fines	Medium
☐	Contract and BAA Review	**Audit rights**	Confirm the contract gives your practice the right to request security documentation or audits periodically	Medium
☐	Access Management (Ongoing)	**Individual staff logins**	Require named accounts for every user, never shared credentials, on both sides of the relationship	High

	Category	Checklist Item	What to Look For / Ask	Priority
☐	Access Management (Ongoing)	**Multi-factor authentication**	Confirm MFA is mandatory for all accounts accessing the vendor platform, including your own staff	High
☐	Access Management (Ongoing)	**Access review cadence**	Set a recurring (quarterly or biannual) review to revoke access for former employees or unused accounts	Medium
☐	Access Management (Ongoing)	**Integration credentials**	Track any API keys or software integrations linking your practice management system to the vendor's platform	Medium
☐	Financial Continuity Planning	**Claims filing deadline tracking**	Maintain your own internal report of claims approaching timely filing limits, independent of the vendor's system	High
☐	Financial Continuity Planning	**Backup submission path**	Confirm you can submit claims directly through a clearinghouse if the vendor's platform goes down	High
☐	Financial Continuity Planning	**Payment posting reconciliation**	Establish a manual process to log and post payments if vendor systems are temporarily inaccessible	Medium
☐	Financial Continuity Planning	**Data export access**	Confirm you can export your own billing and patient account data from the vendor's system at any time, not only during a crisis	Medium
☐	Incident Response Readiness	**Internal response plan**	Maintain a written plan specific to a vendor-side breach, reviewed at least annually	High
☐	Incident Response Readiness	**Cyber liability insurance**	Confirm active coverage and know your carrier's required notification window	High
☐	Incident Response Readiness	**Legal counsel on standby**	Identify breach counsel in advance rather than searching for one during an active incident	Medium
☐	Incident Response Readiness	**Patient communication template**	Prepare a pre-approved notification template so messaging isn't drafted under deadline pressure	Medium
☐	Ongoing Vendor Monitoring	**Public breach disclosure tracking**	Periodically check sources like Ransomware.live or CISA advisories for your vendor's name	Medium
☐	Ongoing Vendor Monitoring	**Annual security re-verification**	Re-request updated audit reports and re-confirm BAA terms are still accurate to current services	Medium

	Category	Checklist Item	What to Look For / Ask	Priority
☐	Ongoing Vendor Monitoring	**Vendor communication track record**	Evaluate how transparently the vendor has communicated during any past disruptions, planned or unplanned	Low

A Note on the Referenced Incident

As of the most recent public reporting, eAssist Dental Solutions was listed on the DireWolf ransomware group's leak site on September 6, 2026. No independently verified details about the root cause, the systems affected, or the specific data types compromised have been confirmed by eAssist, its parent company Henry Schein, or an independent forensic source. Treat any specific figures beyond this as unconfirmed if encountered elsewhere.

**This checklist is provided for informational and operational planning purposes and does not constitute legal advice. Practices should confirm applicable HIPAA, state breach notification, and contractual obligations with qualified legal counsel.*