

Dental Billing Security Action Plan: 7 Steps to Protect Claims, Payments, and Data for Security and Compliance

A short, practical guide and printable checklist for practice owners and front-end staff to choose a dental billing vendor with reliable security protocols, in light of alleged eAssist ransomware attack claimed in September 2026.

7-Step Plan

Select any row to jump straight to that section.

Step	Action	Your Deliverable	Page
01	Map where your billing data goes	A one-page data flow map and an access inventory.	01
02	Complete and document a risk analysis	A dated risk analysis and a tracked remediation plan.	02
03	Tighten access and authentication	A role-based access list with MFA status for every system.	02
04	Protect data in storage and in transit	A written data handling standard and a tested backup.	02
05	Vet and contract with billing vendors	A completed vendor scorecard and a signed BAA on file.	03
06	Prepare your incident and downtime response	A one-page incident response plan the whole team has read.	03
07	Train, test, and review on a schedule	A security calendar with owners, dates, and evidence of completion.	03
72h	Quick reference: the first 72 hours	If a vendor reports an incident	04
✓	Your dental billing security checklist	Printable, fillable checklist	05

Step 1 Map where your billing data goes

You can't protect a data flow you haven't drawn. OCR's own advice starts here: identify where ePHI is located, and how it enters, moves through, and leaves your systems.

- **List every system:** practice management software, clearinghouse, payer portals, payment processor, email, cloud storage, remote-access tools.
- **List every outside party with access:** billing vendor, IT provider, credentialing, collections, subcontractors.
- Note who holds a login to each one, including former staff.

✓ **Your deliverable:** a one-page data flow map and an access inventory.

Step 2 Complete and document a risk analysis

HIPAA requires an accurate and thorough assessment of risks to ePHI. In OCR's April 2026 ransomware settlements, the missing risk analysis was the common thread. So,

- Cover billing systems, vendor connections, and payment workflows, not just practice systems.
- Rate each risk by likelihood and impact, then write a risk management plan with owners and due dates.
- Update it at least yearly, and whenever you change systems or vendors.

✓ **Your deliverable:** a dated risk analysis and a tracked remediation plan.

Step 3 Tighten access and authentication

Stolen or reused credentials are how many attackers get in. HHS lists multi-factor authentication, unique credentials, and credential revocation among its essential goals.

- Turn on MFA for email, practice management software, clearinghouse, payer portals, banking, and remote access.
- Give every user a unique login. Retire shared accounts.
- Separate everyday accounts from admin accounts, and remove access the same day someone leaves.
- Review all accounts each quarter and delete inactive ones.

✓ **Your deliverable:** a role-based access list with MFA status for every system.

Step 4 Protect data in storage and in transit

Billing files move constantly. Encryption, tight folder permissions, and logging limit the damage if one path is compromised.

- Encrypt ePHI in transit and at rest wherever your systems allow it.
- Send attachments and patient statements only through approved secure channels.
- Keep downloaded ERAs and EOBs in restricted folders, and turn on audit logs.
- **Adopt a callback rule:** any request to change bank or deposit details is verified by phone, using a number already on file.
- Keep backups separate from your main network, and test a restore.

✓ **Your deliverable:** a written data handling standard and a tested backup.

Step 5 Vet and contract with billing vendors

Outsourcing shifts the work, not the accountability. HHS requires a written business associate contract, and business associates are directly liable for certain HIPAA requirements.

- Confirm a signed BAA, plus a list of subcontractors and any offshore access.
- Ask for independent proof, such as a recent risk analysis and a SOC 2 report.
- Write an incident notification window into the contract.
 - HIPAA's limit is 60 days, so ask for far less, for example 24 to 72 hours.
- Ask how claims keep flowing during an outage, and what happens to your data if you leave.
- Give vendors scoped accounts, never full admin logins.

✓ **Your deliverable:** a completed vendor scorecard ([page 5](#)) and a signed BAA on file.

Step 6 Prepare your incident and downtime response

When a vendor reports an incident, the first hours decide how tidy the recovery is. HHS also presumes a ransomware event involving ePHI is a breach unless you can show a low probability of compromise.

- Name an incident lead and a backup, and keep a contact list for your IT, legal, and insurance advisors.
- Pre-write your [first-72-hour steps](#).
- **Know the clocks:** business associates must notify covered entities within 60 days of discovery, and individual notices follow the same outer limit.
- Keep a running list of time-sensitive claims and appeals so timely filing limits aren't missed.

✓ **Your deliverable:** a one-page incident response plan the whole team has read.

Step 7 Train, test, and review on a schedule

Controls decay. People change roles, vendors change tools, and attackers change tactics. A calendar keeps the plan alive.

- **Train staff on billing-specific scams:** fake payer emails, password reset requests, and "update our bank info" messages.
- **Run a 30-minute tabletop exercise twice a year:** "Our clearinghouse login was stolen. What do we do?"
- Review access, vendors, and backups every quarter, and refresh the risk analysis every year.
- Watch the proposed HIPAA Security Rule update. It isn't final, but it points toward more mandatory controls, and OCR enforces the current rule today.

✓ **Your deliverable:** a security calendar with owners, dates, and evidence of completion.

Quick reference: the first 72 hours

If a vendor reports an incident, do all that in the first 72 hours:

#	Action	Done
1	Change passwords for your PMS, clearinghouse, claims software, and payer portals. Use new, unique ones.	☐
2	Remove old or inactive accounts, including remote access.	☐
3	Revoke active sessions, saved credentials, API keys, and integrations.	☐
4	Turn on MFA everywhere available, then review recent login activity and save suspicious logs.	☐
5	Record when you were notified, what the vendor could reach, and what you changed.	☐
6	Warn staff about phishing tied to claims, resets, and payment changes.	☐
7	Flag time-sensitive claims and appeals, then consult with your legal advisor.	☐

Your dental billing security checklist

Print this page. Assign an owner and a date next to each item, and re-check quarterly.

	Step	Checklist Item	Owner	Date
☐	Step 1: Map	Data flow map drawn from eligibility check to A/R follow-up		
☐		Every system and vendor that touches billing data is listed		
☐		Every login is tied to a named, current person		
☐	Step 2: Assess	Risk analysis completed, dated, and covers vendors		
☐		Risk management plan has owners and due dates		
☐		Analysis scheduled for yearly update		
☐	Step 3: Access	MFA is on for email, PMS, clearinghouse, payer portals, banking, remote access		
☐		No shared logins remain		
☐		Admin and everyday accounts are separate		
☐		Departing staff lose access the same day		
☐		Inactive accounts removed this quarter		
☐	Step 4: Protect	ePHI is encrypted in transit and at rest where possible		
☐		Attachments and statements use approved secure channels		
☐		Audit logs are on and reviewed on a schedule		
☐		Bank-detail changes require a phone callback		
☐		Backups are separate from the main network and a restore has been tested		
☐	Step 5: Vendors	Signed BAA on file for every billing vendor		
☐		Subcontractors and offshore access disclosed		
☐		Independent assessment reviewed (SOC 2 or equal)		
☐		Incident notification window written into the contract		
☐		Outage plan and exit and data-return terms confirmed		
☐	Step 6: Respond	Incident lead and backup named		
☐		Advisor contact list is current		
☐		First-72-hour plan is written and shared		
☐		Time-sensitive claims tracker is ready to use		
☐	Step 7: Sustain	Staff trained on billing scams this year		
☐		Tabletop exercise scheduled twice yearly		
☐		Quarterly access and vendor review on the calendar		