CYBERSECURITY BOARD REPORT

Peachtree Pediatrics (fictional) · Q4 2026

Data as of November 11, 2026 · Prepared by SureLock Technology

Where we stand

Peachtree Pediatrics' security score is 73% against a target of 80%, up from 71% at the September baseline. Three high-risk gaps were closed in October, including vendor remote access. The biggest open exposures are an out-of-date HIPAA risk analysis, untested backups and unreviewed security logs; multi-factor authentication for the EHR is due by Dec 15.

SECURITY SCORE	CRITICAL GAPS OPEN	REMEDIATION	VENDORS NOT APPROVED	OVERDUE ACTIONS
73%	**13**	**6%**	**1 of 2**	**1**
Target 80% · ▲ 2 pts better	▼ 1 better	3 of 49 items closed	0 rated high or elevated risk	past their due date

Overall: NOT READY - significant gaps (13 critical) against the target frameworks

Decisions requested from the board

What we need from the board this cycle. Each decision has a recommendation and a date.

#	Decision	Why now	Options	Recommendation	By when
1	Approve the HIPAA risk analysis and its remediation plan as a 2027 priority	Required by HIPAA; out of date since 2021 and the top OCR finding.	Approve with Q1 funding / defer to mid-2027	Approve now; cost to be confirmed with SureLock.	Dec 31, 2026
2	Decide on Contoso Imaging Archive	Critical access-control gaps; contract renewal is due in Q1.	Renew with conditions / replace vendor / accept risk	Renew only if MFA and named support accounts are in place by renewal; start evaluating an alternative now.	Jan 31, 2027
3	Fund an annual penetration test starting in 2027	No test has ever been performed; insurers and partners increasingly ask for one.	Fund annually / one-time test / not at this time	Fund annually, first test after MFA and backup fixes.	Mar 31, 2027

What needs to happen next

Over the next 90 days SureLock will finish multi-factor authentication on the EHR, prove that backups can survive a ransomware attack, and help the practice complete its HIPAA risk analysis. Log review, now overdue, starts this month.

What's working

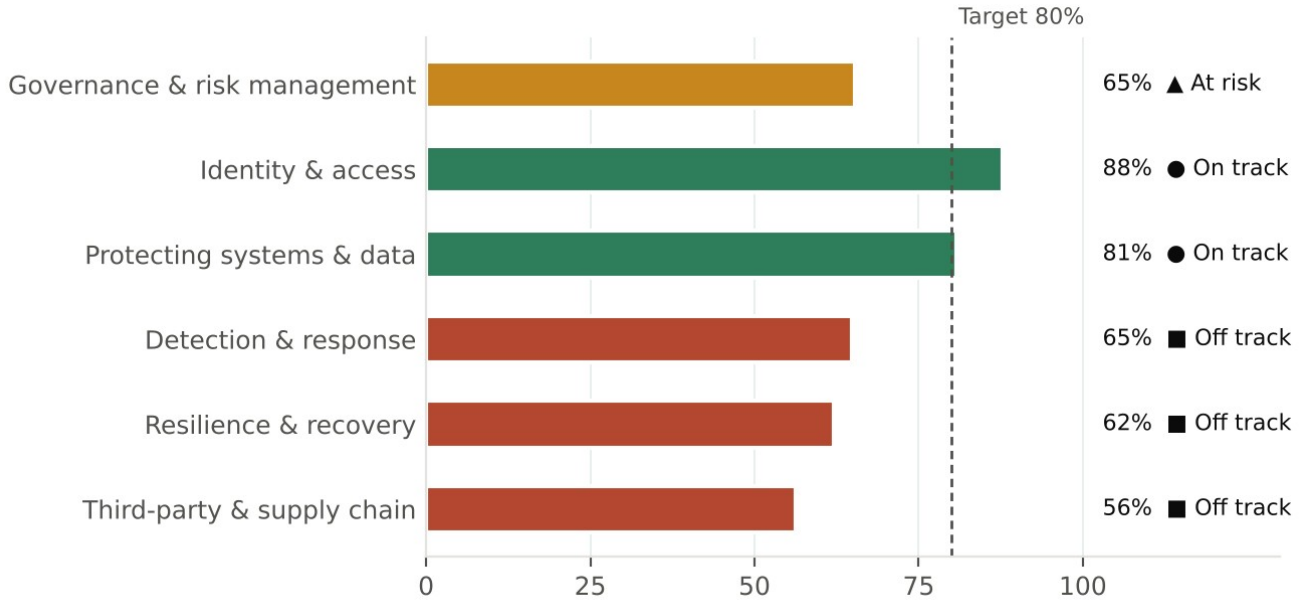
- Vendor remote access now requires named accounts and MFA.
- Monthly phishing simulations started; the first click rate was 18%.
- Every device and installed program is now tracked automatically.

Needs attention

- EHR multi-factor authentication, due Dec 15 (owner: SureLock).
- Microsoft 365 log review is overdue since Oct 31 (owner: SureLock).
- HIPAA risk analysis must be finished by Dec 31 (owner: Practice Administrator).
- Contoso Imaging Archive is not approved; a decision is needed before contract renewal.

Security program health by area

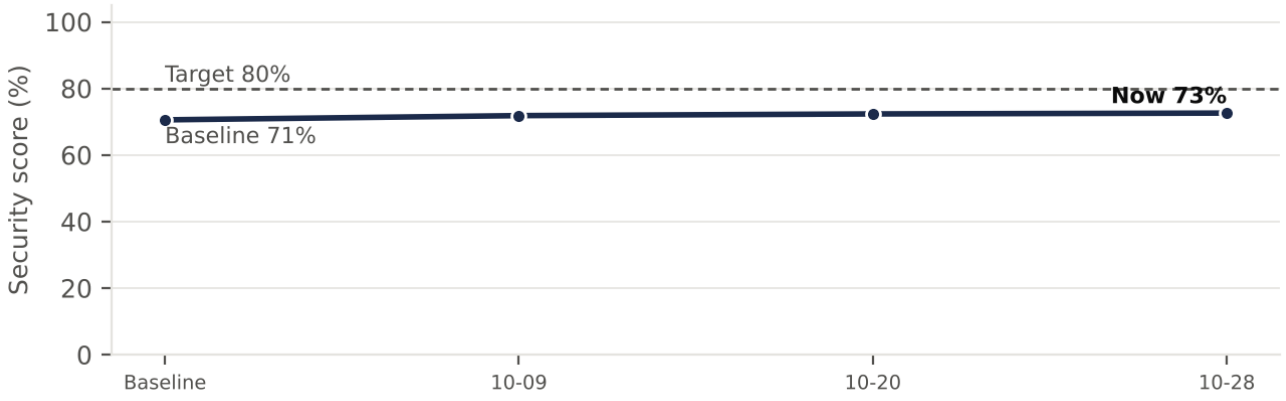
Score against the target of 80%. On track = at or above target; at risk = within 15 points; off track = more than 15 points below.



Area	Score	Status	Critical gaps	Other gaps
Governance & risk management	65%	▲ At risk	4	8
Identity & access	88%	● On track	3	1
Protecting systems & data	81%	● On track	2	7
Detection & response	65%	■ Off track	2	10
Resilience & recovery	62%	■ Off track	1	5
Third-party & supply chain	56%	■ Off track	1	2

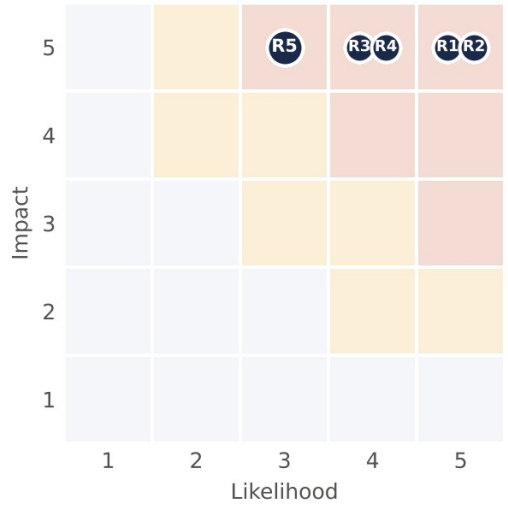
Progress over time

Score after each validated fix, from the baseline assessment.



Top risks and what we are doing about them

Each risk groups the open gaps in one area. Likelihood and impact are rated 1-5 from the assessment results; impact is raised one level when sensitive data is in scope.



Risk summary

R1 Governance & risk management: Because the HIPAA risk analysis is five years old, the practice cannot show regulators it understands its risks, the most common OCR penalty finding.

R2 Third-party & supply chain: Because vendor security is not yet tracked continuously, a weak vendor could expose patient data the practice is responsible for.

R3 Detection & response: Because no one reviews security logs, an attacker could stay in email or systems for months before anyone notices.

R4 Resilience & recovery: Because backups are not yet immutable or restore-tested, a ransomware attack could destroy them and stop the practice from seeing patients for days.

R5 Protecting systems & data: Because the backup device is unencrypted and the network is not scanned, a stolen device or unpatched weakness could lead to a reportable breach.

ID	Risk area	L	I	Open gaps being addressed	Owner	Due	Status
R1	Governance & risk management	5	5	• No penetration test has been performed • HIPAA risk analysis is five years out of date • Control Assessments: only partly in place	Practice Administrator, SureLock (MSP)	2026-12-31	In progress
R2	Third-party & supply chain	5	5	• Supplier Assessments and Reviews: only partly in place • External System Services: only partly in place • Policy and Procedures: only partly in place	Practice Administrator	2027-01-31	Not started
R3	Detection & response	4	5	• Policy and Procedures: only partly in place • Security logs are collected but not reviewed • Incident response has never been exercised	Practice Administrator, SureLock (MSP)	2026-10-31	Not started
R4	Resilience & recovery	4	5	• Contingency Plan: only partly in place • Contingency plan has never been tested • System Backup: only partly in place	Office Manager, Practice Administrator, SureLock (MSP)	2027-01-31	In progress
R5	Protecting systems & data	3	5	• Baseline Configuration: only partly in place • Configuration Change Control: only partly in place • Backup device stores patient data unencrypted	Practice Administrator, SureLock (MSP)	2026-12-15	Not started

Third-party risk portfolio

Vendors assessed with the SureLock questionnaire. Score and rating reflect overall controls; any open critical gap blocks approval until it is closed.

Vendor	Service	Score	Rating	Critical gaps	Decision
Contoso Imaging Archive (fictional)	Cloud PACS image archive	92%	Low Risk	6	NOT APPROVED
Northwind Cloud Billing (fictional)	Medical billing and claims platform (SaaS)	99%	Low Risk	0	APPROVE

Accountability

Open actions by owner. The 46 open remediation items plus 19 vendor items from the third-party assessments make 65 open actions. Overdue items are listed so they can be followed up.

Owner	Open actions	Overdue
SureLock (MSP)	5	1
Practice Administrator	40	0
Vendor	19	0
Office Manager	1	0

Overdue items

Overdue item	Where	Owner	Was due
Security logs are collected but not reviewed	Compliance readiness (gap assessment)	SureLock (MSP)	2026-10-31

Questions the board may ask

Q: If we were hit by ransomware tomorrow, could we keep seeing patients?

A: Partly. Paper downtime procedures exist, but backups are not yet proven to survive an attack. The restore test due Nov 30 will answer this; we will report the result.

Q: Are we compliant with HIPAA?

A: Not fully. The required risk analysis is out of date and is being completed by Dec 31. Most other safeguards are in place or in progress.

Q: What is the single biggest risk right now?

A: A stolen password reaching the EHR. Multi-factor authentication for the EHR is scheduled for Dec 8 and due by Dec 15.

Q: How do we know our vendors are safe?

A: Two key vendors were assessed. Northwind Cloud Billing was approved. Contoso Imaging Archive scored well overall but was not approved because six critical gaps remain open; it needs a decision before renewal.

Q: What will this cost?

A: Most fixes are inside the current SureLock agreement. The risk analysis and penetration test need separate approval; costs to be confirmed.

About this report

Scores come from the SureLock Security & Compliance Questionnaire (NIST SP 800-53 Rev 5 based, mapped to HIPAA, PCI DSS, CJIS, SOC 2, ISO 27001, NIST CSF 2.0, NIST SP 800-171 / CMMC, CIS Controls, GLBA Safeguards and FERPA). Each control is weighted Critical 5, High 3, Medium 2, Low 1; partial answers earn half credit; answers that need evidence earn half credit until the evidence is verified.

Program assessment: Compliance readiness (gap assessment) (Standard depth; targets: NIST 800-53 (baseline), HIPAA). Remediation is counted as closed only after SureLock has seen evidence that the fix works.

Narrative sections were drafted with SureLock's private, on-premises AI from the assessment data and reviewed by SureLock before release. All figures are calculated directly from the assessment records.