WRIGHTBRAINED
SECURITY

SAMPLE DELIVERABLE · HEALTHCARE

Quarterly Leadership Summary

Sample Health Billing Co. (fictional), Q3 2026. What leadership sees each quarter: where things stand, what changed, what's still open and what we need from you.

This is a sample. Sample Health Billing Co. is fictional. This is the quarterly summary our advisory clients' leadership teams receive: one or two pages, no jargon, and a clear ask.

The short version

Status: getting harder to hit. A quarter ago, one stolen password could have locked your billing systems for weeks. Today you have tested backups, two-step logins everywhere that matters, and someone watching around the clock. Two things are still open, and one needs a decision from you.

Where we stand

Area	Last quarter	Now	Trend
Backups you can actually restore	Untested	Tested Aug 2026, 6 hours	▲ Better
Two-step logins (MFA)	Email only	Email, remote access, admins	▲ Better
Computers centrally managed	71%	96%	▲ Better
Someone watching after hours	No	MSSP, 24/7, contract signed	▲ Better
Vendors reviewed	0 of 14	9 of 14	▲ Better
Staff phishing training	2025 cycle	Due November	● Same
Incident playbook practiced	Never	Scheduled Oct 22	● Same

What changed this quarter

Restored the billing platform from backup in a test: 6 hours, well inside the 24 hours the business said it could tolerate.

Two-step login turned on for remote access and all admin accounts. No more exceptions for executives.

Signed a 24/7 monitoring service. First after-hours alert handled in 14 minutes.

Reviewed 9 of 14 vendors that handle patient data. One clearinghouse rated Conditions.

Top risks now

Five vendors not yet reviewed, including the statement printing vendor, which receives full patient files weekly.

The incident playbook hasn't been practiced. A one-hour tabletop is scheduled for October 22.

Two older servers can't be patched and still run a legacy reporting tool.

Decisions we need from you

Retire or isolate the two legacy servers. Replacing the reporting tool is estimated at $38,000. Isolating the servers costs less but carries more risk. We recommend retiring them by the end of Q1.

Attend the October 22 tabletop (one hour). Leadership decisions are the part of an incident most worth practicing.

Next quarter

Goal	Owner	Target
Finish reviewing the remaining 5 vendors	Compliance lead	Nov 30
Run the ransomware tabletop and update the playbook	IT director	Oct 31
Complete the annual HIPAA risk assessment	Wrightbrained, with compliance lead	Dec 15
Staff phishing training, 100% completion	HR	Nov 30

We direct and verify; your team and vendors do the work. Detailed findings, the plan of action and monthly status reports are provided separately.

Want a second set of eyes?

We're assessors. We find the gaps, direct the fix, and check that it holds. **wrightbrainedsecurity.com/contact** · jil@wrightbrainedsecurity.com