

TECH & AI CASE STUDY - TELEHEALTH - 2025

HIPAA-Compliant Engineering That Passed a Telehealth Audit With Zero Findings

Based on a delivery engagement with Willowline Health

zero

AUDIT FINDINGS

100%

BAA COVERAGE

days to 5 min

ACCESS REVOCATION

\$8MHOSPITAL CONTRACTS
UNBLOCKED

A fillable practice edition: the full story, 8 actions,
6 reflections and a 90-day plan - work it with your team.

Free - no email requiredemersontechnology.com

MAKE THIS PRACTICE BOOK YOURS

Work it, do not just read it

This practice book turns the Willowline Health case study into a working session for your team. Read the full story first - what happened, what was built and what it changed. Then tick the 8 actions you can commit to, write short answers to the 6 reflections, and finish with a 90-day plan. Every field in this PDF is fillable: open it in Adobe Acrobat Reader, Chrome, Edge or macOS Preview, type directly into the boxes and save.

YOUR NAME	ROLE
COMPANY	TEAM / DEPARTMENT
DATE	EMAIL (OPTIONAL)

MY GOAL FOR THIS PRACTICE SESSION

- 01 The story** - What happened at Willowline Health - before, during and after the project.
- 02 The results** - The numbers that changed, plus industry benchmarks from public research.
- 03 The 8-action checklist** - Tick boxes as your organization completes each step. Owner and date fields included.
- 04 The 6 reflections** - Fillable questions that pressure-test your own roadmap.
- 05 My 90-day plan** - Three fillable phase cards that turn this case study into your roadmap.

RUN IT AS A 90-MINUTE TEAM SESSION

25 min READ Read the story together. Ask everyone to note the one number that surprised them most.	40 min PRACTICE Work the 8-action checklist and the 6 reflections. Assign an owner and a date to every action you commit to.	25 min COMMIT Fill in the 90-day plan. One goal per phase, one number that tells you it worked. Book a review date before you leave the room.
--	--	---

THE STORY

What happened, and why it worked

01 The Company

Willowline Health is a virtual-care provider employing 120 clinicians who deliver consultations, chronic-care follow-ups and behavioral health sessions through the company's video platform. The company grew the way many modern healthcare startups do: quickly, with clinical quality as the visible priority and infrastructure as the invisible one. Behind the clinician experience sat a collection of tools assembled at speed — video conferencing, a charting system, messaging apps, scheduling software, billing services and several analytics vendors, each adopted by a different team at the moment its need became acute.

Patients were well served and the clinical model worked. What had not kept pace was governance. Patient information — names, appointment records, clinical notes, billing details — flowed through more systems than any single person could list, and the company had never drawn a complete map of where that data lived or who could reach it. Willowline's leadership understood HIPAA primarily as a set of practices the clinical team followed; the idea that the entire data estate would need to stand up to a formal audit by a hospital partner's security team had not yet shaped how engineering, operations or vendor management made decisions.

02 Where Things Stood

An internal inventory undertaken before any external engagement produced the number that changed the conversation: 11 vendors were touching protected health information without signed business associate agreements. Some were minor tools adopted by a single department; others were load-bearing systems handling scheduling or messaging. None had been through a formal security review, because none had been routed through any review at all. The inventory also surfaced shared clinician logins on two systems — a practice inherited from an era when the clinical team was small enough to trust each other implicitly — and the absence of any centralized audit trail covering who had accessed which patient record and when.

Analytics made the exposure worse in subtler ways. Datasets exported to analytics vendors had been stripped of obvious identifiers, but the stripping was manual and incomplete, leaving combinations of fields that a determined party could re-identify. Deprovisioning was equally improvised: when a clinician left, their access ended whenever someone remembered to file the request, which meant departing staff sometimes retained working credentials for days or weeks. There was no single log an investigator could consult after an incident, because logging existed in fragments across 37 applications that touched PHI in one way or another.

The commercial stakes arrived in the form of a health system that accounted for a growing share of referral volume — \$8M in annual revenue — and that required a full HIPAA security audit before allowing Willowline to integrate with its care network. This was not a checklist exercise; the health system's auditors intended to sample systems, interview staff and test evidence. The founders recognized what a failed audit or a reportable breach would mean: an OCR investigation, state penalties, referral losses and a reputational wound that a young company might simply not survive. The audit date was set, and the gap between Willowline's actual posture and the evidence the auditors would demand was wide.

03 The Challenge

The challenge was to convert an undocumented, fast-grown data estate into an auditable compliance program without disrupting clinical operations for 120 practicing clinicians. Auditors test whether an organization knows where its data lives, who can touch it and whether its written policies describe reality — and at Willowline, the honest answers were "partially," "not individually," and "no." Every engineering control, vendor agreement and policy document would need to be built or rebuilt against a deadline owned by someone else.

There was also a sequencing problem that trips up many young healthcare companies. Fixing engineering controls before remediating vendor agreements leaves patient data flowing to parties with no contractual safeguards; fixing paperwork before fixing access controls produces a binder that describes protections that do not exist. Verizon's Data Breach Investigations Report consistently finds that human-centered patterns such as errors and phishing dominate healthcare incidents year after year, and IBM Security's 2024 research rates healthcare the costliest industry for breaches at \$9.77 million per incident — figures that shaped the founders' risk calculus. The program needed an order of operations: know the data, fix the contracts, close the technical gaps, then produce the documented evidence auditors actually sample. HHS's breach portal recorded healthcare breaches affecting more than 168 million individuals in 2023, an all-time high, and Willowline's leadership had no intention of appearing in next year's tally.

04 Discovery and Diagnosis

Emerson Technology began with a three-week data-mapping exercise that traced PHI from patient intake through video consultation, charting, billing and analytics — system by system, flow by flow, including the spreadsheet exports and ad hoc integrations that never appeared in any vendor list. The map confirmed 11 vendors touching PHI without BAAs and identified two analytics tools whose safeguards could not be brought to a compliant standard at reasonable cost. It also surfaced the full population of systems that would need audit logging: 37 applications, each with its own access model and its own gaps.

Diagnosis interviews with clinicians and operations staff added the human dimension that a tooling scan alone would have missed. Shared logins persisted because rotating shared credentials felt safer to clinical leads than managing individual accounts during a staffing crunch, and offboarding lagged because access changes depended on a manual request that competed with a hundred other tasks. The policy library, such as it was, had been copied from a template and described an organization Willowline was not — auditors interview staff, and gaps between documents and practice become findings fast. The discovery phase ended with a sequenced remediation plan and a clear statement of what the auditors would sample: the data map, the vendor file, the access model, the logs, the risk analysis and the incident response record.

05 The Solution

The program followed the order the diagnosis demanded, with each phase producing artifacts the next phase and the auditors would both consume.

Knowing where the data lives

The completed PHI data map became the program's backbone — every system, every flow, every party that stores or transmits patient information, documented well enough to withstand auditor sampling. Vendor remediation came next: business associate agreements were negotiated and signed for all 11 vendors, and the two analytics tools without compliant safeguards were retired outright, with their workloads migrated to a platform that could meet the standard. Retiring rather than absorbing the risk was a deliberate choice — a tool that cannot meet safeguards does not become acceptable because a contract is convenient. The vendor file, complete with agreements and data-flow records, turned from a liability into a sales asset almost immediately.

Access, encryption and the audit trail

Engineering closed the technical gaps in parallel sprints. Encryption in transit and at rest was applied uniformly across databases, backups, message queues and video infrastructure, converting most accidental-exposure scenarios into non-events. Role-based access with break-glass workflows replaced shared logins, and every clinician received a unique identity tied to the scheduling system, so access revokes within minutes of a departure rather than whenever someone remembers. The audit trail was centralized and made immutable across all 37 applications that touch PHI, with coverage rather than raw volume as the design goal — coverage is what auditors verify during sampling. By the end of this phase, a departed clinician's access revoked within five minutes and every PHI touchpoint produced log evidence automatically.

Producing the evidence

The final phase manufactured the artifacts the audit would sample: a penetration test against the production environment, a HIPAA Security Rule risk analysis with documented scope, methodology and tracked remediation, and a tabletop breach exercise in which the team rehearsed notification decisions against real timelines using a scenario where a vendor reports exposed patient data. Policies were rewritten to describe what engineers and clinical staff genuinely do each day, closing the gap between the binder and the building. The after-action memo from the tabletop, the risk analysis and the pen test report together formed an evidence base that outlived the audit itself.

06

The First 90 Days

Weeks one through three were the data map, built through paired sessions between Emerson Technology analysts and Willowline's operations lead, with every flow verified against actual system configuration rather than documentation. Weeks four through six concentrated on vendors: the legal workflow for BAAs ran against a named tracker, and the decision to retire the two non-compliant analytics tools was made and executed inside the window, including migrating the reporting their internal consumers depended on. This was the phase where momentum mattered most — vendor negotiations are where compliance programs quietly stall, and keeping the tracker public kept the signatures moving.

Weeks seven through ten delivered the engineering controls in three concurrent workstreams: encryption, identity and logging. Unique clinician identities were rolled out clinic by clinic, with scheduling-system integration completed before enforcement so no clinician lost a session; the shared logins were formally decommissioned on the same day individual access went live. Centralized immutable logging came online application by application, with each of the 37 systems' coverage verified by test queries rather than assumed from vendor documentation. The break-glass workflow was rehearsed once with clinical leadership so that an emergency access event would produce a documented, reviewed trail rather than a panic.

Weeks eleven and twelve were the evidence phase: the penetration test, the risk analysis documentation and the tabletop exercise, followed by a full internal dress rehearsal that sampled Willowline's own evidence the way the health system's auditors would. The dress rehearsal surfaced two documentation gaps — a policy referencing a decommissioned tool and an access-review record missing one signature — both fixed within days, and both exactly the kind of small defect that would otherwise have become a formal finding. By day 90 the company was running its compliance program as routine operations rather than an emergency project.

07 The Results

The health system's auditors closed their review with zero findings, making Willowline the only telehealth partner that year to clear on first inspection. Every vendor touching PHI now operates under a signed BAA — 100% coverage — departed-clinician access revokes within five minutes, and audit logs cover 100% of PHI systems. Both hospital contracts were signed the following quarter, unlocking the \$8M referral relationship the audit had gated. The risk analysis became the reusable evidence base for payer security reviews, and annual re-audits now run off existing evidence instead of a fire drill.

METRIC	BEFORE	AFTER
Audit findings	-	zero
BAA coverage	-	100%
Access revocation	days	5 min
Hospital contracts unblocked	-	\$8M

The cultural shift was as consequential as the control set. Compliance reviews that once would have triggered a scramble now draw from maintained artifacts, and the operations team treats vendor agreements as onboarding requirements rather than obstacles. The retired analytics tools removed a class of re-identification risk the company had not fully understood, and the rewritten policies survived staff interviews because they described real practice. For a company whose entire revenue model depends on health-system trust, the clean audit converted a security program from a cost center into the thing that opened the door.

08 What Your Business Should Do

The sequence Willowline followed is the sequence that generalizes, and its power lies in the ordering. Map PHI end to end before writing any policy — trace patient data from intake through video, charting, billing and analytics, because auditors test whether you know where PHI lives and most teams underestimate their footprint by half. Remediate vendor agreements next: inventory every third party touching patient data, collect signed BAAs for each, and retire tools that cannot meet safeguards rather than absorbing unmanaged risk into new contracts. Encrypt PHI in transit and at rest across databases, backups, message queues and video infrastructure alike, since uniform encryption converts accidental-exposure scenarios into non-events that auditors accept readily. Give every clinician a unique identity and tie it to your scheduling or HR system so access revokes within minutes of departure — shared accounts defeat every downstream control. Log every PHI touchpoint immutably in a centralized store, remembering that coverage, not raw volume, is what auditors verify during sampling. Run the risk analysis auditors expect, with documented scope, methodology and tracked remediation, because that document becomes the evidence base every subsequent payer and partner review reuses. Write policies that match what your teams actually do each day, since auditors interview staff and gaps between documents and practice become findings fast. Finally, exercise your breach response with a tabletop where a vendor reports exposed patient data, and practice notification decisions against real timelines — the after-action memo is exactly the evidence auditors sample. Take these eight steps in order with the action checklist in this practice book, and return to the reflection questions whenever a new vendor or system enters your environment: can you list every vendor touching patient data with agreements attached, how quickly does a departed clinician lose access, and what would a single reportable breach cost you in referrals, penalties and partner trust — is that number written down anywhere?

REAL-WORLD PROOF & BENCHMARKS

IBM's 2024 Cost of a Data Breach report finds healthcare the costliest industry for breaches at a reported \$9.77 million per incident. - IBM Security, 2024

HHS's public breach portal reportedly recorded healthcare breaches affecting more than 168 million individuals in 2023 — an all-time high for the sector. - HHS OCR portal, 2023

Verizon's Data Breach Investigations Report consistently finds human-centered patterns such as errors and phishing dominate healthcare incidents year after year. - Verizon DBIR, 2024

THE PRACTICE PAGES

The 8-action checklist

Work through the list with your team. Tick each box as your organization completes the step, and fill in an owner and a target date so every action has a name and a deadline.

☐**1. Map PHI end to end before anything**

Trace patient data from intake through video, charting, billing and analytics before writing any policy. Auditors test whether you know where PHI lives; most teams underestimate by half.

OWNER

TARGET DATE

STATUS

--	--	--

☐**2. Remediate vendor agreements first**

Inventory every third party touching patient data and collect signed BAAs for each one. Retire tools that cannot meet safeguards rather than absorbing unmanaged risk into new contracts.

OWNER

TARGET DATE

STATUS

--	--	--

☐**3. Encrypt PHI in transit and at rest**

Apply encryption standards across databases, backups, message queues and video infrastructure alike. Uniform encryption converts most accidental-exposure scenarios into non-events that auditors accept readily during reviews.

OWNER

TARGET DATE

STATUS

--	--	--

☐**4. Give every clinician a unique identity**

Eliminate shared logins and tie identities to your scheduling or HR system so access revokes within minutes of departure. Shared accounts defeat every downstream control.

OWNER

TARGET DATE

STATUS

--	--	--

☐**5. Log every PHI touchpoint immutably**

Centralize audit logging across all systems that store or transmit patient data, backed by tamper-evident storage. Coverage, not raw volume, is what auditors actually verify during sampling.

OWNER

TARGET DATE

STATUS

--	--	--



6. Run the risk analysis auditors expect

Perform a HIPAA Security Rule risk analysis with documented scope, methodology and tracked remediation. This becomes the evidence base that every subsequent payer and partner review reuses.

OWNER

TARGET DATE

STATUS

--	--	--



7. Write policies that match reality

Rewrite security policies to describe what engineering and clinical staff genuinely do each day. Auditors interview staff, and gaps between documents and practice become findings fast.

OWNER

TARGET DATE

STATUS

--	--	--



8. Exercise your breach response tabletop

Run a tabletop where a vendor reports exposed patient data and practice notification decisions against real timelines. The after-action memo is exactly the evidence auditors sample.

OWNER

TARGET DATE

STATUS

--	--	--

AFTER THE CHECKLIST: OUR TOP 3 PRIORITIES

From the eight actions above, write down the three you will start first - and the single number you expect each one to move. Three priorities with owners beat eight without any.

PRIORITY 1 NUMBER IT SHOULD MOVE	PRIORITY 2 NUMBER IT SHOULD MOVE	PRIORITY 3 NUMBER IT SHOULD MOVE
--	--	--

THE PRACTICE PAGES

Reflections for your team

Use these questions in your next planning session and type short answers into the boxes. The gaps you find are usually the fastest wins.

Q1. Could you list every vendor touching patient data in your organization today, with agreements attached?

Q2. How quickly is a departed clinician's access revoked — in minutes, days, or whenever someone notices?

Q3. If auditors sampled one PHI system at random, could you produce its complete access and audit logs?

Q4. Which of your analytics datasets would survive a serious re-identification attempt on 'de-identified' data?

Q5. Do your written security policies describe what your teams actually do, or what a template imagined?

Q6. What would a single reportable breach cost you in referrals, penalties and partner trust — and is that number written down anywhere?

THE PRACTICE PAGES

My 90-day plan

Finish the session by committing to a plan. Three phases, one goal each, one number that tells you it worked. Bring this page to your next leadership review - or to a free consultation with Emerson Technology, and we will pressure-test it with you.

Days 1-30 Focus: audit and alignment

PRIMARY GOAL**KEY ACTIONS****HOW WE MEASURE SUCCESS****OWNER**

Days 31-60 Focus: build and prove

PRIMARY GOAL**KEY ACTIONS****HOW WE MEASURE SUCCESS****OWNER**

Days 61-90 Focus: scale and measure

PRIMARY GOAL

KEY ACTIONS

HOW WE MEASURE SUCCESS

OWNER

Tip: save a copy per team so each group keeps its own answers. Revisit the reflections every quarter - the questions stay the same even as the numbers move.

BOOK THE REVIEW BEFORE YOU CLOSE THE BOOK

Plans without a review date drift. Before you close this practice book, agree on when you will come back to these pages, who will run that session, and when you will check the numbers again. If you want an outside pair of eyes, bring this page to a free consultation with Emerson Technology and we will pressure-test the plan with you.

REVIEW DATE	REVIEWED BY	NEXT CHECK-IN
------------------------------------	------------------------------------	--------------------------------------

Ready for a transformation like Willowline Health's?

Emerson Technology designs and builds the data, AI, cloud and automation systems behind results like these. On a free consultation call we will map this exact playbook to your business - your data, your constraints, your numbers.

Book a free consultation

support@emersontechnology.com

or start online: emersontechnology.com/contact