Texas Association for Home Care & Hospice
Leading ★ Advancing ★ Advocating

57th Annual Meeting

Wednesday, September 2, 2026

Seguin Room

11:15am-12:15pm

1d. Bridging the Gap: Managing Your IT Provider as a Compliance Partner — Security, Continuity, and Smart Automation for Home Care Agencies

Presented by:

Marjorie Costello, Chief Administrative Officer, DSSW/Lifespan

Adam Medders, VP of Operations, Black Lab Solutions

William Cochran, VP of Strategy, Black Lab Solutions

Thank you to our Partners:

Vesta®

HHAeXchange

MAC LEGACY

KanTime
How better happens.

United Healthcare Community Plan

AXXESS

TAHC&H 57TH ANNUAL MEETING · SESSION 1D

Bridging the Gap: Managing Your IT Provider as a Compliance Partner

Security, Continuity and Smart Automation for Home Care Agencies

Marjorie Costello · Adam Medders · William Cochran

September 2, 2026 · 11:15am – 12:15pm · Seguin

BLACK LAB SOLUTIONS

Your Healthcare IT Partner

1

1

Part 1 – Build the Foundation

Managing Your IT Provider as an Compliance Partner

3

2

OPERATIONS PARTNER

Five key categories for improvement

Use these as practical tests of whether your provider is operating as a partner.

1 Support interaction

Every request turns into a clear problem statement, agreed resolution, verified fix, and useful communication.

2 Overall relationship

The cadence is intentional: onboarding, status meetings when needed, and quarterly strategy at minimum. Steps taken / Next steps.

3 Accountability

Ownership is named. Dates are visible. Response and resolution are measured. Root Cause Analysis provided for critical incidents.

4 Detection

Your provider should know a critical system is down before you tell them.

5 Prevention

Repeat tickets decline because root cause, documentation, training, and automation improve.

HCSSA topics: §558.260(a)(8) working with other professional service providers; (a)(3) principles of management; (a)(5) quality improvement.

4

3

SUPPORT INTERACTION

Example of a common support interaction

Example request: Outlook is crashing after opening.

Incoming request

"Outlook crashes a few seconds after I open it."

"I've restarted twice. I'm stuck and need to send email."

What better support hears:

Impact, urgency, reproducibility, ownership, and a clear path to verification.

Troubleshooting workflow

A repeatable process turns a complaint into a verified resolution.

1. Discovery questions
2. Duplicate the issue
3. Define a problem statement
4. Define resolution
5. Resolve the issue
6. Verify the resolution
7. Effective communication with steps taken / next steps format

The goal is not simply "close the ticket." The goal is to fix the issue, prove it, and make the next interaction easier.

5

HCSSA topics: §558.260(a)(8) working with other professional service providers; (a)(5) quality improvement.

4

SUPPORT INTERACTION

Examples of Communication

Three ways to communicate the same Outlook crashing fix

1. Friendly Reply

Fixed, but light on detail

Hi Sarah,

We found the issue and Outlook is working again. It was caused by an Outlook add-in, and we disabled it.

Please let us know if it acts up again.

Thanks,
Adam Medders

2. Wordy Technical Explanation

Accurate, but dense and hard to digest

Hi Sarah,
We initiated a remote session and reproduced the failure condition by launching Outlook and observing the application terminate immediately after opening. We then reviewed Event Viewer, went to Application Log, and located an Application Fault entry indicating the crash was associated with an Outlook add-in. The add-in was disabled and Outlook was relaunched successfully, where it remained stable. To validate the root cause, the add-in was re-enabled and Outlook crashed again under the same condition. Based on that result, the add-in was disabled permanently, Outlook was reopened, and stability was confirmed. The working state was then demonstrated to you.
Regards,
Adam Medders

BEST

3. Best of Both

Clear for the user, with useful follow-up detail

Hi Sarah,
Thanks for your time today. We were able to resolve the Outlook crashing issue. It was caused by an Outlook add-in, which is now disabled. Please see technical notes below.
If the issue returns, please let us know.
Thank you,
Adam Medders

Steps Taken
– Screen shared and reproduced the Outlook crash
– Checked Event Viewer > Application, found an application fault identifying an Outlook add-in as the root cause
– Disabled the add-in and verified Outlook stayed open
– Re-enabled the add-in to confirm the crash returned
– Disabled the add-in permanently
– Verified with the user that the issue is now fixed

Next Steps
– Close the ticket – Document the fix in the internal KB article

6

HCSSA topic: §558.260(a)(8) skills for working with clients, families, and other professional service providers.

5

OVERALL RELATIONSHIP

Building / Maintaining a Relationship: Regular Communication

Better IT has regular communication: the relationship is managed before tickets become frustration.

Relationship cadence

1 First 60 Days — Build

Weekly onboarding

Are we meeting expectations? If not, what do we need to do to meet those or do we need to reset expectations. It is important to start off on the same page.

Steps taken

Review access, open issues, documentation gaps, critical systems, support contacts, and early service pain points.

Next steps

Assign owners and dates, confirm what will be fixed before the next meeting, and document decisions in the ticketing system.

2 Status Meetings — Maintain

Weekly, biweekly, or monthly until aligned

If the relationship feels out of sync, ask for status meetings until both sides are on the same page.

Steps taken

Review open tickets, escalations, missed expectations, pending decisions, recurring problems, and communication gaps.

Next steps

Reset priorities, name owners, define the next update, and reduce cadence only after the relationship stabilizes.

3 Strategy Meetings — Progress

Quarterly at minimum

Move beyond tickets and make sure IT is supporting operations, risk, growth, and continuity.

Steps taken

Review trends, outages, security posture, backups, lifecycle needs, recurring tickets, and upcoming business changes.

Next steps

Approve projects, budget priorities, risk remediation, prevention work, and the roadmap for the next quarter.

8

HCSSA topics: §558.260(a)(8) working with other professional service providers; (a)(3) principles of management.

6

ACCOUNTABILITY

Better accountability after critical incidents

Better IT does not stop at restoring service. It explains what happened, what changed, and how recurrence will be reduced.

Post Mortem / Root Cause Analysis

RCA

The document should make the incident understandable, show the true cause, and define how the same problem will be prevented or handled better next time.

Document should be provided after every critical incident. If not, ask your provider for a Post Mortem.

Components of a post mortem RCA document

Each item should be clearly documented, not implied.

1. Incident Summary	Describe what happened, specific dates/times, and what services, systems, or users were impacted.
2. Root Cause	State the confirmed cause, not just the symptom. Include contributing factors when needed.
3. Resolution	Explain how service was restored and what was done to stabilize the environment.
4a. Root Cause Resolution	Detail the permanent fix that resolves the actual cause of the issue moving forward.
4b. Permanent Workaround	If the root cause cannot be fully resolved, document a stable workaround such as a scheduled script, automated remediation, monitoring alert, or manual failover.
4c. Systematic Change	Capture the broader improvement: process change, training, documentation, automation, monitoring, or tooling that reduces recurrence.

HCSSA topics: §558.260(a)(5) quality improvement; (a)(6) risk assessment and management; §558.259(d)(4) agency responsibilities.

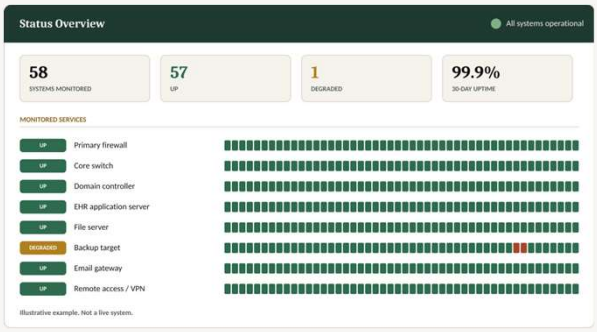
9

7

DETECTION

Down Detection / Visibility

Your provider should know there is a problem before you call them.



Illustrative only — no live or client system is shown.

What better detection looks like

A good provider detects quickly, alerts clearly, and gives you visibility into critical systems.

Monitoring	Critical systems are actively monitored so outages and failures are detected automatically.
Alerting	Alerts reach the right technician or team lead immediately when something important goes down.
Visibility	You should have visibility into the status of key systems, not just trust that someone is watching.

Questions to ask

How fast do you know something is down? · What systems are monitored today? · Who receives the alerts and after how long? · Do we have visibility into our critical systems?

What to be expected

The provider knows about issues before the first support call. · The client gets timely communication when critical systems are down. · Status visibility exists for the systems that matter most.

10

HCSSA topics: §558.260(a)(6) risk assessment and management; §558.259(d)(6) emergency preparedness planning and implementation.

8

TAKE THESE HOME

Helpful questions to ask your IT provider

Use these to get more value, more visibility, and a stronger IT partnership. A few strong questions can reveal whether your provider is reactive, proactive, organized, and accountable.

Detection & Monitoring

- What monitoring and alerting systems do you use?
- How quickly are you alerted when a critical system is down?
- Do we have visibility into the status of our critical systems?

Incidents & Accountability

- Do you maintain an incident list or incident history?
- After a critical incident, do you provide a post mortem or root cause analysis document?
- How do you show what changed to reduce recurrence?

Change Control

- Do you have a change control process?
- How are planned changes documented, approved, and communicated?
- How do you reduce the chance that a change creates downtime?

Communication & Escalation

- How do we request an escalation, and what happens when we do?
- How often should we hold status meetings or strategy meetings?
- During an outage, how often will you update us and who receives those updates?

Policies & Documentation

- Do you have IT and security policies in place?
- Do you document recurring fixes, procedures, and environment details?
- How do you manage administrative access, offboarding, and review of privileged accounts?

Service Improvement

- How do you measure whether support is improving over time?
- What recurring issues could be automated or permanently resolved?
- What should we be doing as a client to get the most out of the partnership?

HCSSA topics: §558.260(a)(8) working with other professional service providers; (a)(2) development and interpretation of agency policies.

11

9

2

Part 2 – Manage IT Compliance

Managing Your IT Provider as a Compliance Partner

12

10

Your IT provider is a business associate.

Whether or not anyone has ever said it out loud.

That single fact reorganizes the whole relationship — the contract, the documentation, and who answers when something goes wrong.

Business associate defined at 45 CFR §160.103.

13

11

Your IT provider is an extension of your organization.

How to operationally partner with your IT provider

IT should be technical customer service.

For regulatory authority, see the Authority crosswalk in the appendix.

14

12

THE LANDSCAPE

Why this matters right now

#1

MOST-CITED DEFICIENCY

Insufficient risk analysis remains the finding OCR cites most often — and it is the agency's obligation, not the vendor's.

3

PLACES IT SHOWS UP

An OCR investigation, a state survey, and your emergency preparedness review all ask about the same controls.

0

OF IT CAN BE DELAGATED

You can outsource the work. You cannot outsource the accountability.

For regulatory authority, see the Authority crosswalk in the appendix.

15

13

1

The Relationship

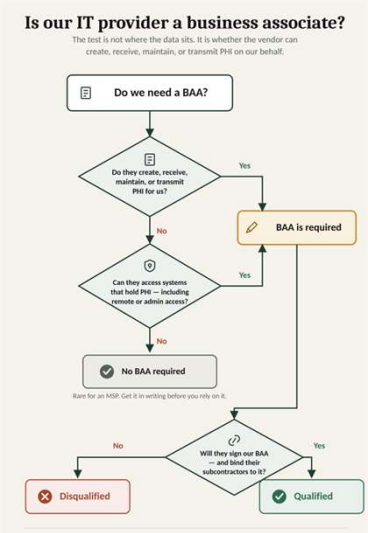
What the agreement has to say — and what it usually doesn't.

16

14

START HERE

Is our IT provider a business associate?



1. **Start with what they do.**
   Do they create, receive, maintain, or transmit PHI for us? If yes, stop — a BAA is required.
2. **If no, test access.**
   Can they reach systems that hold PHI, including remote or admin access? If yes, a BAA is required.
3. **Only if both are no.**
   No BAA is required — rare for an IT provider. Get the basis in writing before relying on it.
4. **Then one question decides it.**
   Will they sign our BAA and bind their subcontractors to it? If not, they are disqualified.

Authority: 45 CFR §160.103 (definition); §164.502(e) and §164.308(b) (contracts required).

17

15

REQUIRED BY REGULATION

What the BAA must contain

- Permitted and required uses and disclosures of PHI
- No use or disclosure beyond the agreement or law
- Appropriate safeguards against improper use
- Security Rule safeguards for electronic PHI
- Reporting of incidents and breaches to you
- Subcontractors bound to the same restrictions
- PHI available for access, amendment, accounting
- Records available to HHS for compliance review
- Return or destruction of PHI at termination
- Your right to terminate for a material violation

A BAA missing any of these is not weak — it is non-compliant.

Authority: 45 CFR §164.504(e)(2). Subcontractor flow-down at §164.314(a)(2)(iii).

18

16

NOT REQUIRED — BUT YOU WANT IT

Beyond the minimum

Breach notice in hours	A stated number. Not “promptly,” not “without unreasonable delay.”
A named contact	A person and an after-hours path, kept current and tested.
Who pays for forensics	And who drafts and funds patient notification.
A subprocessor list	Current, named, with notice before anything is added.
Named admin accounts	Per technician. Shared logins prohibited in writing.
An annual audit report	SOC 2 Type II, or your own right to audit.

Minimum breach notice from a business associate: 45 CFR §164.410. The rest is negotiated.

19

17

SLA TERMS

The service agreement is a separate document

What is in scope

Named systems, named locations, named hours. Anything unlisted is billable or unowned.

Response versus resolution

Two different clocks. Vendors quote the first and are measured on the second.

Escalation and severity

Who decides an outage is critical — you, or them?

Exit and transition

Credentials, documentation, data, and how many days of cooperation.

A BAA governs the data. The service agreement governs whether anyone answers the phone.

20

Authority: 45 CFR §164.504(e)(2). Subcontractor flow-down at §164.314(a)(2)(iii).

18

2

What You Cannot Delegate

The obligations that stay with the agency, whatever the contract says.

21

19

YOURS, PERMANENTLY

Eight obligations no agreement transfers

Risk analysis	Risk management	Policies and procedures	Workforce training
Sanctions	Breach determination	Designated officials	Emergency preparedness

A BAA moves obligations onto your vendor. It does not move accountability off you.

Authority: 45 CFR §§164.306, 164.308, 164.316; emergency preparedness at 42 CFR §484.102 / §418.113.

22

20

OBLIGATION ONE

The risk analysis is yours to direct

1	**Scope it**	Every system holding ePHI — including the ones your provider manages, and any AI tool added this year.
2	**Gather the input**	Your provider supplies technical detail. They do not write your conclusions.
3	**Sign it**	The agency reviews and signs. A vendor-authored, vendor-signed document is not your risk analysis.
4	**Remediate**	Findings get owners and dates. An analysis with no remediation plan is half a document.
5	**Refresh it**	At least annually, and whenever the environment materially changes.

Free tool: the HHS / ONC Security Risk Assessment (SRA) Tool — healthit.gov/privacy-security/security-risk-assessment-tool/

Authority: 45 CFR §164.308(a)(1)(ii)(A)–(B); review and update at §164.316(b)(2)(iii).

23

21

WHAT AN INVESTIGATOR ACTUALLY ASKS FOR

Evidence

Your current risk analysis	Dated within twelve months, signed by the agency.
Your BAAs	Executed, with subcontractor terms.
Access records	Who has administrative access, and when it was last reviewed.
Training records	Every workforce member, with dates.
Incident documentation	What happened, what you decided, and why.

Every item is a document. None can be produced retroactively.

Documentation and six-year retention: 45 CFR §164.316(b).

24

22

3

Continuity

Your IT continuity plan is part of emergency preparedness — not separate from it.

25

23

NOT A SEPARATE BINDER

Continuity belongs inside your emergency preparedness plan

- **Backups exist** — On a schedule, with at least one copy off-site and immutable.
- **Restores are tested** — In the last twelve months, documented, with a named tester.
- **RTO and RPO are agreed** — In writing, per system. How long down, how much data lost.
- **Downtime procedures exist** — For the EHR, scheduling, and clinical communication.
- **Field staff are trained** — They know what to do when systems are unavailable.

Authority: 45 CFR §164.308(a)(7) contingency plan; 42 CFR §484.102 (HH) / §418.113 (hospice).

26

24

4

Policies You Own

Your provider can help draft them. They cannot own them for you.

27

25

AGENCY-OWNED

Five policies that must be yours

1	**Acceptable use**	Signed by every workforce member.
2	**Mobile device and BYOD**	Field staff, personal phones, lost-device procedure.
3	**Sanctions**	Consequences for violations — and evidence you applied them.
4	**AI use**	What staff may put into which tools. Covered next.
5	**Annual review**	Dated and recorded, whether or not anything changed.

Authority: 45 CFR §164.316(a) policies; §164.308(a)(1)(ii)(C) sanctions; §164.308(a)(5) training.

28

26

5

Smart Automation

Where automation safely reduces burden — and where it must not go.

29

27

AND WHERE IT DOES NOT

Where automation earns its place

Safe to automate

- Eligibility and benefit checks
- Scheduling and route optimization
- Claim scrubbing before submission
- Document routing and filing

Automate with review

- Documentation drafting
- Coding suggestions
- QA chart sampling
- Referral intake triage

Do not automate

- Clinical decisions
- Eligibility or discharge determinations
- Anything signed without reading
- Patient communication without review

Authority: 45 CFR §164.308(a)(1)(ii)(A); §164.502(e).

30

28

THE APPROVAL GATE

Four questions before any new tool

1	**Does it process PHI?**	If yes: a BAA before use, a security review, and an entry in the risk analysis.
2	**What breaks if it is wrong?**	Classify low, moderate, or high. Oversight matches the classification.
3	**Can we pilot it small?**	One office, one workflow, thirty days, with success measures set beforehand.
4	**Who owns it?**	A named person — not a department. No owner, no approval.

Answers get written down and kept. A question that cannot be answered is answered "no."

Authority: 45 CFR §164.308(a)(1)(ii)(A); §164.502(e).

31

29

Every AI tool is a new business associate.

A new BAA. A new line in the risk analysis. A new entry in your tool register.

And know which tier you are in. The enterprise version of a product may be covered by a BAA while the free or personal version of the same product is not — identical interface,
entirely different contractual posture.

Authority: 45 CFR §160.103; §164.504(e); risk analysis at §164.308(a)(1)(ii)(A).

32

30

BRINGING IT TOGETHER

Score the relationship you already have

Contract and BAA 5 controls	**Access control** 5 controls	**Risk analysis** 5 controls	**Backup and continuity** 5 controls
Monitoring and patching 5 controls	**Incident response** 5 controls	**Agency policies** 5 controls	**Offboarding** 5 controls

Eight domains, five controls each — forty in all. Score every one 0, 1, or 2.

A control reads: "A restore was tested in the last 12 months, and documented."

"I think our IT company does that" is a zero, not a one.

Authority: 45 CFR §164.308(a)(1)(ii)(A); §164.502(e).

33

31

START HERE MONDAY

Three questions to ask this month

1. **Show me our executed BAA — and the subcontractors it covers.**
   You are testing whether it exists, and whether it reaches their bench.
2. **Show me the date of our last successful restore test.**
   A date, with evidence. Not a description of the backup schedule.
3. **Show me every account with administrative access, and who owns each one.**
   The most common real finding is an account belonging to someone who left.

A provider doing the job well answers all three inside a week. How long it takes is your real score.

For regulatory authority, see the Authority crosswalk in the appendix.

34

32

CLOSE

Three things to take home

1. **Your IT provider is a business associate.**
   Get the BAA, check the subcontractor terms, know where it is filed.

2. **You can delegate the work, not the accountability.**
   Eight obligations stay with you. The risk analysis is the first one.

3. **Every new tool is a new entry in the risk analysis.**
   Ask the four questions before adoption, and write the answers down.

Your materials: an oversight scorecard, a BAA checklist, and a model AI use policy.

For regulatory authority, see the Authority crosswalk in the appendix.

35

33

APPENDIX

Authority crosswalk

Business associate status

Definition
45 CFR §160.103

Contract required
§164.502(e), §164.308(b)

Required BAA terms
§164.504(e)(2)

Subcontractor flow-down
§164.314(a)(2)(iii)

BA breach notice to you
§164.410

What stays with the agency

Risk analysis
§164.308(a)(1)(ii)(A)

Risk management
§164.308(a)(1)(ii)(B)

Sanction policy
§164.308(a)(1)(ii)(C)

Security official
§164.308(a)(2)

Workforce training
§164.308(a)(5)

Breach notification
§§164.404–164.408

Continuity and records

Contingency plan
§164.308(a)(7)

Policies and procedures
§164.316(a)

Documentation, 6 years
§164.316(b)

Periodic review
§164.316(b)(2)(iii)

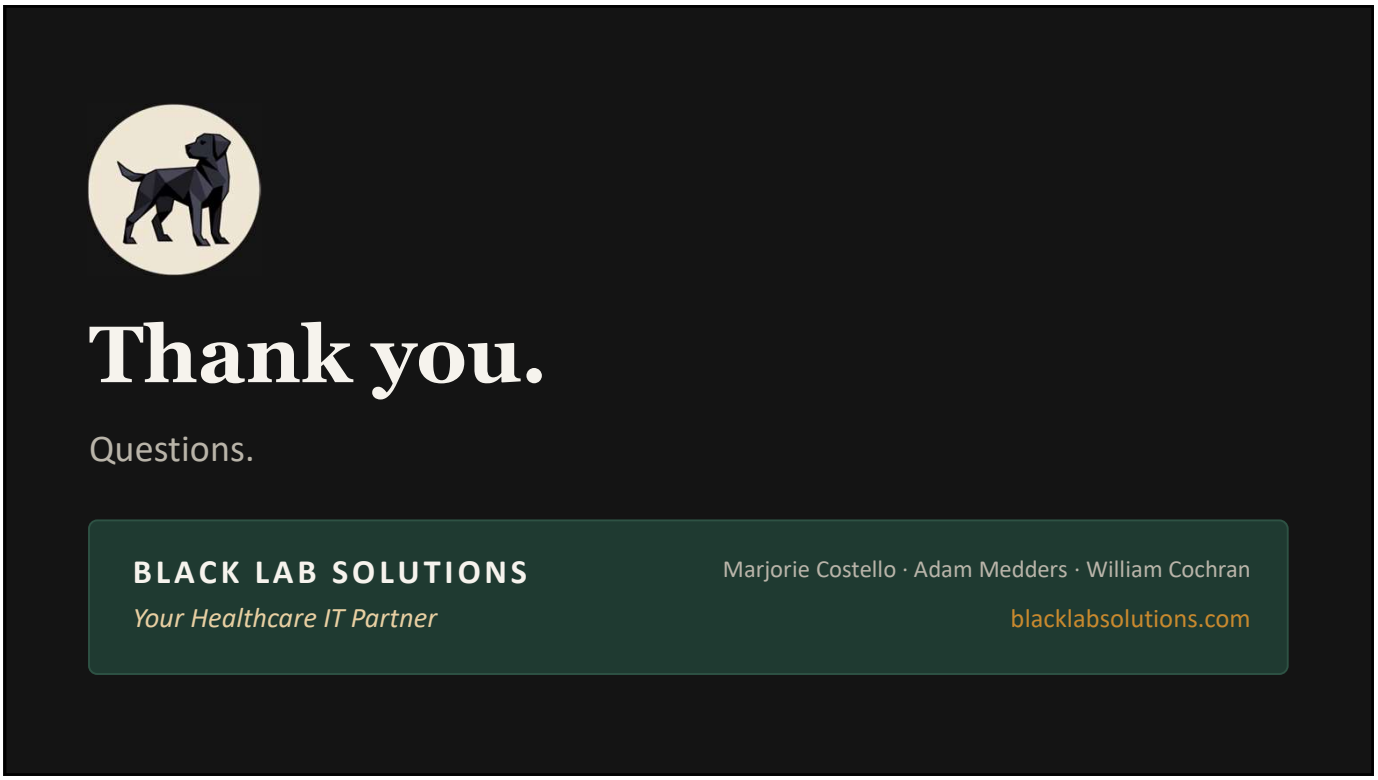
Emergency preparedness
42 CFR §484.102 / §418.113

Texas medical records
Tex. Health & Safety Code ch. 181

Unless noted, citations are to 45 CFR. Reference only — not legal advice.

36

34


Thank you.
Questions.
BLACK LAB SOLUTIONS
Your Healthcare IT Partner
Marjorie Costello · Adam Medders · William Cochran
blacklabsolutions.com

35