
THE INDUSTRY EDITION / 9 OCTOBER 2026

The hospital perimeter moved.

Ransomware reached hospital building systems, AI agents arrived without approval, and regulators drew the same line twice: document the risk and keep a licensed human in charge.

HEALTHCARE & LIFE SCIENCES

THE OPPORTUNITY

Ambient AI at scale, with note quality you actually sample.

THE CYBER QUESTION

Which building systems can reach the clinical network?

THE ACTION

A 90-day agenda: find it, own it, prove it.

In this issue.

Seven sections for the people who run a health system's technology, secure it and have to sign off what AI is allowed to do.

01	The briefing	The perimeter now includes the doors and the agents. Five dated signals, and what they do not establish.
02	AI in practice	Ambient AI at federal scale, and agents as identities. Scale is arriving before the quality evidence.
03	Cyber front	Ransomware reached the building. A phone call reached the network. Two incidents and one settlement.
04	The 90-day playbook	Find what is outside scope, put an owner and a control on it, then prove it works.
05	The decision desk	The regulator's bill is the small one. Figures from the public record, and the human-decides line.
06	Monday's agenda	Give every system an owner. A conversation for security, facilities, clinical informatics and the sponsor.
07	Sources & editorial notes	Eleven numbered references, each with what it does and does not establish.

HOW TO READ THIS EDITION

Reported events are attributed to their sources and were checked on 6 October 2026. Where a company has not confirmed something, we do not report it as fact.

The 90-day agenda, questions and checklists are original editorial proposals and a practitioner heuristic, not a published standard and not verified Agents Stack customer results.

This edition covers US and Canadian events. Have your legal or compliance specialist confirm which rules apply to your organization.

The perimeter now includes the doors and the agents.

For healthcare CISOs, CIOs and clinical technology leaders: this month's risks sat in systems, people and software that nobody had in scope.

The editor's view

Healthcare's attack surface widened in two directions this month. It went down, into building systems and front-line staff. It went out, into AI agents that many organizations have not formally approved. Neither direction is exotic. Both are places where a security program's inventory tends to stop.

The coverage window

Roughly 6 September to 6 October 2026, with one August incident included as context.

What regulators did

Regulators answered the same way on both fronts. For cyber, the first question is still whether you have a documented risk analysis. For AI, the direction is a licensed human making the final call, with bias and lifecycle controls behind the tool. [\[4\]](#) [\[7\]](#) [\[9\]](#)

The common thread

Every signal in this edition is a system, a person or an agent that sat outside someone's scope. So the recommendation is not a new product category. It is inventory and ownership: find what is unlisted, put a name on it, and prove the control works.

WHAT SAT OUTSIDE SCOPE THIS MONTH

01

Building systems

Doors and ventilation.

02

The help desk

A call from a familiar number.

03

AI agents

Deployed without approval.

04

Ambient notes

Scaled ahead of the evidence.

Five signals behind the recommendation.

What the public record supports, and what it does not.

01 / Ransomware hit the building, not the record

Winnipeg's Health Sciences Centre disclosed in August that ransomware affected facility maintenance systems, including door access and HVAC. Shared Health said there was no indication patients had been affected. [\[1\]](#) [\[2\]](#)

02 / A spoofed phone number opened the door

Astrana Health told the SEC that attackers impersonated company personnel and spoofed its main corporate telephone number. It considers the incident material. No number of affected people has been disclosed. [\[3\]](#)

03 / Agents are ahead of approval

In a survey of 250 US healthcare leaders by Vanson Bourne and Imprivata, 86% were fairly confident they can govern AI agent actions. In the same survey, 72% said some AI tools or agents are deployed without formal IT approval. [\[6\]](#)

04 / Two regulators, one line

California signed AB 1979 and SB 503 on 30 September. FDA's device center published its FY 2027 guidance agenda on 1 October, with AI lifecycle guidance among the top priorities. [\[7\]](#) [\[8\]](#) [\[9\]](#)

05 / Ambient AI reached federal scale

The VA's multi-award ambient scribe contract has a total ceiling of US\$775.72 million over five years, shared across eligible vendors. [\[10\]](#)

Every signal this month is a system, a person or an agent that sat outside someone's scope.

AGENTS STACK PERSPECTIVE

Research cut-off: 6 October 2026. The survey figures come from vendor-sponsored research; quote them with that attribution.

Ambient AI is at federal scale. The evidence is catching up.

What the VA contract does and does not tell a health system that is about to scale an AI scribe.

What was awarded

The US Department of Veterans Affairs selected Abridge under an enterprise ambient scribe contract. It is a multi-award vehicle: the US\$775.72 million ceiling over five years is shared by every vendor eligible to compete for task orders, not awarded to one company. Knowtix told Nextgov/FCW it was also selected. [10]

Where it already runs

Abridge says its scribe integrates with VA health records at more than 75 medical centers, across both the legacy and the new record systems. That is the company's own account of its product. [10]

The counterweight

Earlier Nextgov/FCW reporting notes that the VA did not provide data on note quality, and that a VHA-funded study found AI-generated notes scored lower than human-written notes across five standardized care cases. The VA says clinicians review and approve each note before it enters the record. [11]

Why this is a security question too

An ambient scribe writes into the legal medical record from a recorded patient conversation. That makes it a clinical-quality control and a high-value data store at once. Audio, transcripts and drafts each need an owner, a retention rule and an access list.

FOUR THINGS TO SETTLE BEFORE SCALING A SCRIBE

01

Note-quality sampling

A fixed sample, re-checked.

02

Consent handling

Clear for every recording.

03

Audio retention

How long, and where.

04

Vendor access

Matched to the data captured.

An agent is an identity with privileges.

Confidence in governing AI agents is high. The same survey suggests the inventory is incomplete.

What the survey found

A report by Vanson Bourne and Imprivata surveyed 250 US healthcare leaders responsible for security and AI strategy. 86% said they are fairly confident they can fully control and govern AI agent actions today. 72% said some AI tools or agents are deployed without formal IT approval. 57% ranked security as a top-three concern. [6]

Read it with care

This is vendor-sponsored research from an identity security company. Quote the percentages as survey findings with that attribution, and read the full report before using them in a board paper. The direction is still worth acting on.

Why identity programs miss it

An agent that reads the EHR, books appointments or files prior authorizations is a non-human identity with privileges. Most hospital identity programs were built for clinicians and service accounts, not for software that chooses its own next action.

Four questions to ask

Does every agent have its own identity, or does it borrow a person's session? Are permissions scoped per task and per patient context, with expiry? Can you produce a log of what an agent read and changed, in a form an auditor will accept? Who can switch it off, and how fast?

You cannot govern an agent that nobody approved.

AGENTS STACK PERSPECTIVE

Ransomware reached the building, not the record.

The most instructive healthcare incident of the quarter was about doors and ventilation, not patient files.

What happened in Winnipeg

Health Sciences Centre, Manitoba's largest hospital, disclosed on 10 August that ransomware had hit facility maintenance systems, including door access and heating, ventilation and air conditioning. Shared Health said clinical services continued and that there was no indication patients had been affected. The investigation was ongoing. [1] [2]

What we left out

Leak-site posts named several US providers and vendors in September. Those are attacker claims, not confirmed breaches, so they are not reported here.

A documented gap

Manitoba's auditor general reviewed Shared Health's cyber incident response process in December 2024. As summarized by Packetlabs, the audit found a plan and resources in place, recommended testing the plan through exercises, and noted that ransomware scenarios had not been tested. The audit does not establish a link to the 2026 incident. [2]

Why facilities sit outside scope

Building management systems often sit outside the clinical security scope, run older embedded controllers and keep vendor remote access open. Yet they hold operating-room air pressure, isolation-room ventilation and the doors to the pharmacy.

THREE QUESTIONS TO ASK THIS QUARTER

01

Network paths

Which building systems reach the enterprise or clinical network?

02

Vendor remote access

Is it still enabled, and who approves each session?

03

The tabletop

Was the facilities vendor in the last exercise?

A phone call is still the cheapest way in.

Two September events, one new and one six years old. Both come back to the basics.

Astrana Health, disclosed 22 September

The California-based company told the SEC that attackers impersonated company personnel and spoofed its main corporate telephone number to gain access to systems. It believes private or confidential information on its servers was accessed or acquired. It reset affected credentials, restricted remote access tools, restored certain systems from clean backups and expanded monitoring. [3]

What the filing does not say

Astrana calls the incident material because of the potential sensitivity of the data, and says it does not expect a material effect on its financial condition or results. The filing gives no number of people affected and does not mention ransomware. [3]

Ambry Genetics, announced 17 September

HHS's Office for Civil Rights settled with the genetic testing company for US\$700,000 and a two-year corrective action plan, over a January 2020 phishing attack affecting 225,370 people. OCR's findings start where they usually do: a risk analysis that was not accurate and thorough. [4]

The help desk control

The Astrana pattern argues for out-of-band verification on any credential or access request that arrives by phone, even from a number that looks internal. Caller ID is not an identity control.

A number that looks internal is not a verified person.

AGENTS STACK PERSPECTIVE

Find it. Own it. Prove it.

An Agents Stack agenda for healthcare CISOs and CIOs. It is a practitioner heuristic, not a published standard.

DAYS 0 TO 30

Find what is outside scope

Map building management, HVAC, access control and elevator systems, with their network paths and vendor remote access. Inventory every AI tool and agent in use, sanctioned or not, with the data each can reach. Confirm the security risk analysis is current, enterprise-wide and documented.

DAYS 31 TO 60

Put an owner and a control on each

Segment facility systems onto a managed network with controlled gateways. Give each AI agent its own identity, task-scoped permissions and an audit log. Add out-of-band verification for any access request arriving by phone.

DAYS 61 TO 90

Prove it

Run a tabletop where ransomware hits facilities, with the building vendor in the room. Document the human sign-off point for each clinical AI use case, plus its bias check and change control plan. Sample ambient scribe notes for quality and confirm audio retention rules.

THROUGHOUT

Keep the evidence

Retain the facility system map, the AI inventory, the risk analysis, agent audit logs, the tabletop record and the note-quality sample. This becomes the starting audit trail. It is not a claim of regulatory compliance.

Review group: security · IT · facilities and biomedical engineering · clinical informatics · compliance.

Two gates decide whether AI stays in use.

Write both of them down before the next agent or scribe goes live, not after the first wrong note.

GATE ONE

Control gate

Confirm each agent has its own identity and cannot act outside its task. Confirm a licensed clinician signs off wherever the tool informs a clinical decision. Keep a record of each test and of the configuration being evaluated.

GATE TWO

Pause conditions

Stop after unauthorized access, an agent acting outside its scope, an unreviewed note reaching the record or loss of the audit log. Route the event through the organization's incident process before any restart.

Why the inventory comes first

Segmentation, agent identities and sign-off points all depend on a list that is complete. An unlisted HVAC gateway or an unapproved agent defeats the control without anyone having to bypass it.

What a pause should look like

A named person, reachable during operating hours, with the authority and the access to switch an agent off without a committee. The manual process should already be rehearsed, so reverting is routine.

An inventory with gaps is a control with gaps.

AGENTS STACK PERSPECTIVE

The regulator's bill is the small one.

Figures from the public record of one phishing breach. They show how costs stack up, not what any other organization will pay.

ONE BREACH, TWO BILLS

US\$700K

OCR settlement, announced September 2026

US\$12.25M

Class action settlement fund, reported 2022

Reported figures in US dollars for the January 2020 Ambry Genetics breach. Not a forecast or a benchmark.

The timeline

The phishing attack happened in January 2020. The class action settled in 2022 with a US\$12.25 million fund. The federal resolution arrived in September 2026, more than six years after the breach, with two years of monitored corrective action still to run. **[4] [5]**

What it means for the business case

Private litigation cost far more than the regulator's figure, and it arrived first. A case for security basics that counts only regulatory penalties understates the exposure. It also leaves out six years of legal and compliance attention.

THE FIGURES BEHIND THE EXAMPLE

225,370

People affected

Per OCR.

6+ years

Breach to federal resolution

January 2020 to September 2026.

2 years

Corrective action plan

Monitored by OCR.

3

Potential violations cited

Risk analysis listed first.

AI informs. A licensed human decides.

Two regulators moved within 48 hours of each other, and both point the same way.

California, 30 September

Governor Newsom signed 11 AI bills on the last day of the signing period. Three touch healthcare. AB 1979 limits AI to an advisory role in licensed clinical functions and brings consumer healthcare chatbots under the state's medical confidentiality law. SB 503 requires developers and deployers of clinical decision support to make reasonable efforts to identify and mitigate biased impacts. [7] [8]

Check the rule before you buy

Treat any vendor claim that you must comply with a "new 2026 Security Rule" with caution. Check the Federal Register for the current status of the HIPAA Security Rule update before it shapes a purchase.

FDA, 1 October

The device center's FY 2027 guidance agenda makes finalizing lifecycle management guidance for AI-enabled device software a top priority, along with a draft on generative AI conversational devices for mental health. A draft on postmarket device cybersecurity is on the secondary list. Comments are open until 30 November 2026. [9]

The procurement checklist

If you sell or deploy clinical AI in the US, design for a documented human sign-off at each decision point, a bias assessment you can show and a change control plan for model updates. These are converging into the default checklist, whatever the state.

Before you cite the California bills: confirm effective dates and specific duties in the chaptered text. This edition relies on trade press summaries of both.

Give every system an owner.

A conversation for security, facilities, clinical informatics and the executive sponsor.

Ask facilities for the map

Which building systems have a network path to the enterprise or clinical network? Which vendors can reach them remotely, and who approves each session? If nobody can draw it on one page, that is the first finding.

Ask the help desk for the script

What happens today when someone calls from an internal-looking number and asks for a password reset or remote access? Agree the call-back step and who is allowed to skip it. The answer should be nobody.

Ask clinical informatics for the AI list

Which AI tools and agents are in use, approved or not? For each one, what data can it reach, whose identity does it use, and where does a licensed clinician sign off?

Ask compliance for the risk analysis

When was it last updated, and does it cover the whole enterprise, including facilities and AI tools? It is the first document a regulator asks for.

WHO HAS TO BE IN THE ROOM

01

Security lead

Owns the risk analysis.

02

Facilities

Brings the building map.

03

Clinical informatics

Brings the AI list.

04

Executive sponsor

Assigns the owners.

Rehearse the building outage in the same meeting.

A tabletop with the facilities vendor in the room tells you more than the written plan does.

Ask the vendor to join

Run the scenario where ransomware takes out door access and ventilation controls. Who secures the entrances? Who decides whether procedures continue? How do you reach the building vendor at 2 a.m.? Tested answers are worth more than a plan nobody has opened.

Ask the sponsor for one decision

Pick the date by which every agent and every facility system has a named owner. Do not mix that with a broader AI strategy discussion. Ownership is the deliverable.

The question to take to your team

Which system, person or agent in our organization could fail this week without appearing on anyone's list?

What to leave the meeting with

A facility system map, an AI inventory with owners, a call-back rule for the help desk and a date for the tabletop. If any of the four is missing, the plan is not yet testable.

Ownership is a control. Write the name down.

AGENTS STACK PERSPECTIVE

Planned next edition: retail and e-commerce. Not yet written or researched.

Evidence you can inspect.

Numbered references match the articles. All sources were checked on 6 October 2026.

[1] Ransomware Attack Disables Canadian Hospital's Doors, HVAC

BankInfoSecurity (ISMG) · 12 August 2026
Trade press. Reports Shared Health's statements; does not explain how the systems were reached.

[2] Health Sciences Centre ransomware attack

Packetlabs · 2026
Security vendor commentary. Our source for the December 2024 audit summary; read the auditor general's report before quoting it.

[3] Astrana Health, Inc. Form 8-K

US Securities and Exchange Commission · event date 22 September 2026
Primary source. The company's own disclosure; the investigation was ongoing at filing.

[4] OCR settles HIPAA investigation of Ambry Genetics

US Department of Health and Human Services · 17 September 2026
Primary source. OCR describes potential violations; a settlement, not a court finding.

[5] Ambry Genetics settles class action for \$12.25 million

The HIPAA Journal · September 2022
Trade press. Reports the settlement fund for the same January 2020 breach.

[6] Agentic AI access is a pressing governance challenge for providers

Healthcare IT News · 15 September 2026
Trade press on a Vanson Bourne and Imprivata survey of 250 US leaders. Vendor-sponsored research.

[7] California Gov. Newsom signs 3 bills to govern healthcare AI

Healthcare IT News · 1 October 2026
Trade press summary of AB 1979, SB 503 and AB 1609. Effective dates not stated.

[8] Gov. Newsom wraps California term by enacting 11 more laws on AI safety

Transparency Coalition · 2026
Advocacy organization summary. Our source for the 30 September signing date and the count of 11.

[9] FDA's device center releases guidance agenda for FY 2027

RAPS Regulatory Focus · October 2026
Professional body reporting. An agenda sets priorities; it is not final guidance.

[10] VA selects Abridge ambient scribe under new enterprise contract

Nextgov/FCW · 22 September 2026
Original reporting. Deployment figures are the vendor's own; the ceiling is shared across vendors.

[11] VA to gradually expand medical AI scribe following successful pilots

Nextgov/FCW · 14 September 2026
Original reporting. Cites a VHA-funded study of five standardized cases; we did not review the study itself.

EDITORIAL NOTES

Reported events are attributed to their sources. Attacker claims that a company has not confirmed are not reported. The 90-day agenda, questions and checklists are original editorial proposals, not verified Agents Stack customer results.

This magazine does not provide legal, clinical, financial or regulatory advice. Publication requires a named editor's approval and a final source check. No affiliation or endorsement by cited organizations is implied.



NEXT IN THE SERIES

Retail & e-commerce

Planned, and not yet written or researched.



Agents Stack

One industry. Useful AI. Accountable cybersecurity.

agentsstack.com