



The CISO's guide to healthcare AI governance

Healthcare has to find its AI-built tools before it can govern them, from a survey of 151 healthcare leaders

Contents

Executive summary	01
01 AI-built tools already handle patient data	02
02 Real patient data goes into the build	04
03 IT's controls cover the tools on its list	06
04 AI-built tools handled PHI without IT or security knowing	09
05 Leaders rank shadow IT low on list of concerns despite hidden AI-built tools	12
06 Governance starts with finding every tool	14
Recommendations checklist	16
Where Paubox fits	17
Methodology	18
Sources	19
Key findings	20

Executive summary

In a July 2026 Paubox survey of 151 healthcare leaders, 70% said their organization has found that an AI-built tool handled PHI without IT or security knowing.

This report covers AI-assisted development: healthcare staff using AI coding assistants to build tools, scripts, automations, and integrations, and how organizations govern that work. It draws on the same survey as The AI Build Benchmark [1], Paubox's report on adoption, and focuses on governance instead. Every respondent works at an organization that handles PHI electronically and uses AI coding assistants.

Healthcare leaders describe strong controls, and they also report what has already happened outside them:

- 85% say their organization's AI-built tools have handled, stored, or transmitted PHI.
- 87% say security, privacy, or compliance always or usually reviews PHI-handling AI code before deployment.
- 70% have found that an AI-built tool handled PHI without IT or security knowing.
- 54% say AI-generated code has contributed to hardcoded credentials or API keys, and 51% say it has contributed to PHI exposure.

Review and BAA checks only reach tools on IT's list, so an unlisted tool gets neither. That matters more now that HHS Office for Civil Rights (OCR) expects organizations to show they acted on the risks they document [2], because an unlisted tool never gets documented. So governing AI-assisted development starts with an inventory: a list of every AI-built tool and whether it touches PHI.

By the numbers

85%

say their organization's AI-built tools have handled, stored, or transmitted PHI

87%

say security, privacy, or compliance always or usually reviews PHI-handling AI code before deployment

70%

have found that an AI-built tool handled PHI without IT or security knowing

51%

say AI-generated code has contributed to PHI exposure

54%

say AI-generated code has contributed to hardcoded credentials or API keys

SECTION 01

AI-built tools already handle patient data

Tools that touch patient data belong inside the HIPAA compliance perimeter.



AI-built tools already handle patient data

85% of healthcare leaders said their organization's AI-built tools have handled, stored, or transmitted PHI. Only 9% said none have, and 6% didn't know.

organizations had deployed patient-facing AI-assisted tools into production. Because they handle patient data, HIPAA applies to them like any system that handles patient data.

These tools are already live. In the AI Build Benchmark [1], from the same survey, 80% of

Whether AI-built tools have handled PHI

PAUBOX 

85%

AI-built tools have handled, stored, or transmitted PHI

6%

don't know



■ Yes **85%** ■ No **9%** ■ Don't know **6%**

Source: Paubox survey of 151 healthcare leaders, July 2026.

• PAUBOX FORMS

Collect patient data with HIPAA compliant forms

Paubox Forms comes free with every paid Paubox plan.

[See Paubox Forms](#)

PAUBOX 

Patient intake form

Full name *

Date of birth *

[Submit](#)

SECTION 02

Real patient data goes into the build

Patient data reaches AI coding assistants before deployment, so a list of deployed tools misses it.



Real patient data goes into the build

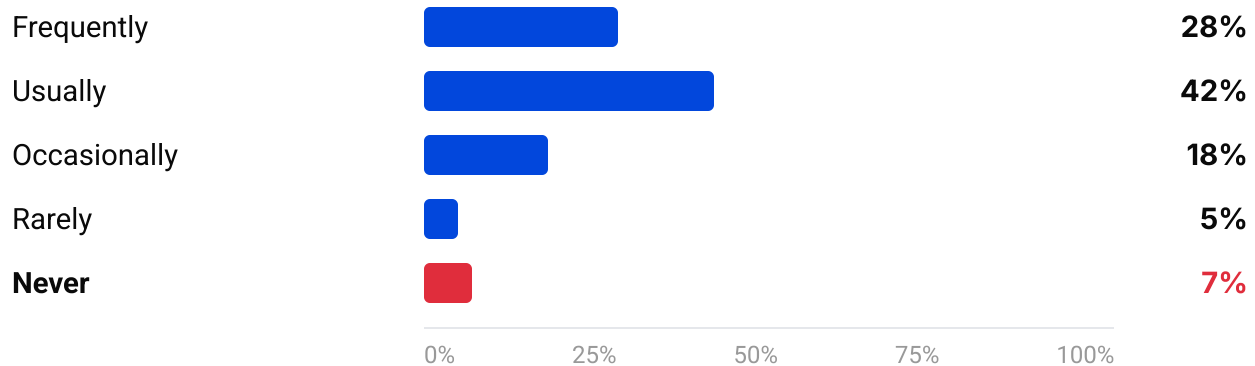
93% of healthcare leaders say real PHI reaches AI coding assistants at least some of the time while staff build, test, or debug, and frequently or usually is the most common answer. Only 7% say it never happens.

Each time that happens, patient data goes to an outside company, the coding assistant's vendor, before the tool is even finished.

How often staff enter real patient information into AI coding assistants

PAUBOX 

While building, testing, or debugging. n=151



Source: Paubox survey of 151 healthcare leaders, July 2026.

Real PHI reaches the assistant before deployment

PAUBOX 

STEP 1

Staff build, test, or debug



STEP 2 · THIRD-PARTY
VENDOR

AI coding assistant



STEP 3

Deployed tool

A list of deployed tools starts here

- **93%** of healthcare leaders say real PHI reaches AI coding assistants at least some of the time, while staff build, test, or debug.

Source: Paubox survey of 151 healthcare leaders, July 2026.

SECTION 03

IT's controls cover the tools on its list

Review and BAA checks only work on tools already on IT's list.



IT's controls cover the tools on its list

Healthcare leaders report the standard controls for AI-assisted development at high rates:

AI governance controls organizations report

PAUBOX 

Each bar comes from a separate question. With a margin of error of plus or minus 8 points, the first five controls sit too close together to rank. n=151

CONTROL		SHARE REPORTING IT
Prepared or very prepared to govern AI-assisted development over the next 12 months		85%
Security, privacy, or compliance always or usually reviews PHI-handling AI code before deployment		87%
Always or usually verify a BAA is in place before AI-built tools connect to third-party services that may handle PHI		87%
All or most AI coding assistant vendors have BAAs		83%
Trained all or some staff on safe use of AI coding assistants		93%
Written policy on AI coding assistants is fully implemented		50%

Source: Paubox survey of 151 healthcare leaders, July 2026.

Three of these controls depend on IT already knowing a tool exists: a pre-deployment review needs something submitted to review, a BAA check needs someone to report the connection, and a vendor BAA covers only the assistants under contract.

"...you can't do risk management unless you've done a good risk assessment. If you haven't done a risk assessment, you can't do risk management. So, the two...go hand in hand."

Paula M. Stannard · Director, HHS Office for Civil Rights [7]

The other three measure readiness: 85% feel prepared and 93% have trained staff, but only half have a fully implemented written policy on AI coding assistants. Feeling prepared and training staff don't tell IT which tools exist.

A written policy can. It can require staff to list every AI-built tool, name an owner for it, and get

it reviewed before it goes live with PHI. The list has to come first. OCR Director Paula M. Stannard has said there's no risk management without a good risk assessment first [7], and a risk assessment can only cover the tools an organization knows about.

What each control can see

CONTROL	TOOLS ON IT'S LIST	UNLISTED TOOLS
Review before deployment		Not reached
BAA check before a tool connects to an outside service		Not reached
BAA with the AI coding assistant vendor		Not reached

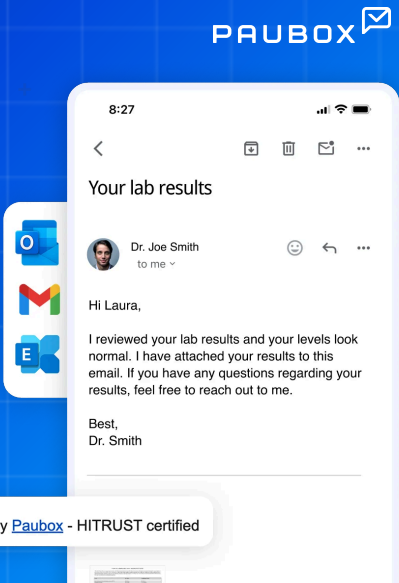
● An inventory finds unlisted tools.

● PAUBOX EMAIL SUITE

Encrypt every email by default

Paubox works with Google Workspace and Microsoft 365 to encrypt every email by default.

See how it works



Secured by Paubox - HITRUST certified

SECTION 04

AI-built tools handled PHI without IT or security knowing

Organizations that review AI code before deployment are still finding unreviewed tools.



AI-built tools handled PHI without IT or security knowing

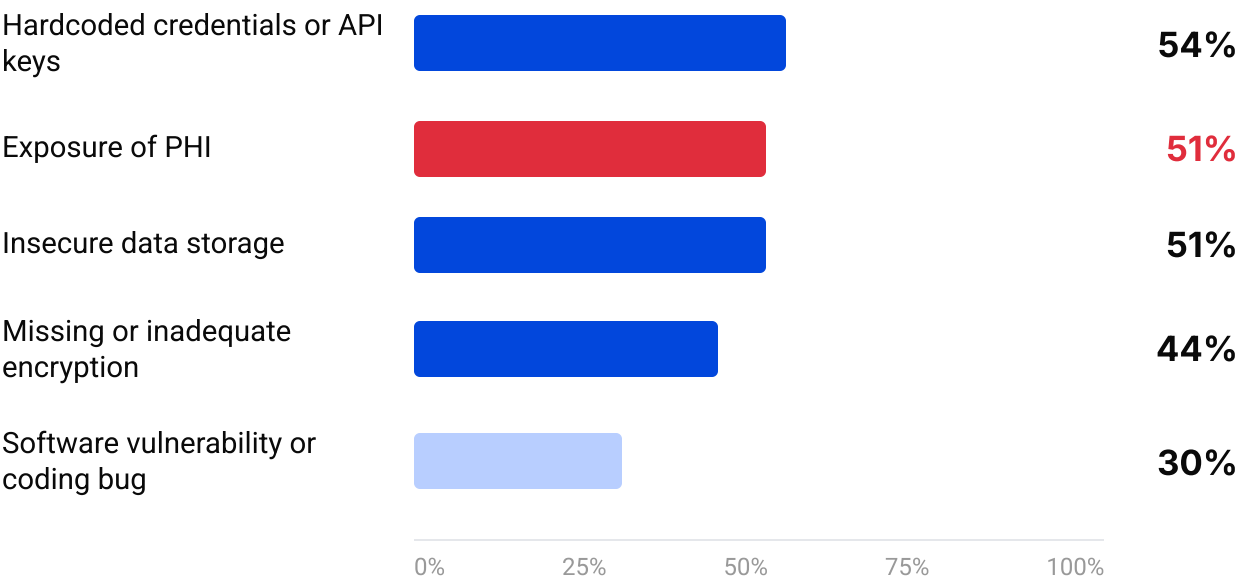
Seven in ten healthcare leaders (70%) say their organization has found that an AI-built tool handled PHI without IT or security knowing. That's true even though these same organizations report reviewing AI code before deployment. Review can only catch the tools someone submits for it.

Healthcare leaders also report what AI-generated or AI-assisted code has already contributed to:

AI-generated code contributed to security or privacy issues

PAUBOX

Share of organizations. The first four sit within ten points of each other, so they read as one group. Multiple selections allowed. n=151



Source: Paubox survey of 151 healthcare leaders, July 2026.



Seven in ten have found an AI-built tool that handled PHI without IT or security knowing

PAUBOX

Source: Paubox survey of 151 healthcare leaders, July 2026.

A high review rate and a high incident rate in the same organizations

PAUBOX 

n=151

Security, privacy, or compliance always or usually reviews PHI-handling AI code before deployment



87%

AI code contributed to PHI exposure



51%

0% 25% 50% 75% 100%

Source: Paubox survey of 151 healthcare leaders, July 2026.

The survey didn't ask whether reviewed code caused these issues, so the data can't tie them to review failures. It does show the same organizations reporting high review rates and high incident rates. One explanation is that AI exposes gaps that were already there, a point Frane Borozan, a Microsoft MVP, made in Syskit's State of M365 Governance Report 2026 [3].

"AI doesn't create new permissions; it shines a spotlight on existing ones."

Frane Borozan · Microsoft MVP [3]

● PAUBOX MCP SERVER

PAUBOX 

Keep API keys out of the model

Let your AI agents send HIPAA compliant email with the Paubox MCP server.

See how it works

```
mcp.json
{
  "mcpServers": {
    "paubox": {
      "url": "https://mcp.paubox.com"
    }
  }
}
```

Leaders rank shadow IT low on list of concerns despite hidden AI-built tools

Shadow IT ranks near the bottom of healthcare's concerns, and most organizations have already found it.



Leaders rank shadow IT low on list of concerns despite hidden AI-built tools

On PHI exposure and insecure code, what healthcare leaders worry about matches what they've already seen. Shadow IT, meaning tools staff use without IT's knowledge or approval, is the exception. Leaders rank it near the bottom

of their concerns, even though most have already found AI-built tools handling PHI without IT or security knowing. Here's how they compare:

Named as a concern vs. already reported



Concerns and issues allow multiple selections. n=151

NAMED AS A CONCERN

ALREADY REPORTED

Exposure of PHI



61%

AI code contributed to PHI exposure



51%

Insecure or vulnerable code



54%

AI code contributed to insecure data storage



51%

Shadow IT



25%

Found an AI-built tool handling PHI without IT or security knowing



70%

Source: Paubox survey of 151 healthcare leaders, July 2026.

On PHI exposure the two line up closely: six in ten list it as a top concern, and half say AI code has already contributed to it.

Shadow IT shows the widest split. One in four names it as a concern, yet 70% have already found an AI-built tool handling PHI outside IT's view. Third-party vendor risk is underrated

the same way, at 17%, even though every tool in this survey depends on an AI coding assistant vendor.

For both, Dr. Erik Huffman, a cyberpsychology researcher, gives simple advice in ManageEngine's The Psychology of Being Breached: verify first, then trust [4].

"We need to move from 'trust but verify' to 'verify, then trust.'"

Dr. Erik Huffman · Cyberpsychology researcher [4]

SECTION 06

Governance starts with finding every tool

An unlisted AI-built tool can't be in a risk analysis,
and seven in ten organizations have already
found one.

Governance starts with finding every tool

OCR has expanded its risk analysis enforcement initiative to cover risk management [2], so in an investigation it now wants evidence that an organization acted on the risks in its risk analysis. A tool IT doesn't know about never makes it into that analysis, and seven in ten organizations in this survey have already found one.

In a July 2026 settlement announcement, OCR Director Paula M. Stannard warned that organizations that don't know what threatens their ePHI "will often learn the hard way when their systems are hacked" [8].

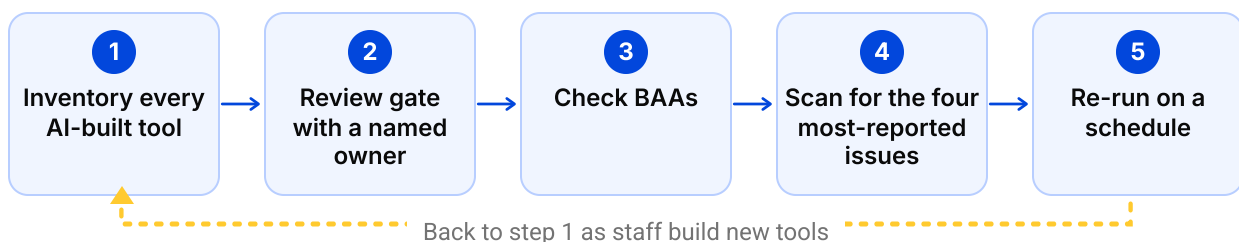
"An accurate and thorough HIPAA risk analysis is not only required by law, but it is also necessary to protect health information and prevent or mitigate ransomware attacks. If a HIPAA regulated entity doesn't know what threats and vulnerabilities exist to its electronic protected health information (ePHI), they will often learn the hard way when their systems are hacked."

Paula M. Stannard · Director, HHS Office for Civil Rights [8]

A one-time inventory won't stay complete, because most of these organizations told Paubox they expect AI-assisted development to

increase over the next 12 months [1]. The inventory needs a way to catch new tools as staff build them.

An inventory is a loop, not a one-time project

PAUBOX 


Recommendations checklist

OCR RECOMMENDED STEP

- 1 **Inventory every AI-built tool that touches PHI, plus the AI coding assistants behind it.**

Seven in ten organizations have already found one outside IT and security's view.

"Identify where ePHI exists in the organization, including how ePHI enters, flows through, and leaves the organization's information systems."

[HHS Office for Civil Rights](#) · recommended step for regulated entities [9]

- 2 **Put every listed tool behind a pre-deployment review gate with a named owner.**

Review only covers submitted tools.

- 3 **Check BAAs on every inventoried tool and its outside services.**

About one in eight organizations (12%) verify a BAA only sometimes, rarely, or never before those connections go live.

- 4 **Scan listed tools for the four most-reported issues: hardcoded credentials or API keys, PHI exposure, insecure data storage, and missing or inadequate encryption.**

Each affected between 44% and 54% of organizations.

- 5 **Set one rule on synthetic test data and enforce it in the tools themselves.**

Training alone hasn't kept real PHI out of coding assistants.

- 6 **Write the policy around the inventory, so every listed tool has a named owner and a review step.**

Only 50% have a fully implemented written policy today.

- 7 **Re-run the inventory on a schedule, because these organizations expect build volume to grow [1].**

Where Paubox fits

Once the inventory shows which AI-built tools touch PHI, each one needs a safe way to send it.

 **100% HIPAA compliant**



☆ 4.9/5 stars in G2

More than 9,000 healthcare organizations use Paubox

"You can't protect an AI-built tool you don't know exists. Reviews, BAA checks, and policies only work on the tools IT can see, so finding every tool that touches patient data has to come first."

Rick Kuwahara · Chief Operating Officer, Paubox

Paubox covers that layer, where patient data leaves the organization, with encryption on by default.

1 Give AI-built tools a compliant way to send PHI

When an AI-built tool needs to email a patient or a partner, the Paubox Email API sends it with TLS 1.2 or higher encryption by default, and a BAA comes with every plan, including the free tier [5]. Teams with an existing mail library can point it at the Paubox SMTP relay instead of rebuilding.

2 Keep credentials out of the model

More than half of respondents (54%) say AI code has contributed to hardcoded credentials or API keys. The Paubox MCP server lets Claude and other AI agents send HIPAA compliant email, and the API key stays with the server process [5][6].

3 Make encryption the default

44% say AI code has contributed to missing or inadequate encryption. For email, Paubox Email Suite closes that gap: it works with Microsoft 365 and Google Workspace to encrypt every email by default, so staff don't have to remember a step [5].

More than 9,000 healthcare organizations use Paubox.
Start for free with the Paubox Email API.

Start for free

Methodology

Paubox surveyed 151 healthcare leaders in July 2026 through TrendCandy. Every respondent works at an organization that creates, stores, or transmits PHI electronically, and every organization uses AI coding assistants, whether the organization formally adopted them (88%) or employees use them informally (12%). The margin of error is plus or minus 8 percentage points at the 95% confidence level.

Most respondents (77%) are IT or security leaders, with clinical or operations staff (9%), developers or engineers (8%), and executives,

compliance or privacy officers, and others making up the rest. Hospitals and health systems account for 63% of organizations, followed by healthcare consulting or services organizations (13%), payers (9%), and behavioral health providers (9%). Three in four organizations (76%) employ between 201 and 5,000 people.

This survey also produced the AI Build Benchmark [1], which reported adoption data. This report covers the governance questions from the same survey.

Sources

1. Paubox, *The 2026 Benchmark for Building with AI in Healthcare* (The AI Build Benchmark), August 2026. <https://www.paubox.com/research/2026-benchmark-building-with-ai-in-healthcare>
2. Steve Alder, "HHS Updates Security Risk Assessment Tool," *The HIPAA Journal*, September 11, 2026. <https://www.hipaajournal.com/hhs-security-risk-assessment-tool-3-7/>
3. Syskit, *The State of M365 Governance Report 2026: The Confidence Gap*, September 2026. Quote: Frane Borozan, Microsoft MVP. <https://www.syskit.com/ebooks/state-of-m365-governance-report-2026>
4. ManageEngine, *The Psychology of Being Breached*, September 10, 2026. Quote: Dr. Erik Huffman, Cyberpsychology Researcher. <https://www.manageengine.com/insights/survey/the-psychology-of-being-breached.html>
5. Paubox product pages, accessed October 13, 2026. <https://www.paubox.com/> ; <https://www.paubox.com/products/paubox-email-api> ; <https://www.paubox.com/products/email-suite>
6. Paubox, "How to send PHI from an AI agent without exposing it," July 17, 2026. <https://www.paubox.com/blog/how-to-send-phi-from-an-ai-agent-without-exposing-it>
7. Health Care Compliance Association, "OCR Director Stannard: Enforcement Widening To Encompass Risk Management, Parents' Access," *Report on Patient Privacy*, January 2026 (interview conducted December 2025), via JD Supra. Quote: Paula M. Stannard, Director, HHS Office for Civil Rights. <https://www.jdsupra.com/legalnews/ocr-director-stannard-enforcement-9412645/>
8. HHS, "HHS' Office for Civil Rights Settles Ransomware Investigation with Healthcare System," July 29, 2026. Quote: Paula M. Stannard, Director, HHS Office for Civil Rights. <https://www.hhs.gov/press-room/hhs-ocr-settles-ransomware-investigation-with-healthcare-system.html>
9. HHS, "HHS' Office for Civil Rights Settles Ransomware Investigation with Health Plan," June 18, 2026 (OCR recommended steps). <https://www.hhs.gov/press-room/ocr-settles-ransomware-investigation-health-plan.html>

KEY FINDINGS

The CISO's guide to healthcare AI governance

25%

name shadow IT as a concern

12%

verify a BAA only sometimes, rarely, or never before AI-built tools connect to outside services

61%

name PHI exposure as a top concern

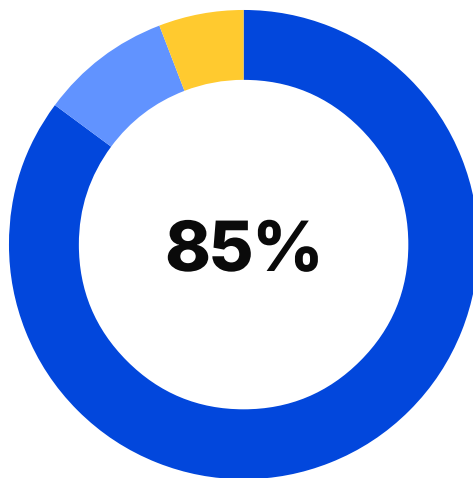
70%

have found an AI-built tool that handled PHI without IT or security knowing

AI-built tools have handled, stored, or transmitted PHI

PAUBOX 

Share of healthcare leaders. n=151



Yes	85%
No	9%
Don't know	6%

Source: Paubox survey of 151 healthcare leaders, July 2026.

KEY FINDINGS

Review and BAA checks only reach tools on IT's list

Review rate vs. reported PHI exposure

PAUBOX 

n=151

Security, privacy, or compliance always or usually reviews PHI-handling AI code before deployment



87%

Say AI code contributed to PHI exposure



51%

Source: Paubox survey of 151 healthcare leaders, July 2026.

93%

say real PHI reaches AI coding assistants at least some of the time

50%

Only 50% have a fully implemented written policy on AI coding assistants

Source: Paubox survey of 151 healthcare leaders, July 2026.

AI-generated code contributed to security or privacy issues

PAUBOX 

Shown as one group: all four are within 10 points. Multiple selections allowed. n=151

Hardcoded credentials or API keys



54%

PHI exposure



51%

Insecure data storage



51%

Missing or inadequate encryption



44%

0% 25% 50% 75% 100%

Source: Paubox survey of 151 healthcare leaders, July 2026.



Give AI-built tools a **compliant way** to send PHI

When AI-built tools need to email a patient or a partner, the Paubox Email API sends it encrypted by default.

Start for free

