

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."

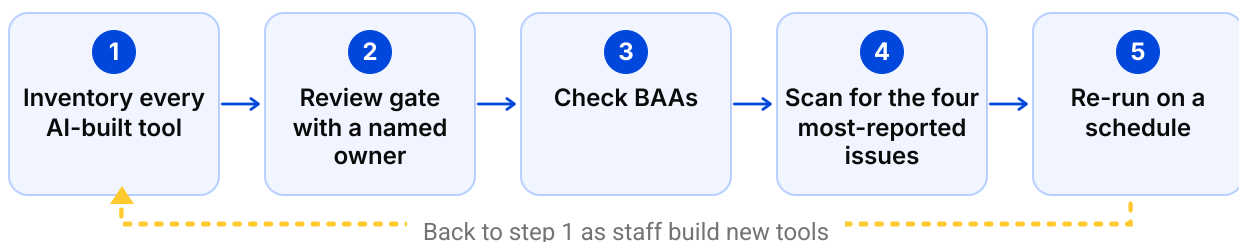
Paula M. Stannard · Director, HHS Office for Civil Rights [8]

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



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

