

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

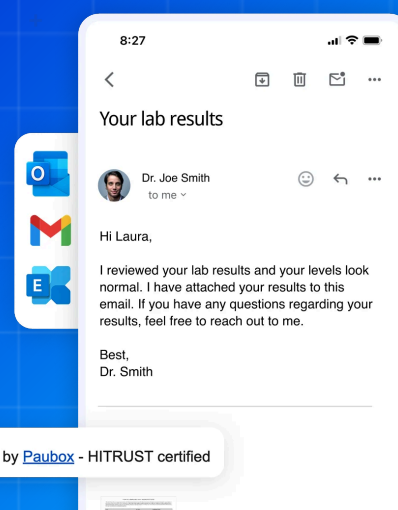
● **An inventory** finds unlisted tools.

● 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](#)





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

