

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

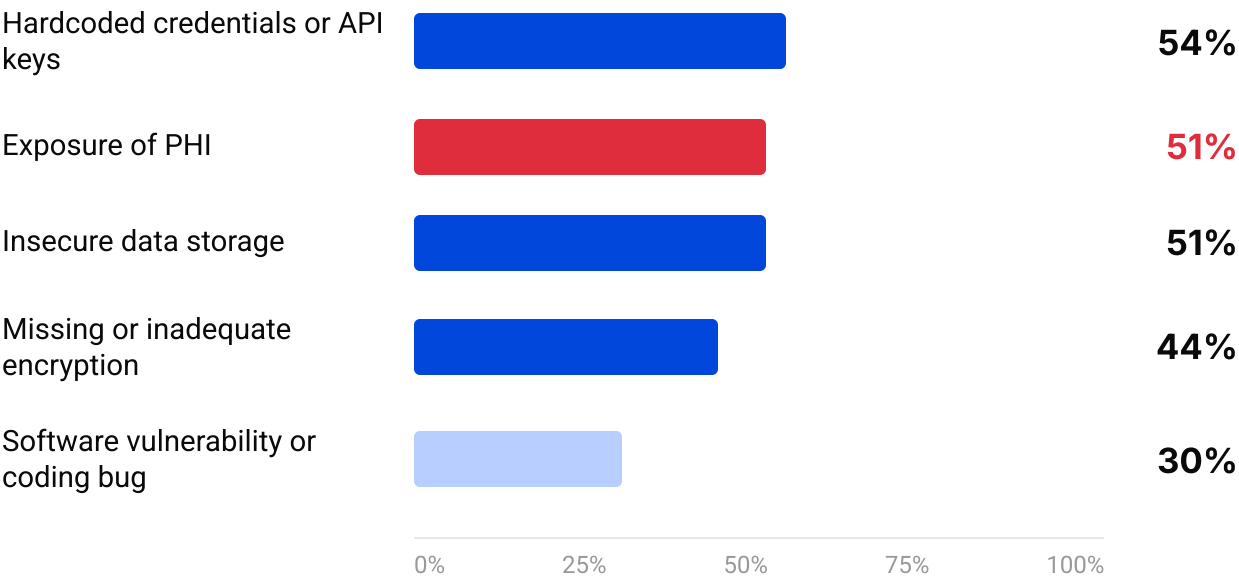
Seven in ten healthcare leaders (70%) say their organization has found that an AI-built tool handled PHI without IT or security knowing. That's true even though these same organizations report reviewing AI code before deployment. Review can only catch the tools someone submits for it.

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]

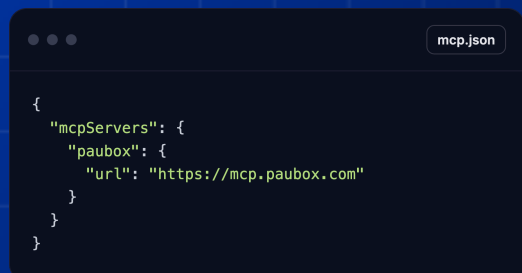
● PAUBOX MCP SERVER

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"
    }
  }
}
```



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

