SECTION 05

What comes next

Seventy percent of these organizations expect AI-assisted development to increase over the next 12 months. One percent expect a decrease.

Where it's heading

Seventy percent of these organizations expect AI-assisted development to increase over the next 12 months. One percent expect a decrease.

Outside healthcare, 89% of development executives told Forrester's Developer Survey, 2025 that their firm is either currently implementing or actively planning a citizen developer strategy [2]. The difference in healthcare is the mechanism: AI coding assistants, versus the low-code platforms that carried the earlier wave. Low-code platforms shipped with guardrails an administrator configured. Consumer AI coding assistants can ship with no compliance layer. Teams are able to move faster, but organizations need to be prepared with policies to keep patient data secure.

Gartner projects that by 2027, more than 65% of engineering teams using agentic coding will treat integrated development environments as optional, shifting control, governance, and validation to automated platforms [3].

> "What began as a race to deliver the most 'magical' developer experience is now evolving into a contest of operational excellence, commercial maturity, and enterprise readiness."
>
> **Philip Walsh** · Sr Director Analyst, Gartner [3]

Three things worth planning around

The builder pool will keep widening. Non-developer enablement is already an important driver for 81% of these organizations, and 70% expect AI-assisted development to increase over the next 12 months. Planning for software that comes only from an engineering team will describe fewer and fewer organizations.

Patient-facing output will keep growing. A majority already build patient-facing forms and portals with AI assistance, and 80% have shipped patient-facing tools to production. The next 12 months add to that base.

The gap between vendor AI and self-built AI will widen. Health systems report real difficulty scaling vendor AI, with only 4% reporting measurable outcomes at scale and 74% blocked by EHR vendor roadmaps [1]. Self-built AI-assisted tooling has no such dependency, which is part of why the volume is what it is.

RECOMMENDATIONS

Recommendations

1. **Inventory who builds, alongside what runs**

   Ask each department head which tools their team has built or changed with AI in the last 12 months. Most inventories catalog systems. This one catalogs authors, and it is the only way to find the 38% case where clinical staff are shipping software.

2. **Add one question to your review intake**

   "Was any part of this built with an AI coding assistant?" A yes routes into the same review, logging, and access control as everything else. One field is cheaper than a new process, and it tells you what your inventory missed.

3. **Pull the patient-facing list**

   Every AI-assisted tool a patient sees, submits to, or receives a message from. In this study 80% of organizations have at least one. Review that list on its own track, separately from internal tooling.

4. **Map the integration surface and name an owner for each connection**

   82% of these organizations connect systems to AI through APIs and 79% use MCP connections. Document them while the count is still small enough to document.

5. **Time the sanctioned path against the workaround**

   Publish the approved toolset, then measure how long it takes to ship something through it versus around it. If the approved path is slower, policy will not fix that. Design will.

6. **Size governance for next year's volume**

   Seventy percent of these organizations expect AI-assisted development to increase. Review capacity sized for today's output is already behind.

7. **Check the delivery layer on everything in that list**

   For each tool that emails a patient, sends a reminder, or delivers a result, confirm the channel it sends through is encrypted and covered by a BAA. This is the fastest item on the list and the one with the shortest path to a reportable breach.

PAUBOX

EMAIL ENCRYPTION

Secure email for healthcare

What effective implementation looks like

100% HIPAA compliant

r2 HITRUST CERTIFIED

4.9/5 stars in G2

The findings in this report describe a production reality: more software, built by more people, reaching patients, connected to more systems. Each of those trends adds another channel PHI travels through.

1. **Secure the outbound layer specifically**
   Paubox Email Suite and the Paubox Email API encrypt every message by default, with no tags, portals, or user decisions required at send time.

2. **Give agents a compliant way to act**
   The Paubox MCP server lets agents send HIPAA compliant email through the Paubox Email API, and the API key stays with the server process, never entering the model's context.

3. **Build on infrastructure that carries its own proof**
   Paubox signs a business associate agreement (BAA) with every customer on every plan, enforces TLS 1.2 or higher by default, and is HITRUST certified.

4. **Building with AI in healthcare**
   Paubox's working guide to which AI providers will sign a BAA, safe patterns for running models on patient data, and how an agent can send PHI without holding the credential that sends it [5].

> "Nobody set out to turn their operations team into developers. It happened anyway. That's a net positive, but it means the risk surface has shifted and compliance and security teams have to catch up. And that starts with knowing who is building what."
>
> **Rick Kuwahara** · Chief Compliance Officer, Paubox

PAUBOX

Build on a compliant layer

Paubox encrypts every message by default, signs a BAA with every customer on every plan, and gives AI agents a compliant way to send PHI.

Start for free

Ryan Winchester
Paubox Customer, CareM