

PATIENT IDENTITY MANAGEMENT AT ENTERPRISE SCALE

Why healthcare organizations need identity that persists across systems, channels and time



The Reality

Healthcare Has Digitized Access Faster Than Identity Could Keep Up

More than 50% of individuals now manage multiple patient portals or online medical records.*

-  Patients now engage across multiple systems and portals.
-  Patient information changes across encounters, channels and years.

-  Identity is often established early, then implicitly trusted.
-  Fragmentation accumulates quietly as records drift over time.

Only 7% report using tools to combine information from multiple portals.*

The Impact

When Identity Weakens, Trust Diminishes

Identity failure doesn't stay operational. It shows up across the organization.

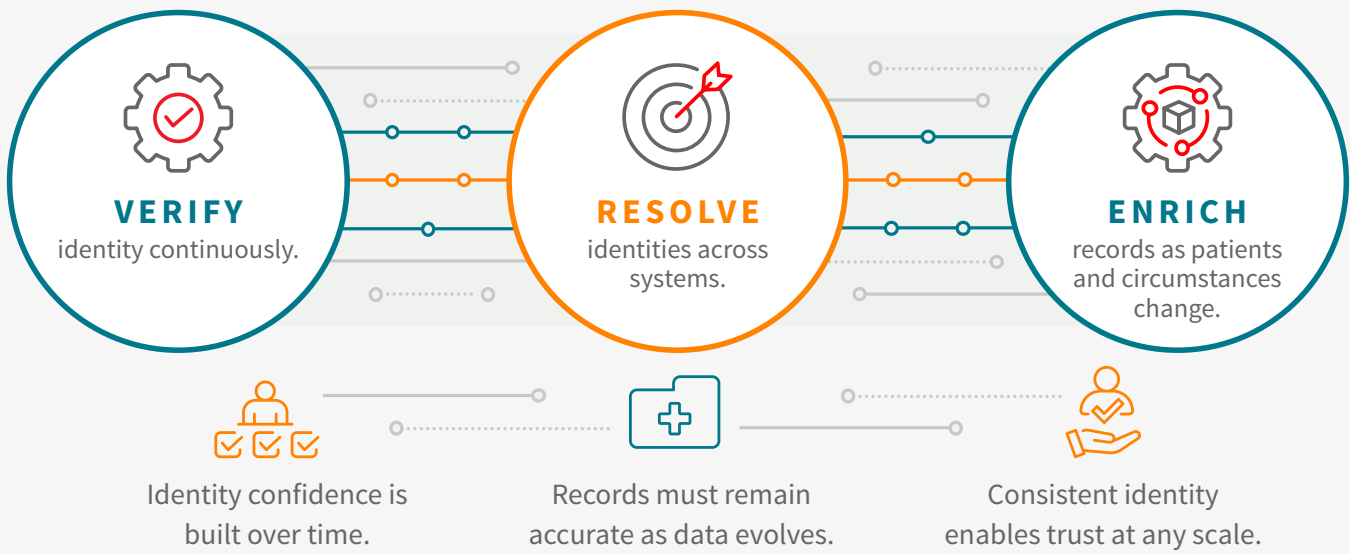
-  **Cyber risk**
Every interaction is an identity decision.
-  **Digital friction**
Legitimate patients feel the cost.
-  **Data integrity risk**
Analytics and AI depend on trusted identity.
-  **Operational and financial impact**
Errors compound across workflows.

What appears as fragmentation is often the result of enterprise identity decisions that don't persist across verification, resolution and enrichment over time.

The Shift

Identity Must Follow the Patient Over Time

Patient identity has to persist across interactions, systems and years — just like care does.



Key Takeaway

Modern healthcare data cannot be managed with transactional identity management.

This is why patient identity increasingly shows up in board level discussions about trust, risk and scale.

Sources

* National Institutes of Health, "Individuals' Access and Use of Patient Portals and Smartphone Health Apps." <https://www.ncbi.nlm.nih.gov>