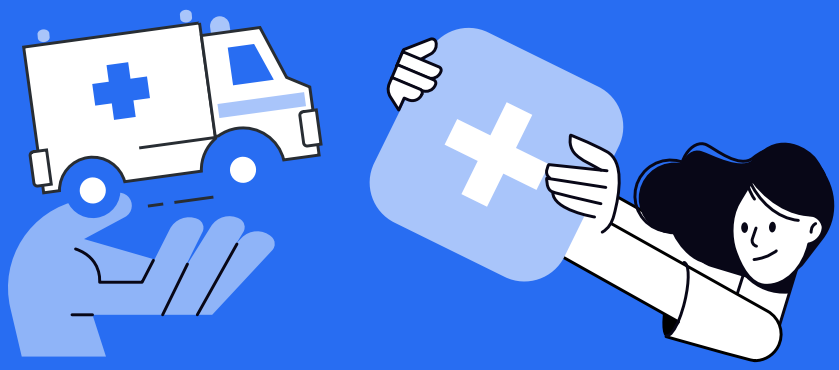
Nametag



HEALTHCARE IDENTITY · 2026

What Unverified Identity Costs Healthcare Every Year

A breakdown of the operational, financial, and security costs healthcare organizations pay every year for trusting that the person behind the account is who they claim to be.

$7.8M
annual cost of the identity gap

$150K
realized exposure, every week

2%
license cost vs. manual TCO

Modeled on a 15,000-employee healthcare organization

getnametag.com

EXECUTIVE SUMMARY

The cost of trusting a credential

Healthcare has led every industry in breach cost for 14 consecutive years. The widening is not because healthcare invests too little in security. The tools built to protect it were built for a different threat. They were designed to keep attackers away from credentials, not to verify who is using them once they are in.

The cost of not verifying who is behind every credential shows up in four places at once. Clinical hours lost to identity friction — the dominant cost in healthcare, and the only one measured in patient care rather than dollars. Breach loss from helpdesk social engineering and credential theft. IT labor absorbed by identity-related tickets at $70+ per reset. And a newer category: AI-assisted hiring fraud and state-sponsored candidates entering the workforce with credentialed access before anyone notices.

The McKesson breach in August 2026, where attackers called employees, impersonated IT teams, and used the resulting access to steal an estimated 284 million patient data records, is the most recent illustration of how this plays out in practice. No sophisticated exploit. No zero-day. A phone call that nobody verified.

For a 15,000-employee healthcare organization, those four costs amount to $7.8M annually — roughly $150,000 per week. Four days of undetected access cost McKesson an estimated 284 million patient records. At $150,000 per week, the math on delay is unambiguous. A single verified human layer at the helpdesk, at hire, and before privileged actions closes all four cost categories. The enterprise IDV license lands at approximately 2% of the manual TCO it replaces.

What follows is the math behind each of those costs, the patient-care impact, and what changes when those costs are closed. If you want to skip ahead, the closing section explains how to get a model built against your own numbers.

SECTION 01 · THE GAP

The most targeted industry in the world is defended by credentials no one verifies.

Healthcare has held the top position in breach cost rankings for 14 consecutive years. The average cost of a healthcare data breach reached $7.42M in 2025, more than double the cross-industry average. In 2024 alone, more than 275 million patient records were exposed, the largest volume in U.S. history.

But healthcare breaches are different in kind, not just in cost. A breach at a bank delays a transaction. A breach at a retailer leaks email addresses. A breach in healthcare delays surgeries, stops pharmacies from filling prescriptions, and forces hospitals to run on paper while patients wait for care. The cost shows up in dollars on a balance sheet. The damage shows up in the people who could not be treated.

The tools that were built to protect healthcare were built for a different threat. They were designed to keep attackers from getting credentials in the first place, not to verify the humans using them once they did.

Authentication proves which account is acting. Verification proves which human is acting.

- Healthcare has invested heavily in the former.
- Almost nothing protects the latter.

How breaches actually happen

The McKesson breach in August 2026 shows how quickly this plays out when the human behind the credential goes unverified. ShinyHunters, the group that claimed responsibility, told BleepingComputer they gained access by calling McKesson employees and impersonating internal helpdesk and IT teams. Those vishing calls led to the compromise of multiple employees' Okta single sign-on accounts. From there, the attackers accessed Salesforce and Snowflake environments and exfiltrated an estimated 1TB of data over four days before anyone noticed. The group claims the stolen data contains approximately 284 million patient-related records and demanded a $55M ransom.

No sophisticated exploit. No zero-day vulnerability. Someone called, impersonated a trusted colleague, and got a credential. The process for verifying who was on the other end of that call never existed.

CASE STUDY · AUGUST 2026

McKesson

284M	4 days	$55M
patient data records claimed stolen	of undetected exfiltration	ransom demanded

Source: BleepingComputer, August 28, 2026.

Entry point per ShinyHunters' claims. McKesson's investigation remains ongoing and has not independently confirmed initial access.

The Change Healthcare breach in 2024 followed a similar pattern. Stolen credentials on a Citrix portal with no MFA. Nine days of lateral movement before ransomware. For weeks afterward, pharmacies across the country could not process prescriptions, hospitals reverted to paper records, and providers went without reimbursement. Two of the largest healthcare incidents in recent history trace back to the same root cause.

SECTION 02 · WHY HEALTHCARE

Why healthcare is the highest-value target.

McKesson and Change Healthcare are not outliers. They are the predictable result of five forces that make healthcare uniquely attractive and uniquely vulnerable to attacks that start with a phone call or a stolen credential.

01 Irreplaceable data

Medical records command $260+ on dark markets, ten times the value of a credit card. A diagnosis cannot be cancelled and reissued.

02 Dispersed, 24/7 workforces

Tens of thousands of staff across dozens of sites and shifts make consistent identity verification nearly impossible under manual processes.

03 Clinical urgency as a security liability

When a helpdesk agent gets a call from someone claiming to be a locked-out nurse, the path of least resistance is to reset the account. Urgency is the social engineer's most reliable tool.

04 Privileged access concentrated in clinical credentials

EHR access, prescription authority, and controlled substance ordering all sit behind credentials that double as high-value targets.

05 A tightening regulatory environment

The HIPAA Security Rule is undergoing its first major overhaul since 2013, with MFA now mandatory and stricter rules arriving in H2 2026.

$7.42M	279 days	275M+	$260+
average healthcare breach cost	average dwell time	patient records exposed 2024–25	dark-market price per record
IBM 2025	IBM 2025	HHS OCR 2025	Intel 471

SECTION 03 · THE MATH

The identity gap has four cost pillars. They compound.

Those five forces translate into a specific annual cost. For a 15,000-employee healthcare organization, that cost is the sum of four separate categories running in parallel — each compounding the others, each adding to the weekly exposure rate.

These pillars are not equal. In healthcare, one dominates the others by a wide margin: the clinical hours lost to identity friction translate directly to patient care that does not happen. Every other pillar is a financial argument. The first pillar is a care argument.

PILLAR 01 · DOMINANT COST

Workforce productivity

$2.50M lost annually

Every hour the helpdesk spends on identity verification is an hour a clinician spends waiting. Identity friction costs 22,500 clinical hours annually — equivalent to 5,400 primary care visits that did not happen.

RECOVERED WITH IDV

$2.25M

plus 22,500 clinical hours returned to patient care

PILLAR 02

Annual loss expectancy

$2.60M

Breach probability multiplied by breach cost yields an expected annual loss of $2.60M with unverified identity at the helpdesk. Closing that vector and compressing the 279-day dwell time reduces it to $200K — a $2.40M risk reduction from a single control.

PILLAR 03

Operational efficiency

$1.25M

Identity-related tickets represent 20–50% of all service desk volume, at $70+ per password reset. Self-service recovery and pass/fail agent-assisted verification cut per-ticket cost by 86%, returning $1.08M in IT labor annually.

PILLAR 04

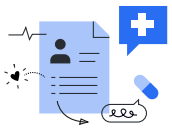
Hiring fraud exposure

$1.45M+

The first three pillars are ongoing operational costs. The fourth is newer. Remote hiring assumes the candidate who passed the interview is the person who shows up on Day 1; the FBI's NKIT advisory and a 220% YoY rise in AI-powered hiring fraud (CrowdStrike 2025) confirm that assumption is no longer safe. Fraudulent hires gain access to ePHI, prescription systems, and administrative infrastructure before the fraud is detected. OFAC sanctions liability sits on top and is not in the total.

SECTION 04 · THE WEEKLY RATE

The cost of doing nothing runs by the week.



Stacked together, the four pillars amount to $7.8M annually. The more useful number is the weekly rate. Every seven days without verified identity at the helpdesk, at hire, and before privileged actions, $150,000 of accumulated exposure converts to realized cost the moment a successful breach, a fraudulent hire, or a regulatory finding occurs.

EVERY SEVEN DAYS

$150,000 / week

What unverified identity costs a 15,000-employee healthcare organization while it stays unaddressed. Every week is a decision.

$7.8M
annual exposure, four pillars combined

The math runs the other direction once the gap closes. A single verified human layer resolves the helpdesk social engineering vector, the lateral movement risk, the hiring fraud exposure, and the HIPAA compliance exposure simultaneously. The enterprise IDV license for a 15,000-employee organization lands at roughly $600K annually — approximately 2% of the manual TCO it replaces.

STATUS QUO

Workforce productivity	**$2.50M**
Annual loss expectancy	**$2.60M**
Operational efficiency	**$1.25M**
Hiring fraud exposure	**$1.45M**
Total annual exposure	**$7.8M**

Baseline cost carried today, every year, with no control in place.

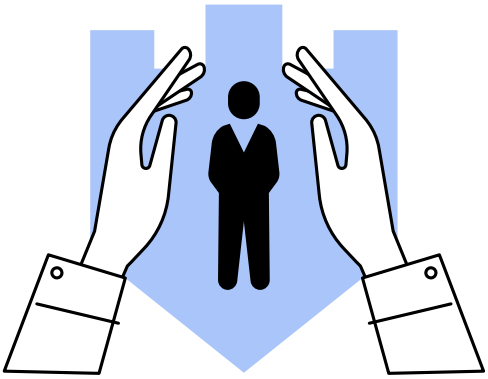
WITH VERIFIED IDENTITY

Workforce productivity	**$2.25M**
Annual loss expectancy	**$2.40M**
Operational efficiency	**$1.08M**
Hiring fraud exposure	**Closed**
Net recoverable value	**$5.7M+**

License cost ≈ 2% of the manual TCO it replaces

What changes when the gap closes.

The cost of doing nothing in healthcare is paid in the same currency the business runs on. Clinical hours that should be delivering care. Helpdesk capacity that grows with every new hire. Breach risk that compounds with every unverified recovery. Hiring pipelines that assume identity rather than verify it.



Addressing each of these returns them to the organization. Dwell time compresses from months to days. IT headcount stays flat as the workforce scales because self-service absorbs the volume that has historically grown with it. Each outcome is produced by the same control, deployed once.

CFO

- License cost at roughly 2% of the manual TCO it replaces.

CISO

- A 92% reduction in annual rate of occurrence.

CIO

- The helpdesk serving more people without adding staff.

This is not a credential problem. It is a human verification problem.

- Credentials prove what someone has.
- Verification proves who someone is.

Nametag

WHAT ARE YOUR NUMBERS?

The numbers in this ebook are illustrative. Yours will be different.

We will build the model against your headcount, your ticket volume, and your risk profile. No deck, no generic pitch — a working conversation.

Talk to the Nametag team →