Nametag · HEALTH CARE SECURITY CHECK-UP

6 questions to ask before you're the next disclosure.

In August 2026, McKesson lost an estimated 284 million patient records when unauthorized system access was granted to one unverified helpdesk caller. They now face a $55 million ransom demand. Use these questions to assess the likelihood that your organization will be next.

Healthcare has led every industry in breach cost for 14 consecutive years. For a 15,000-employee health system, unverified identity costs roughly $150,000 a week, even outside of the cost of a breach. At that rate, implementing a fix costs far less than waiting for a breach.

☐ Does your helpdesk verify the caller's identity, or just their answers?

Name, employee ID, and "security questions" are exactly what a social engineer prepares before they call. Bind every high-risk helpdesk request to a verified government ID and a liveness check. Every reset becomes a defensible decision, not a guess.

☐ Is a password or MFA reset bound to a verified human?

Account recoveries are often based on the agent's read of the situation, and social engineers know it. Make verification automatic and mandatory to remove agent judgment calls from the process.

☐ Does SSO login mean "verified," or just "authenticated"?

Okta confirmed an account was accessing McKesson's systems. It never verified which human was behind that account. Authentication proves which credential is acting. Verification proves which singular person is.

☐ Do you reverify before someone reaches Salesforce, Snowflake, or the EHR?

The breach didn't happen at login, it happened four steps later, when a verified-looking session reached the systems holding patient data. Add an identity verification checkpoint at the privileged-access boundary to stop lateral movement before it reaches the highest value systems.

☐ Would your team catch a lookalike domain before it's used against you?

McKesson claims looked legitimate enough to support a live social-engineering campaign. Employee security training reduces risk, but doesn't stop a convincing caller. Add verification that returns a clear pass or fail decision, rather than a score an agent has to interpret under pressure.

☐ Could you detect four days of exfiltration before day five?

~1TB left McKesson's environment over four days without tripping an alarm, because the session looked exactly like a verified employee's. Add identity verification at the session level to flag what credential-based detection misses.

The whole industry is falling sick to these attacks:

- **Medtronic** — ~3.8M individuals notified after an April 2026 breach of corporate IT systems (HIPAA Journal, BleepingComputer)
- **Baxter International** — ShinyHunters claimed 7.1M Salesforce records, including patient and employee PII (HIPAA Journal)
- **Boston Scientific** — Cyberattack disrupted global operations and order processing (BankInfoSecurity, HIPAA Journal)
- **Abbott Laboratories** — ShinyHunters claimed data from Abbott and its Exact Sciences business (HIPAA Journal)

Learn how healthcare organizations verify identity & prevent breaches *before they start.*

LEARN MORE TODAY

Sources: BleepingComputer (Aug 28, 2026); HIPAA Journal; HHS Office for Civil Rights; UnitedHealth Group; Nametag, "The Cost of Doing Nothing" (2026). McKesson's investigation is ongoing; attack-chain details reflect ShinyHunters' claims as reported by BleepingComputer. © 2026 Nametag Inc.