The HIPAA Compliance Automation Checklist

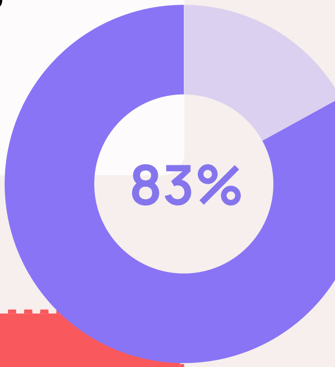
This checklist helps you assess automation solutions and your organization's readiness. Use it to operationalize HIPAA's requirements and transition from compliance in theory to compliance in practice.

Data Control & Deployment

- □ Can the system be deployed entirely inside your environment (on-premises, VPC, or private tenancy), without requiring outbound data transfer?
  - □ If not, can you trace how the data moves through external systems and where it's stored?
- □ Have you considered edge cases (e.g., how tracking pixels may interact with or expose your data)?
- □ Do you have a written data retention and secure deletion policy enforced at the system level?

In Barclays' 1H 2024 CIO survey, 83% of CIOs intended to "bring back" workloads to private clouds or on-prem infrastructure, the all-time high in the survey's history. Security and reducing "lock-in risk" were listed among the top drivers for repatriation.

Source



Case Study:

Kaiser Permanente

In 2024, Kaiser Permanente reported that web tracking pixels on its websites and apps had transmitted the personal information of 13.4 million members to third-party platforms such as Google. The data included names, IP addresses, and even health-related search terms.

Case Study:

HCA Healthcare

In 2023, HCA Healthcare said attackers accessed data from an external storage location managed by a vendor to format patient emails, leading to exposure impacting roughly 11M patients (names, contact info, appointment details). The compromised data set lived outside HCA's core systems.

The HIPAA Compliance Automation Checklist

Data Integrity

□ Is there a “human-in-the-loop” mechanism for exception handling?

□ Do you understand how the system monitors its own performance and how quickly it can generate malfunction alerts?

□ Can the system receive, transform, and share data reliably between all other connected systems?

A meta-analysis of 36 studies on workload reduction in medical image interpretation showed that human–AI collaboration ("human-in-the-loop") cut reading time by ~27%. Sensitivity (i.e., fewer false negatives) rose by ~12% while specificity remained stable, demonstrating efficiency gains without compromising accuracy.

Source

Human–AI collaboration

("human-in-the-loop")

cut reading time by

↓ 27%

sensitivity rose by

↑ 12%

Case Study:

U.S. Department of Veterans Affairs

In 2024, reports revealed that during 2022 and 2023 the VA’s new Oracle Cerner EHR, introduced under its modernization program, experienced multiple failures in transmitting prescription orders, allergy data, and scheduling information between modules and across “new” and “legacy” systems.

The HIPAA Compliance Automation Checklist

Audit Readiness

- □ Do your logs themselves contain PHI? If yes, how are they protected?
- □ If you use a third-party platform with “community” extensions installed, have you validated them against your compliance requirements?
- □ If an auditor requested a reconstruction of one patient’s data journey through your system, could you generate it completely and accurately?

Research shows that automated data lineage (the ability to trace data paths) in distributed data ecosystems enables real-time auditing and policy-based governance, improving compliance readiness at scale.

Source

Case Study:

Confidant Health

In 2024, an independent security researcher discovered a Confidant Health server on the open Internet exposing ~1.7M patient activity logs, including sensitive session data. No encryption or authentication was in place.

Case Study:

PrimedLogging

In 2020, engineer Prashanth (Andy) Menon developed and released PrimedLogging on the UiPath Marketplace to enhance the platform’s native logging features. However, UiPath disclaims all liability for community extensions and does not certify they meet the same security and privacy obligations as its core platform.

The HIPAA Compliance Automation Checklist

Human Factors

- □ Could a lack of technical expertise on your team result in gaps where PHI is exposed, mishandled, or undocumented?
- □ Do you have a clear method of tracking, authorizing, and revoking access privileges for employees and contractors?
- □ Do you have safeguards against "shadow workflows" that sit outside the official system and create compliance risks (e.g., using ChatGPT)?
- □ Is there a governance framework that makes compliance ownership and accountability explicit?

A 2025 report revealed 88% of organizations maintain active accounts for ex-employees and contractors, leaving these "ghost users" with access to sensitive systems and a gap for attackers to exploit.

Source

Case Study:

University of Vermont Medical Center

In 2020, a ransomware attack shut down UVM's EHR for nearly a month. Limited in-house cybersecurity expertise forced reliance on outside consultants, prolonging PHI exposure and driving recovery costs above $50M.

Case Study:

DeepSeek

In 2025, a misconfigured DeepSeek database was found to have leaked more than a million log records containing chats, secret keys, and system details, showing why strict security reviews of AI apps are essential.