Securing Healthcare Data in the Age of AI

skyflow | HEALTHCAREDIVE

Custom content for Skyflow by studioID

Executive Summary

For CTOs trying to balance innovation and compliance, enabling AI to drive real healthcare outcomes hinges on solving one of the industry's toughest challenges: securing data mobility without compromising privacy.

Artificial intelligence (AI) has become a critical driver of better healthcare outcomes. It accelerates diagnoses, personalizes treatment plans, and streamlines clinical workflows. AI also brings efficiencies to healthcare operations, from billing and claims to clinical trials and population health analysis. These improvements apply both to US-based processes and offshore activities. However, despite its potential, data privacy challenges often limit AI's impact. Strict regulations, fragmented data environments, and concerns about safeguarding patient information create barriers to accessing the high-quality data AI needs to deliver trustworthy results.

The central challenge for healthcare organizations is achieving data mobility: the ability to securely move and access data across systems to support care delivery, enable real-time clinical decisions, and accelerate research and innovation.

The solution lies in advanced data-protection technologies housed within data privacy vaults. These vaults secure sensitive patient data using polymorphic encryption, tokenization, masking, and redaction. Together, these techniques ensure personal information is concealed while still allowing authorized users to access the insights they need.

By securing sensitive data with a data privacy vault and enabling controlled access, healthcare organizations can unlock AI's full potential while maintaining patient trust and meeting strict privacy requirements.

The Case for Safe AI Usage in Healthcare

AI, which was revolutionary in the not-too-distant past, is now a mainstay in the healthcare industry.

Case in point: The Medscape & HIMSS AI Adoption by Health Systems Report 2024 found that most medical workplaces have used AI for at least 10 months. Last year marked the year of applying generative AI, whereas 2023 was for "discovery."

AI is used in healthcare to improve outcomes by enabling faster and more accurate diagnoses through the analysis of medical images, lab results, and patient data. It also helps personalize treatment plans by analyzing large datasets to predict how individuals might respond to specific therapies. Additionally, AI streamlines workflows—such as automating administrative tasks or predicting patient deterioration—freeing up clinicians to spend more time on direct patient care.

One of the most exciting uses for AI in healthcare is uncovering treatments for rare diseases. A recent *New York Times* article details how AI is speeding up drug repurposing so scientists in labs across the globe can find treatments faster using existing medicines.

One patient was battling a rare blood disorder called POEMS syndrome, and all options had been exhausted. In a Hail Mary move, the patient's girlfriend reached out to David Fajgenbaum, a Philadelphia doctor the couple had met previously at a rare-disease summit. In 2022, Fajgenbaum founded a nonprofit, Every Cure, to use machine learning to quickly compare thousands of drugs and diseases all at once.

The next morning, Fajgenbaum replied with a possible treatment, including a unique combination of chemotherapy, immunotherapy, and steroids previously untested to treat the syndrome.

Within a week, the patient was responding to treatment, and today is in remission.

Besides improving outcomes, AI is transforming healthcare businesses in many other ways.

AI for Healthcare Businesses

AI can harness and use data for a variety of business applications, including operational efficiency and cost management, billing and claims processing, population health analysis, clinical trials, and pharmaceuticals.

"Big data has been around for over a decade in the healthcare industry, but with AI, we can now consume that data, operationalize it, ask more comprehensive questions about the interrelationships of data, and get greater insights," said Skyflow's Chief Product Officer, Amruta Moktali.

For pharmaceutical companies that rely on clinical trials, AI has been a game changer.

Novartis, one of the world's largest pharmaceutical companies, uses AI to streamline some of the most time-consuming clinical trial processes: determining trial sites and principal investigators (PIs) to lead trials.

> "Big data has been around for over a decade in the healthcare industry, but with AI, we can now consume that data, operationalize it, ask more comprehensive questions about the interrelationships of data, and get greater insights."
>
> Amruta Moktali
> Chief Product Officer at Skyflow

GoodRx

The company's AI platform accesses a massive amount of data, from forty-six hundred thousand clinical trials, more than seven hundred thousand clinical sites, and details of six hundred thousand industry-wide PIs and millions of healthcare professionals. Additional data on patient diversity and de-identified patient lives, covering 1,100 diseases and indications, enables trials to be conducted with broad and diverse participation.

GoodRx, which offers a platform for medication savings in the US, is a good example of a company in the healthcare retail space using AI.

Its product-development team integrated AI into the GoodRx pricing platform to streamline its medication-pricing strategy.

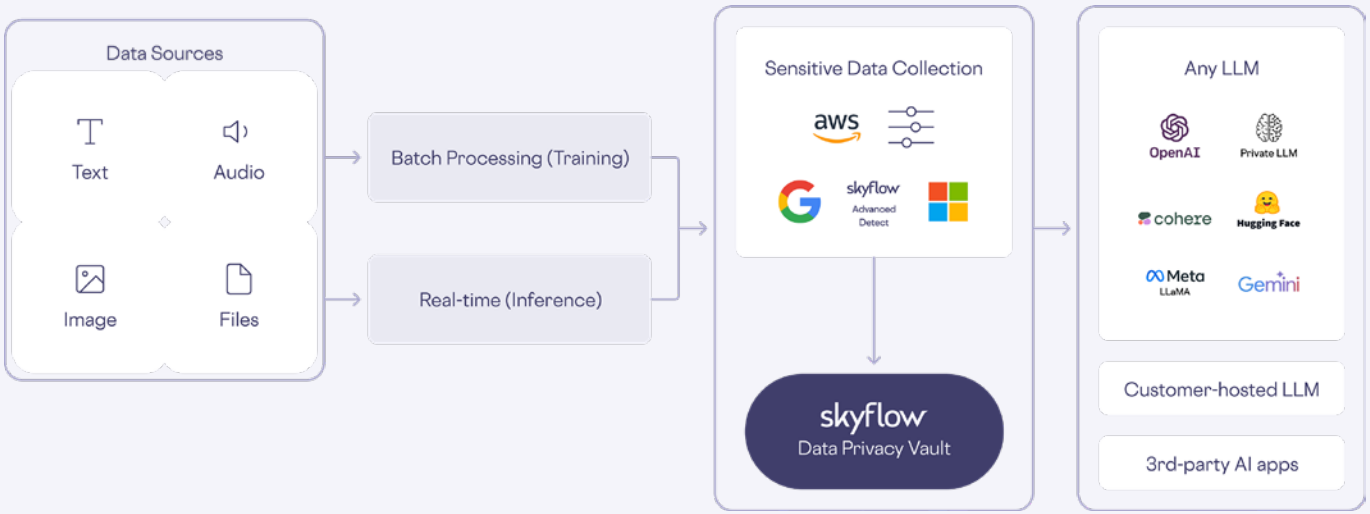
This allows GoodRx to deliver better pricing and product quality, which benefits consumers and pharmacies.

AI is a critical component for genomics companies that provide research, diagnostics, treatment development, and/or genetic testing for individuals.

AI helps identify data patterns to detect genetic variants and mutations faster than traditional methods. This speeds up everything from research to clinical decision-making.

AI also helps genomics companies tailor treatment strategies based on an individual's genetic profile.

Learn more about GoodRx's use case here.



skyflow

The Challenge

How to Keep Healthcare Data Private

Strict regulations, fragmented data systems, and the inability to fully safeguard patient data can make it difficult to access and share the high-quality information AI needs to deliver accurate, trustworthy results.

In the Medscape & HIMSS AI Adoption by Health Systems Report 2024 mentioned above, which found that 86 percent of respondents used AI, 72 percent shared that data privacy was a significant risk.

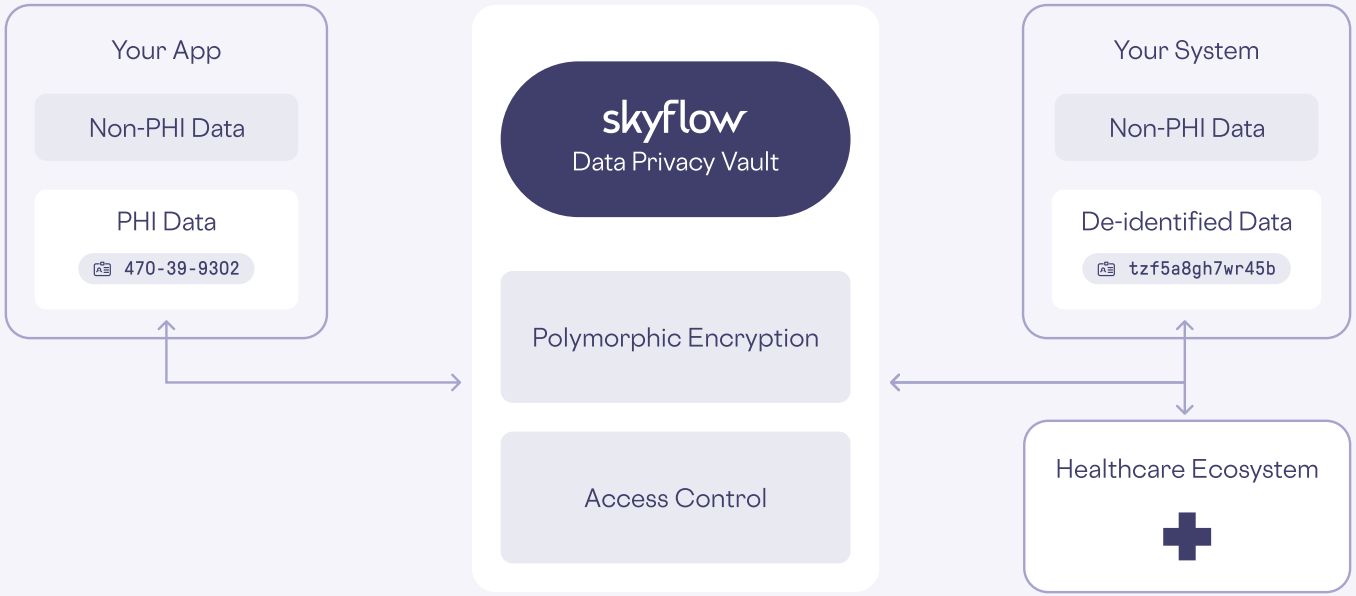
"Why do we take data privacy so seriously? Part of it is simply the law," said Riju Khetarpal, Riju Khetarpal, ex-Global Director, Healthcare & Life Sciences, Google. "Privacy laws were written long before AI or even computers, but they've evolved. Privacy is deeply rooted in the human psyche—people just feel better when they know their information is protected."

When considering data privacy, Khetarpal said, the financial services industry usually comes to mind, but healthcare has more impactful use cases.

> "Privacy laws were written long before AI or even computers, but they've evolved. Privacy is deeply rooted in the human psyche—people just feel better when they know their information is protected."
>
> Riju Khetarpal
> CEO of Metis Advisory, Inc.
> Former Global Director,
> Healthcare & Life Sciences, Google

“What do people care more about, health or money? Money is clear. Don’t steal it. healthcare is not something that’s stolen from you. But we spend more effort on privacy and security on financial services because it’s a direct asset. Healthcare is a reputational asset—people’s diseases and conditions—it’s our responsibility to keep these private,” Khetarpal said.

US and international healthcare laws govern the use of sensitive patient data, and organizations are required to follow strict rules for how they collect, use, store, share, and protect that information. Common examples of sensitive patient information include protected health information (PHI), such as medical diagnoses, prescriptions, and health insurance IDs, and personally identifiable information (PIIs), such as names, contact information, and Social Security numbers. Payment card information (PCI), such as credit card numbers and billing addresses, is another common type of sensitive information used by healthcare companies and is protected by the Payment Card Industry Data Security Standard.



AI and Data Privacy in Healthcare Offshoring

The US healthcare outsourcing industry is undergoing rapid expansion, with its market size projected to grow from $366.6 billion in 2025 to $662 billion by 2028, according to the latest report from Black Book Insights titled *The Rapid Expansion of Healthcare Outsourcing: Strategic Outlook 2025-2028*. Key areas driving this surge include revenue cycle management, medical billing, clinical documentation, and healthcare IT services, which are seeing compound annual growth rates between 6.2 percent and 15.3 percent. Many of these services use AI.

Yet when healthcare companies offshore activities, the data is subject to the same privacy laws. Even with the robust growth of the healthcare offshoring industry, data privacy challenges continue to hinder healthcare companies, as the data needs to be filtered and protected before it can be used.

"A leader at a Fortune 500 healthcare company shared with our team that his company had millions of dollars of operational efficiency just in offshoring claims processing. But they can't touch it because of data-security concerns," Khetarpal said.

> "A leader at a Fortune 500 healthcare company shared with our team that his company had millions of dollars of operational efficiency just in offshoring claims processing. But they can't touch it because of data-security concerns."
>
> Riju Khetarpal
> CEO of Metis Advisory, Inc.
> Former Global Director,
> Healthcare & Life Sciences, Google

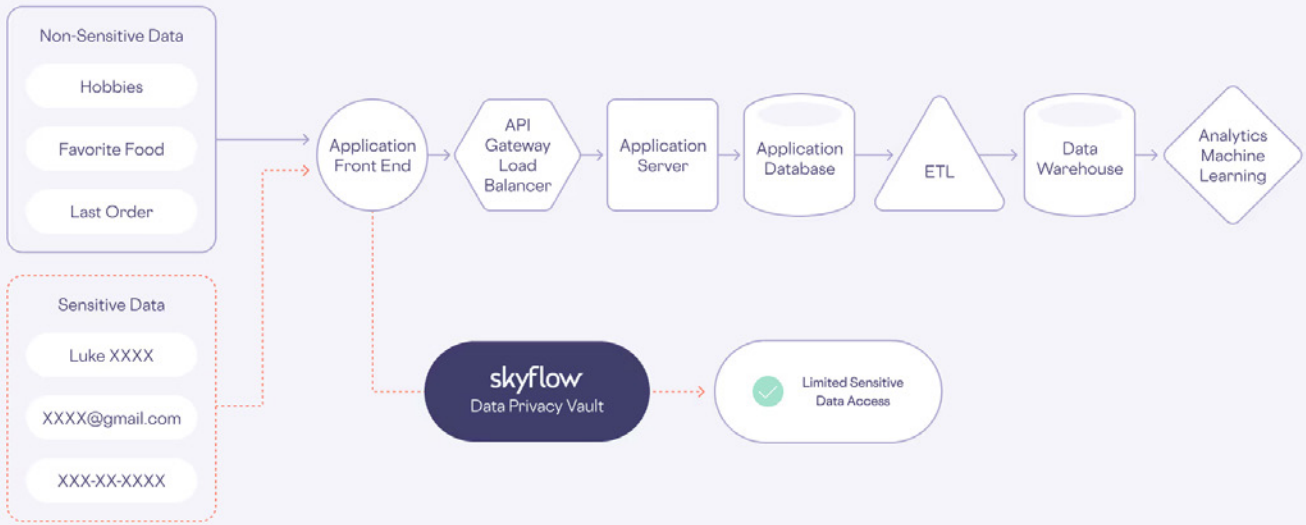
The Goal

Safe Data Mobility to Drive Better Healthcare Outcomes

"The ultimate goal for healthcare companies and organizations is to provide better healthcare outcomes for patients and providers. From an operational standpoint, this is unlocked with data mobility," Khetarpal said.

Data mobility is the ability to securely and efficiently move, access, and use data across different systems, applications, platforms, or geographic locations—whether on-premises, in the cloud, or across hybrid environments.

Data is often brought together from different sources, organized and analyzed by AI, then sent to various teams. To ensure safe data mobility, safe data-governance practices based on organizational rules for access must be applied to all PII or PHI.



The first step is to determine who requires access to specific information. Your physician must be able to view your name, date of birth, height, diagnoses, prescription details, and related medical information. The receptionist, however, should have access only to data necessary for administrative purposes, such as your health insurance identification and payment information. They should not have access to your medical diagnoses or other clinical data.

The data must also be stored in such a way that makes it useless in the event of a leak or a data hack, which at this point is a "when," not an "if." Why? According to the American Medical Association, sensitive healthcare data is up to fifty times more valuable than financial data on the black market.

In 2024 alone, several major healthcare organizations reported data breaches. Change Healthcare reported that 100 million individuals were affected, with a projected cost to the company of more than $2 billion. Kaiser Foundation Health Plan confirmed that 13.4 million individuals were affected, and the Centers for Medicare & Medicaid Services announced that over 3 million individuals were affected.

A 2024 IBM report found that the healthcare industry faced the most expensive data breaches, with average costs reaching $10.93 million, nearly double that of the financial industry, which averaged $5.9 million. On average, healthcare breaches went undetected for 213 days, higher than the cross-industry average of 194 days.

> "The ultimate goal for healthcare companies and organizations is to provide better healthcare outcomes for patients and providers. From an operational standpoint, this is unlocked with data mobility."
>
> Riju Khetarpal
> CEO of Metis Advisory, Inc.
> Former Global Director,
> Healthcare & Life Sciences, Google

The Solution

Technology to Protect Sensitive Data

“Historically, there has always been a divide between the people who want to use data and those who want to protect the data,” said Anshu Sharma, cofounder and CEO, Skyflow.

Technology now provides a bridge to close that divide.

Data privacy vaults hide personal details as needed for each user through the following processes:

- **Polymorphic encryption:** Allows data to be changed into a different encrypted form without needing to decrypt it first. The original meaning stays the same, and the data can still be unlocked by the intended recipient.
- **Tokenization:** Enables sensitive data to be replaced with a token—an alphanumeric value that holds no meaningful value and serves only as a placeholder for the original information. Sensitive data can be quickly retrieved by “detokenizing” it, and it provides an extra layer of security.
- **Masking/Redaction:** Permits sensitive data to be partially or fully hidden, depending on the context. Sensitive parts are either blacked out, masked, or replaced with placeholder text.

Once the data has been secured, the next challenge is determining how it should be managed.

The answer is to keep this sensitive data separate from the rest by securely centralizing it in a data privacy vault.

Key Features of a Data Privacy Vault:

- **Isolate:** Protecting sensitive data with a data privacy vault reduces the risk of it replicating across systems and services. This prevents "data sprawl," which increases compliance complexity and the potential for hacks. Isolating data ensures that only approved systems and users can interact with it directly.

- **Secure:** Sensitive data should be protected using both encryption and tokenization. Encryption secures the data inside the vault, while tokenization replaces real values with safe, nonsensitive placeholders. This approach helps prevent exposure and minimizes risk during day-to-day operations.

- **Tightly Control Access:** Access to sensitive data is restricted using zero-trust principles, along with role-based and attribute-based controls. These mechanisms ensure users and systems see only what they truly need. This reduces the chance of accidental exposure or misuse.

- **Data Residency Compliance:** A data vault can provide data residency without duplicating technology by serving as a secure, centralized repository that physically resides in the required geographic location. Instead of duplicating entire technology stacks across multiple regions, the data vault isolates and stores sensitive data locally while allowing global applications to access it in a controlled, compliant manner.

- **Governance:** Managing sensitive data means deciding what to protect, how to protect it, and how to share. By governing sensitive data across the entire data pipeline, sensitive data can be safely shared with analytics, AI, and third-party services.

- **Monitor:** Audit logging allows you to track exactly how sensitive data is accessed and used. You can see which users or systems accessed which fields and when. This visibility helps detect misuse and supports regulatory compliance.

- **Utility:** A strong data privacy vault lets you safely use sensitive data in approved workflows. You can analyze data without decrypting it, supporting functions such as identity verification or credit checks. You can also analyze de-identified data to drive insights while keeping PII, PHI, and PCI protected.

GoodRx: A Data Privacy Solution in Action

Learn how one healthcare provider solved its data privacy challenges.

Company Overview

GoodRx

GoodRx is the leading platform for medication savings in the US.

The company processes hundreds of millions of prescription claims containing sensitive patient information to help Americans access affordable healthcare.

With more than thirty million consumers and over one million healthcare professionals using GoodRx annually, GoodRx's data needs combine enormous scale with strict protection and security requirements.

Solution

skyflow

Using Skyflow to protect PII inside its platform, the GoodRx engineering team was able to focus on their mission and improve the GoodRx experience for their customers while simultaneously improving their privacy posture.

"We were able to successfully deploy Skyflow's zero-trust vault architecture in less than three weeks, and our total cost of ownership decreased by sixty-seven percent," said Nitin Shingate, CTO of GoodRx.

Transforming Privacy Challenges into AI Solutions

To fully realize the promise of AI in healthcare, CTOs must lead with strategies that prioritize both digital transformation and data management. With the right data privacy infrastructure, healthcare systems can move beyond privacy barriers and turn data into a powerful tool for innovation.

Call to Action

For more in-depth information about how Skyflow's technology works, see our white paper *Tracking New Trends in Data Privacy for Healthcare Providers and Healthtech*.

skyflow

About Skyflow

Skyflow is the security and privacy platform for the modern AI data stack built to radically simplify how companies isolate, protect, and govern their customers' most sensitive data. With its Data Privacy Vault, Skyflow enables businesses to store, process, and share sensitive data securely. Skyflow is backed by leading investors and is trusted by Fortune 500 and growth companies across financial services, healthcare, travel and hospitality, and retail.

Skyflow has headquarters in Palo Alto, California, and was founded in 2019. For more information, visit www.skyflow.com or follow Skyflow on LinkedIn and YouTube.

studio / ID BY INDUSTRY DIVE

studioID is Industry Dive's global content studio offering brands an ROI rich tool kit: Deep industry expertise, first-party audience insights, an editorial approach to brand storytelling, and targeted distribution capabilities. Our trusted in-house content marketers help brands power insights-fueled content programs that nurture prospects and customers from discovery through to purchase, connecting brand to demand.

Learn more