



Why Security Must Be on Every Evaluation Checklist for Employer Plan Sponsors

A Buyer's Guide for Organizations Evaluating Pharmacy or Medical Benefits Administration and Other Benefits Plan Partners

Table of Contents

02	Introduction: The Security and Tech Questions You May Not Be Asking
03	What Your Benefit Administrator's Security Posture Tells You
04	The Security-Related Credentials That Tell You a Vendor Is Serious
05	Why Whether Your Vendor Owns Its Platform Matters
06	What Security in Practice Looks Like
07	Don't Let Security and Technology Be the Last Things You Care About
07	Your Next Step

INTRODUCTION

The Security and Tech Questions You May Not Be Asking, But Should Be

When your organization evaluates a pharmacy benefit manager (PBM), medical benefit administrator, or any other specialty care or service provider, you're likely focused on cost, overall transparency, reporting, and member care, to name just a few obvious factors that weigh on the decision. Those are the right things to focus on; however, three questions are often asked last, if at all: how secure is this platform, where is the data stored, and who owns the infrastructure?

Those questions matter more than most buyers realize. Your PBM or medical benefit administrator sits at the center of some of the most sensitive data your members will ever generate, including diagnoses, prescriptions, claims history, and eligibility records. A breach doesn't just expose data. It triggers regulatory action, erodes member trust, and can cost millions to remediate. Whether your potential future partner developed and owns the platform or bought it matters, too.

This "guide" is written for technology, security, and benefits leaders involved in the due diligence that supports the request for proposal (RFP)/vendor evaluation process.

Throughout it, I'll share some of the experiences and insights gleaned from leading Judi Health™ through the process of achieving FedRAMP® Ready status, HITRUST certification, and a range of other security milestones. This perspective is grounded in practice, not theory, and that matters more now than ever before because last year alone, there were more than 750 breaches affecting more than 500 individuals, ranging from relatively smaller incidents impacting a couple of thousand people to the massive Change Healthcare compromise, which touched hundreds of millions of Americans¹ and crippled the system.

Read on to gain an appreciation for what security maturity looks like for a leading health benefits platform, what credentials to look for, and how to ask the right questions, before you sign your next partner contract.



Shane Garoutte
Chief Information Security
Officer, Judi Health

What Your Benefit Administrator's Security Posture Tells You

Most PBM and medical benefit administrator proposal requests – commonly referred to as RFPs – include security questions; however, they are treated as a formality.

In the average RFP, questions about platform and data security are generally not given sufficient weight or placed in the proper context. That's a problem because the answers to these questions reveal more about the fundamentals of how a vendor operates day-to-day than people realize.

A benefit administrator who handles your data responsibly will treat security as an organizational commitment, not a checklist item. The 'behavioral side' has to change. How you think about everyday activities and processes, and how you and your partners handle the plan's data, including member data, must be prioritized.

That behavioral commitment doesn't start with the security team. It starts at the top of your organization.

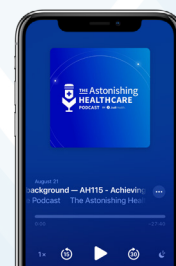


I really challenged the business when we first went down this road toward FedRAMP® Ready status. I said it can't be something that's driven by the security team. It has to be something that's driven by the executive team and the C-suite."



PODCAST EPISODE

Achieving FedRAMP® Ready Status & Why Security is a Team Sport



When security is a C-suite priority, it shows up in how data is handled across every team, from implementation to member services to account management. When it's treated as an IT problem, gaps appear exactly where you can't afford them.

And if an organization's security culture is built on fear rather than trust, it becomes actively dangerous. You don't want employees to fear retribution from the security team if someone approaches them with a risk or possible mistake. You could be actively circumventing your security program and making it less secure.

✓ Key takeaways:

- A vendor's security posture is a proxy for how seriously they take sensitive business data – including health plan members' data.
- If the C-suite drives security, it's going to be more durable than security owned by one team.
- A culture of accountability surfaces problems early; a culture of fear hides them until it's too late.

? Questions to ask:

- How is security responsibility distributed across your organization?
- Who owns security at the executive level?
- How does security-related accountability flow to the teams handling the client relationship and plan members' data?

The Security-Related Credentials That Tell You a Vendor Is Serious

How can an employer plan sponsor or benefits consultant read past the marketing “fluff” to find the proof?

Every benefits administrator and vendor will tell you they take security seriously. What separates meaningful assurance from marketing language is independent verification.

The technology-first versus healthcare-first distinction matters for security. A platform designed from the ground up will be built differently from a legacy system trying to catch up or an acquired platform.

Judi Health’s use of Judi® reflects that. The platform runs on a serverless, cloud-native model built on fully managed AWS services. With no “always-on” servers sitting exposed, there’s a dramatically smaller attack surface and reduced ransomware risk. Additionally, the environment is monitored continuously for unexpected behavior, malware, and vulnerabilities.

Here’s what to look for, and what each credential confirms.



I was impressed by how much thought had been put into Judi® as a stack when it was first architected, and how much Judi Health was really a technology company focused in the healthcare space, not a healthcare company that is trying to use technology as much as they can.”

Shane Garoutte

Credential

What it confirms

FedRAMP® Ready	Cloud-native platform continuously verified against federal security requirements. Very few healthcare administrators hold this.
SOC 2 Type 2	Security and privacy controls operated effectively across an extended review period, not just a single audit point.
SOC 1 Type 2	Financial operational controls are effective over time.
HITRUST	The recognized independent benchmark for HIPAA compliance. No official HIPAA certification exists; HITRUST is the real signal.
NIST 800–53	The rigorous federal control framework underpinning FedRAMP, FISMA, and other high-stakes programs.



A note on FedRAMP® specifically: it’s a cloud-only status for CSPs, or Cloud Service Providers. It is not a one-time or annual certification in which someone assesses the vendor and then returns months later. It is continuous and constant.

Continuous monitoring means the platform’s controls are verified as it evolves, not just at the moment of a snapshot audit. That’s the level of assurance your data, and your members’ data, deserve.

✓ Key takeaways:

- Credentials only mean something when they’re independently verified and continuously maintained.
- SOC 2 Type 2 and HITRUST are the floor; FedRAMP® Ready status signals a higher level of maturity.
- A technology-first architecture, serverless, cloud-native, and built on NIST 800–53, is meaningfully more secure than a legacy platform.

? Questions to ask:

- Are your SOC reports Type 2?
- What framework underpins your certifications?
- Do you hold FedRAMP® Ready status?
- How is continuous monitoring maintained between audit cycles?

Why Whether Your Vendor Owns Its Platform Matters

Platform ownership is not just a technical distinction; it determines how quickly a vendor can adapt, improve, and respond when plan sponsors need something. It may also determine where your data is stored, which could be much farther away than anyone would expect.

In a market where some PBMs have accelerated their business strategies by acquiring other companies' platforms and capabilities, Judi Health's organic, ground-up approach stands apart. The architecture, roadmap, and release schedule are all controlled within a single connected environment.

With a partner who developed their tech stack organically, you get “future-proof” infrastructure that provides:



Greater flexibility for plan design.

A vendor that owns its platform can configure benefits, networks, accumulators, reporting, and workflows with fewer constraints, helping plan sponsors adapt as business needs, regulations, and member populations change.



Faster innovation and responsiveness.

When the product roadmap and release schedule are internal, enhancements do not depend on a third-party vendor's priorities, timelines, or willingness to make changes.



Added security and compliance.

Platform ownership gives the vendor direct accountability for how data is protected, monitored, updated, and governed across the technology stack.



Less operational risk.

Vendors that rely on rented, acquired, or stitched-together technology may introduce more handoffs, data gaps, integration delays, and upgrade dependencies, all of which can create friction for plan sponsors and pose risks to members. Plan data could also be stored offshore, which introduces another level of risk.



Key takeaways:

- Platform ownership affects far more than technology – it shapes a vendor's ability to adapt, innovate, secure data, and support plan sponsor needs over time.
- Vendors that invest in and build their own infrastructure can respond more quickly to plan sponsors' needs and market events because their roadmap, release schedule, and architecture are under their control.
- Rented, acquired, or stitched-together technology can introduce operational friction through more handoffs, integration gaps, upgrade dependencies, and possible data risk.



Questions to ask:

- Do you own and control the core technology platform used to administer our plan, or do you rely on acquired, licensed, or third-party systems?
- What parts of your roadmap, release schedule, configuration process, or reporting capabilities depend on external technology partners?
- If we chose you, where would our plan data and our plan members' data be stored, and will any of it reside outside the U.S.?
- How long does the average custom request or configuration take to complete, and why?

What Security in Practice Looks Like

| We're connecting compliance credentials to real-world protection for health plan members.

Credentials confirm that a platform was built securely. But the vendor evaluation should also probe how the vendor manages security day to day, and how that affects everything from your implementation to the ongoing relationship.

Most organizations are not choosing between a perfectly secure private data center and a cloud provider. They are choosing between their own security budget and the security capabilities of AWS, Azure, or GCP, which generally operate at a scale and maturity far beyond what most private enterprises can compete with.

In reality, the threat environment is constantly evolving:

There's no other space in the engineering field where you have a continual adversary trying to work against you. You don't even have a face or a name for the adversary. Their tactics change constantly, and they are becoming increasingly sophisticated,² with agentic AI shifting the threat landscape in ways that demand defenses as adaptive as the offense. A platform grounded in continuous, real-time monitoring is far better positioned than one relying on annual assessments and static controls. **This translates to concrete considerations:**



Data in transit and at rest:

Confirm that member data is encrypted at every stage, not just in storage.



Access controls:

Ask how the vendor applies the principle of least privilege: who can reach member data, under what conditions, and with what verification.



Incident response:

A well-run security program has a defined, tested response plan. Ask to see it. Ask how quickly they'd notify you of a breach and what that process looks like.



Vendor chain:

Your administrator may use sub-processors or third-party point solutions. Each one is a potential risk surface. Ask how third-party security is evaluated and monitored.



Integration security:

A unified platform that processes medical and pharmacy data on a single system with one data layer carries less risk than a patchwork of vendors exchanging data across multiple handoff points.



Key takeaways:

- Real-time monitoring and a minimized attack surface distinguish modern platforms from legacy systems.
- Your evaluation should probe incident response, access controls, and third-party vendor security.
- A unified, single-platform architecture carries meaningfully lower risk than fragmented multi-vendor setups.



Questions to ask:

- How do you monitor for threats between audit cycles?
- What does your breach notification process look like?
- How do you evaluate the security of your sub-processors and integration partners?

Don't Let Security and Technology Be the Last Things You Care About

Choosing the right benefits administration or care coordination partner is a high-stakes decision.

The administrator or care provider you choose to help manage your pharmacy, medical, vision, dental, or ancillary benefits plan, or coordinate care for your plan members, will hold some of your and your members' most sensitive information. They will also process claims that affect members' care and integrate with your existing systems. Done poorly, those connections can expose you to risk; done correctly, they can improve the member experience and overall outcomes.

The organizations that get this right are the ones that put security and technology on the evaluation checklist from the start, not as a cursory due diligence item, but as a filter applied from the first conversation.

Judi Health was built with that filter in mind. The platform was architected as a technology-first system, verified continuously, and backed by a security culture that runs from the C-suite to every team that touches member data. That's the healthcare infrastructure of the future, and security you don't have to second-guess.

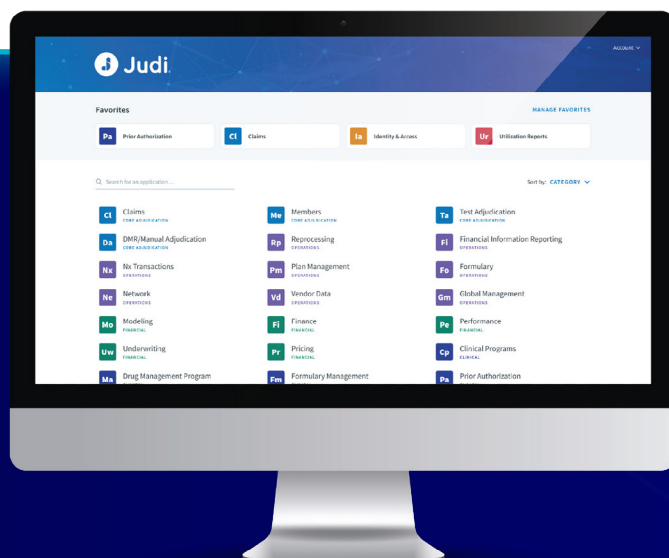
Your Next Step

If you're evaluating a pharmacy or medical benefit administrator and want to understand how Judi Health approaches security, compliance, and seamless implementation, connect with the team for a technical conversation. Bring your hardest questions. That's exactly the kind of due diligence this platform was built to support.

Want To Learn More?

Contact the Judi Health team today to learn about our transparent, financially aligned approach to pharmacy benefit management.

Contact Us Today



Follow Us On LinkedIn & Subscribe to Our Newsletter.



References

1. U.S. Department of Health and Human Services Office for Civil Rights. [Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information](#). Accessed September 16, 2026.
2. Verizon Business. [2026 Data Breach Investigations Report \(DBIR\)](#). Accessed September 16, 2026.