Pillar Technology
PARTNERS

What mid-market leaders need to know:

SaaS Security

in the Age of AI

Executive Insight

SaaS platforms now drive critical business functions— from HR and billing to analytics and collaboration. With AI deeply integrated, they deliver powerful efficiencies but also create new, often hidden, security risks.

AI-driven automation can accelerate workflows, improve insights, and reduce human error. But it can also silently change how sensitive data is stored, accessed, and even shared. And when those tools are handling personal health information (PHI), customer financials, or business-critical IP, the stakes are too high to ignore.

This guide helps mid-sized organizations—especially in healthcare—reclaim visibility and control in a rapidly evolving SaaS landscape.

IS YOUR CURRENT SaaS ENVIRONMENT CREATING MORE RISK THAN VALUE?

Use this quick self-assessment to find out:

1 Do any of your SaaS vendors use embedded AI or machine learning?

2 Do you know where your sensitive data (PHI, PII, IP) lives across SaaS platforms?

3 Have you reviewed SaaS contracts or data policies in the last 12 months?

4 Are SaaS user permissions regularly audited and managed?

5 Do you have visibility into how vendors are using or training AI with your data?

How many questions can you answer?

0–2 "Yes" : High exposure, low visibility. Prioritize a SaaS audit now.

3–4 "Yes" : Moderate control—but potential blind spots. Take corrective steps.

5 "Yes" : You're ahead of the curve. Stay vigilant.

SaaS VENDOR RISK QUESTIONNAIRE

Use this AI Security checklist when onboarding or reassessing a vendor:

- Does the vendor embed AI or integrate third-party AI tools?
- What types of data are used to train or feed AI features?
- Is sensitive data (PHI/PII) used in AI training? If so, can you opt out?
- What data retention policies apply to AI-generated outputs?
- Where is data stored and processed (geolocation, cloud region)?
- What contractual safeguards exist for data misuse or breach?

Include this as part of every procurement or vendor review process.

SECURITY CHECKLIST for AI-Era SaaS

Ensure compliance with HIPAA, or CCPA where applicable (GDPR)

Access & Permissions

□ Use least-privilege access models

□ Enforce SSO and MFA across all apps

□ Automate offboarding to remove stale accounts

Data Handling

□ Identify all SaaS platforms with PHI or sensitive data

□ Ensure encryption at rest and in transit

□ Limit data sharing to only essential integrations

Monitoring & Response

□ Establish alerts for unusual user or AI behavior

□ Audit admin activity and access logs regularly

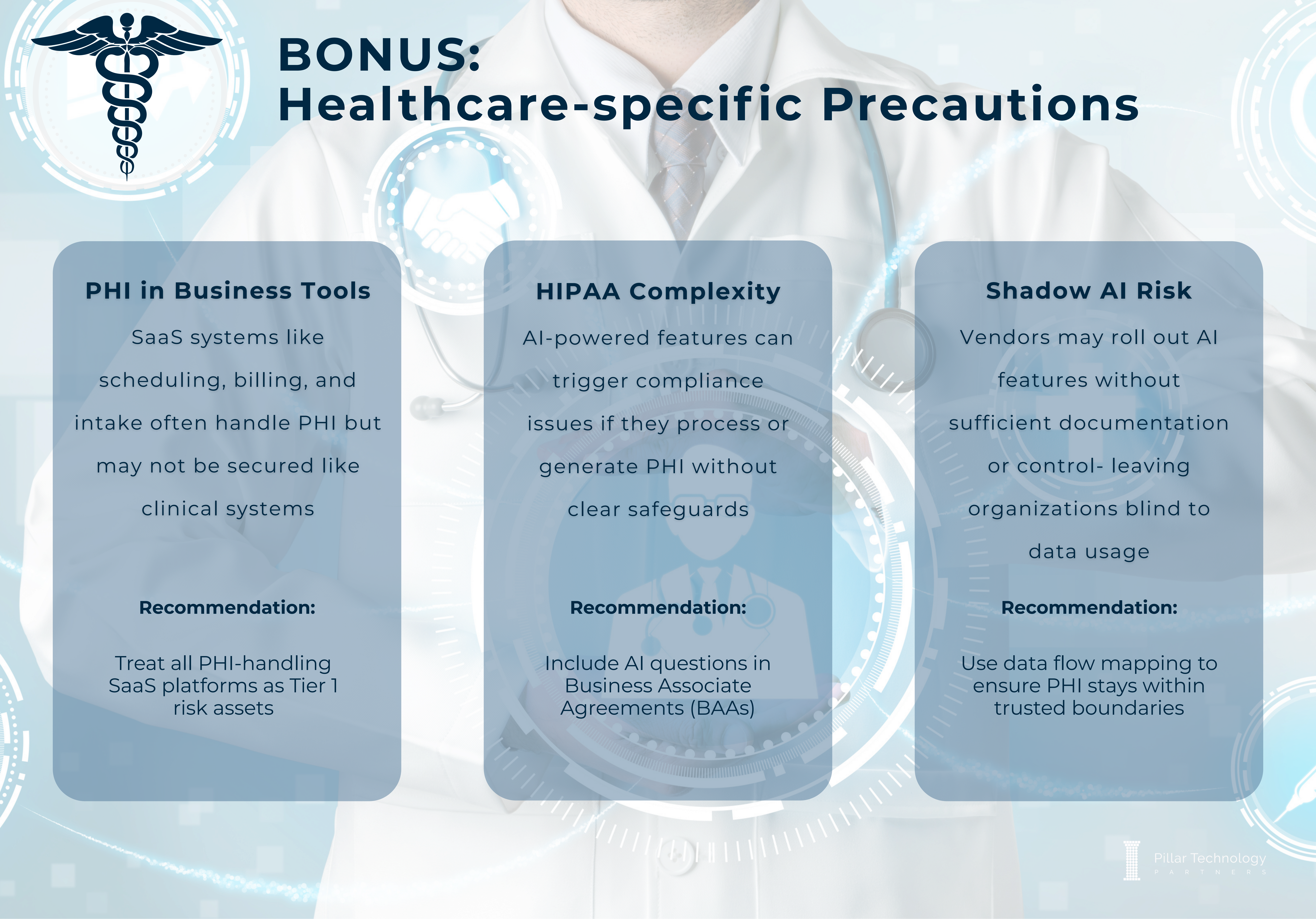
□ Test incident response procedures involving SaaS platforms

Vendor Controls

□ Review contracts for AI and data handling clauses

□ Require breach notification terms specific to AI misuse

□ Ensure opt-out rights for AI training



BONUS: Healthcare-specific Precautions

PHI in Business Tools

SaaS systems like scheduling, billing, and intake often handle PHI but may not be secured like clinical systems

Recommendation:

Treat all PHI-handling SaaS platforms as Tier 1 risk assets

HIPAA Complexity

AI-powered features can trigger compliance issues if they process or generate PHI without clear safeguards

Recommendation:

Include AI questions in Business Associate Agreements (BAAs)

Shadow AI Risk

Vendors may roll out AI features without sufficient documentation or control- leaving organizations blind to data usage

Recommendation:

Use data flow mapping to ensure PHI stays within trusted boundaries

This could easily happen...

Illustrative Situation:

A mid-sized healthcare provider in the southeastern US uses multiple SaaS tools to manage electronic health records (EHR), appointment scheduling, and patient communications.

Incident:

A new AI feature is automatically enabled in their scheduling SaaS platform allowing anonymized usage data to be shared for “model training.” Due to lack of visibility and vendor oversight, the system ends up exposing protected health information (PHI) through metadata logs stored on a third-party server.

Potential Impact:

- Patient Record exposure for an extended period of time.
- The organization is required to notify patients and report the incident under HIPAA breach rules.
- Regulatory fines, reputational damage, and need to re-evaluate all SaaS contracts for AI usage.

Lesson Learned from this scenario:

Even “invisible” features like background AI training or integration logs can lead to compliance violations. Proper vendor assessments, opt-out controls, and real-time monitoring are critical.

Pillar Technology
PARTNERS

Pillar Insights

Explore more insights and resources for security leaders:

Cybersecurity Risks of AI

Actionable roadmap empowering CISOs to assess, prioritize, and accelerate cybersecurity maturity through strategic alignment, governance, and risk-informed decisions.

> AI Risks

Unexpected Emergency

Learn more how we work hand-in-hand with organizations large and small to resolve complex incidents and protect critical data.

> Incident Response

Complete Security Program

Gain insight how we offer a customized cybersecurity program tailored to give control over risk, protect sensitive data, and fortify defenses. How we provide what you need, when you need it.

> Managed Security

Security Leadership & Coaching

Security programs can be overwhelming. Even the most effective leaders benefit having a trusted coach who sharpens strategy, challenges blind spots, and offers a different perspective. Find more information how we help security leaders lead with confidence.

> Leadership & Coaching

Why clients choose Pillar

Precision over excess

Healthcare-ready solutions

Cybersecurity is our only focus

We don’t just defend systems.

We defend futures.

Contact Us

At Pillar, we help mid-market and healthcare organizations simplify security, sharpen focus, and reduce risk—without adding noise or complexity.

☎ 678-304-9099

✉ info@ptechcyber.com

🌐 www.ptechcyber.com

YOUR TRUSTED PARTNER IN MID-MARKET AND HEALTHCARE CYBERSECURITY

Pillar Technology
PARTNERS