zip | Ambience

Cybersecurity and Healthcare in 2024: Assessing 3rd Party Vendors

A Healthcare provider's guide to navigating the cybersecurity risks associated with 3rd Party Vendors, to ensure that your organization, and the patients you serve are protected against cyber threat.

Contents

2 Why this Guide Exists
3 Scope of this Guide
4 Technical Controls to Prioritize
7 Practices + Operational Controls to Prioritize
10 Assessing a Potential Vendor: A Checklist
12 Conclusion
13 About the Authors

Why this Guide Exists

> "The healthcare system is a complex web of organizations and technologies. The last year has shown us the importance of building resilience into this web, but it remains difficult. We're thrilled to team up with our friends at Ambience Healthcare to equip healthcare organizations with the right strategies to overcome this challenge"
>
> **Josh Zweig**
> CEO, Zip Security

The healthcare landscape is a complex web of organizations and technologies.

For the past decade, much of the conversation around cybersecurity for Healthcare Providers (HCPs) and their vendor partners has centered around data privacy regulations. HIPAA, BAAs, and other data privacy requirements have driven the direction of compliance, and therefore the cybersecurity story in the industry. While these continue to be critical priorities, the cyberattacks on HCPs in 2023 call into focus a different priority: ensuring access to care and availability of systems in the face of cyber attacks.

2023 was a record year for cyberattacks that impacted access to care. For instance, a chain of New York City providers experienced multiple breaches during 2023, requiring them to take their networks offline at 2 hospitals and a nursing home, meaning patient records could not be accessed for over 24 hours. Ambulances were diverted and patients rerouted to other facilities, resulting in delayed access to care.

The availability of systems and data in order to provide care for patients must be a top priority in technology management and cybersecurity. In crafting a cyber defense strategy, HCPs need to invest in preventing

attacks and protecting data, but must equally invest and plan for the instance where a critical process or system is compromised, and have a contingency plan in place for how they can continue to provide patient care, and ensure availability of systems and data.

It's also important to remember the methods and tools for delivering care are evolving too. We are seeing the benefit in both quality and efficiency of delivering care through the utilization of third-party technologies - particularly in the space of Generative AI, and how this can improve physician's workflows. These applications and technologies are contributing to the general increase of hosted services by vendors. While their impact and benefit are overall very positive, they do pose an additional consideration in the cybersecurity conversation.

As the threats and opportunities have changed, we need to ask the question: How can HCPs be proactive in integrating vendors + partners into their own security practices to fulfill their obligations to their patients in 2024? This guide seeks to answer that question.

Scope of this Guide

Producing an effective security strategy in the healthcare space is complex. Maintaining confidentiality, integrity and availability of patient data and systems is a high priority task for all organizations in 2024.

When establishing a security strategy an organization must consider both what their security objectives are, how they are best able to achieve them, and how their vendors' play a role in their security strategy. Positively, there has been exciting growth in the security space of providers and tools that can help healthcare organizations and their vendors achieve their security objectives.

This whitepaper offers an overview of the key considerations for cybersecurity strategy in healthcare, and provides tactical resources to

support organizations in asking the right questions when selecting health tech vendors as partners.

What are the Technical Controls to Look for in your Vendors?

When integrating a new partner it is important to assess their approach to structuring your security strategy, and understand at a high level if the controls and levers that they intend to implement align with best practices. Understanding at a high level if these practices are being deployed correctly is a good indicator for how a vendor approaches the full spectrum of security:

Understand Which Systems Are Mission Critical to Offer Care, Build Redundancy, and Offer Availability Guarantees

For every piece of technology you buy, assess if it is a critical component of providing care. If it is, ensure that technical controls for resiliency of that technology are in place. This means that in the case of breach or disruption, the critical process or information of that system can be diverted to a functioning alternative pathway, and the critical component can still be accessed. Let's take a look at some use-cases and best practices:

1. In the case of on-premise device issues (such as malware), having decoupled backup systems that can be deployed is a key practice to prevent disruption to operations and normal practices.
2. In the case of EHR compromise, the ability to spin up separate instances from backups quickly is key in ensuring minimal disruption to access of records.
3. In the instance of password breaches, an organization having a plan of action for validating identity through 2 additional factors of authentication and processes like disaster recovery phone trees, will allow users to still use their credentials to access systems.

Establish Technical Controls to Effectively Mitigate and Manage Cyber Risks

Effective cybersecurity strategy is both an offensive and defensive game. A vendor should demonstrate they've taken into consideration both what controls should be set up, and then how to manage those controls most effectively.

Firstly, it is important to set up controls and best practices to ensure users and devices are secure and protected. Establishing controls that (1) ensure vendors comply with existing MFA and password requirements, for example through requiring federated SSO integration, and (2) ensures devices are enrolled in software that enables device management (things like conditional access, remote wiping/locking of a device, and version control), means IT/Security teams are best equipped to monitor, and manage users and devices across their organization.

Secondly, it is important to be able to identify if any of these controls are not effectively deployed and ensure, in the case of an incident, an appropriate response time. Establishing controls that enable a device to be locked and wiped if stolen, being able to take action for non-compliant devices (by prompting or forcing enrollment, updates, encryption etc), are all factors a vendor should have mechanisms in place for.

Establish Separate Networks and Systems for Business related activities (Corporate) and Patient related activities (Production)

Understanding a potential vendor's approach to establishing networks within your organization is a helpful indicator of their views on core security principles when working in the healthcare sector and with PHI.

It is highly recommended to separate out the networks that are responsible for housing different data and activities within your organization. Having these separations requires different login credentials for each, and also allows the appropriate level of controls to be implemented. The more confidential the data being housed, the more extensive the controls (e.g. introducing MFA, SecureKeys and other such controls).

For instance, an organization can have Google accounts (gmail, drive) with every employee and have login credentials. If there was a data breach, and login credentials were compromised, the impact of this would be unnecessarily greater, if those same credentials were used to access the database of patient data. By having separate networks, with credentials only issued to those that require access, the risk of a breach is both decentralized, and the impact reduced.

Ensure Patient Data (PHI) is Only Accessible to those that Strictly Need it (Least Privilege)

At the cornerstone of efficient security practices is ensuring that employees only have access to the data and information that directly relates to their own work. This is done by establishing access controls and a robust separation of PHI.

By having a clear list of *who* should access certain types of data, and then implementing steps to ensure *only those authorized people can access this data*, we are setting up 'access controls' that help PHI be managed safely. This ensures confidentiality by preventing unauthorized access, and preserves data integrity by reducing the risk of unauthorized changes to the data sources.

For instance, a maintenance worker within a hospital should never be able to access patient records, but may need login credentials to the system to log things like tickets and review an incident log. Access controls

creates a user profile that allows an employee to see only the information they need, and blocks all other accesses. Health systems should require vendors to maintain access control lists of all subcontracted personnel who have access to sensitive data.

What are the Security Practices & Operational Controls to look for in a Vendor?

Technical controls (as spoken about above) are the essential building blocks for an effective security strategy. In this next section, we discuss the operational principles that a vendor should abide by to deploy and manage these controls and practices most efficiently and effectively.
In order to effectively implement a cybersecurity program, security needs to be a priority across the organization, a shared responsibility between your organization and your vendors.

Invest in Building a Culture of Security Consciousness Across the Entire Organization

A good vendor should be able to demonstrate to health system security leaders and administrations they have built a culture of security across their entire vendor organization. They should demonstrate how they plan to engage and educate the vendor organization on security matters, and demonstrate their understanding that security consciousness should be built across the entire organization, and not just within the IT/security function of the organization.
Considering the following criteria when assessing a vendor relationship will help answer this:

- Are the security operators siloed, or deeply integrated into the company's technology? The most effective security operators have experience with on-the-ground development that enables them to work closely with engineering and product teams

- Are the vendor's sales teams close to the security team? Vendors that put security first are able to put technical personnel on calls and effectively address health system concerns directly.
- Is the vendor's security team able to effectively align with your needs? The best vendors articulate their security posture simply and clearly to identify alignment with health system requirements. Security-minded organizations are eager to communicate their posture.
- Is security a demonstrated priority across the entire vendor organization? Vendors should be able to demonstrate their investment in educating and building buy-in from leaders across the organization. When asked they should have a clear articulation of how they run regular tabletop exercises, adhere to compliance requirements, and make information (such FAQs) readily available will empower employees to actively participate in keeping an organization secure

Demonstrate Respect for the Confidentiality of your Organization's Information and What Controls Should Remain In House

Partnering with a good vendor can significantly lighten the burden on an organization to navigate the complexities of an effective security strategy. Good security should be easy to understand, and a vendor should have a clear surface area that fits well into the existing surface area of your organization.

The right vendor can bring expertise, capacity (for things like 24/7 monitoring), and tools that make your organization more secure, fast, and more efficient. That being said, there is a balance of what should be outsourced and what should remain in-house. Key controls you should look for:

- Authorization and how it integrates the health system's existing structure. For example, a good vendor should always integrate with

your identity provider, and not create undue burden to manage access controls and identity in any secondary systems.
- Authentication and how access controls are managed. For instance, only the organization itself can accurately map the details of roles and responsibilities to the data accesses they need. Outsourcing this to a vendor increases the risk of inaccurate mapping and minimizes the efficacy of the access controls all together.
- Ensuring the integrity and accuracy of health system data integration is paramount. A reliable vendor prioritizes the seamless integration of data within your software ecosystem, minimizing errors and maintaining data integrity.
- Effective event logging is essential for security monitoring. A trustworthy vendor ensures the integrity and observability of logs, providing sufficient scope for analyzing and responding to security incidents.

Outsource the activities that are not unique, and verify that your vendor has taken responsibility for the portions of the security program that are not unique to them.

Navigates a Complex and Dynamic Environment in an Effective Way

Having robust controls and policies in place are the fundamental building blocks for an effective security strategy. However, it cannot stop there. Both the environment (who your employees are and the job they are doing, their devices, and their ways of work), and the nature of risks (think evolutions in how cyber attacks happen), are dynamic. Therefore, in order for controls in place to be effective, it is essential that your security strategy, and the providers you're working with, have factored that into consideration.

- A good vendor will help develop standardized processes to ensure the lifecycle of software and devices are secured in an automated

manner, meaning you don't have to rely on humans to remember to off-board an employee correctly. Having clearly articulated MDM policies with dedicated IT and security staff to enforce is a key part of this.

- A good vendor should have a fully in-house development team that can be held accountable to the full software surface area management. This demonstrates attention to detail and reduces turnaround time for vulnerability resolution.
- It's also essential to have regular reviews of access controls to ensure they remain up to date and efficient. If an employee's role and subsequent access requirements change, it's imperative that access controls are updated systematically to reflect this.
- Finally, official compliance frameworks in place that include third party auditing, such as SOC2. This verifies third-party audits of compliance standards are being regularly and reliably completed.

Validating and Assessing a Potential Vendor

Vendor Security Assessment Checklist

Now we've laid out the fundamentals in terms of how responsible vendors should operate and the types of controls they should be deploying. The below checklist offers a consolidated list of the key questions it is important to discuss with any potential vendor partnership.

Technical Controls

What technical controls do you plan to deploy?

- ☐ Clear awareness of controls across major security areas, including: identity protection, device management, and EDR.

Do you establish separate networks for production and corporate activities?

- ☐ Demonstrated plan for separating production and corporate environment.

How do you manage access controls to PHI?

- ☐ Demonstrated understanding of the importance of access controls, and clear mechanisms for implementing systems that allow for robust controls on systems containing PHI.

Best Practices

How do you plan to engage and educate our organization and employees on security matters? (*What types of training exercises and tabletop exercises would you run? How would you engage with leaders of non-security functions (clinical and business side)*?

- ☐ Robust training, communication & engagement plan for employees. Clear plan for how to build security champions across the organization (not just within the security function).

What activities will be outsourced to you, and which will remain for us to manage in-house?

- ☐ Demonstrating respect for the information/activities that should remain in-house. Processes like application audits, access reviews, and mappings should be in-house. More common processes like deploying, configuring, and managing EDR can be outsourced.

How do you maintain and manage the security strategy over time? (*How do you ensure the lifecycle of software and devices are secured? How do you propose maintaining accurate access controls?)*

- ☐ Demonstrated plan for systematic reviews and updates of controls, and automation of processes as a result of change (e.g. off-boardings).

Way of Working Together

How do you plan to engage our security team in case of an incident?

- ☐ Provision of a clear plan of action, and historical examples, of roles and responsibilities between vendor and organization, which demonstrates proactive and timely engagement in the event of an incident.

What are your change controls processes?

- ☐ Demonstrated robust access controls mechanisms for process changes, such as multi party authentication for making any critical changes to systems, and tiering for change types aligning to different change control processes.

What certifications and compliance frameworks do you adhere to?

- ☐ Adherence to HIPAA, HITRUST, willing to sign a BAA, or any other standard HIPAA protocols your organization adheres to.

Conclusion

The past few years have brought about a shift in priorities and considerations for healthcare system security assessments. Alongside traditional concerns about data privacy and compliance with regulations like HIPAA, the emphasis has increasingly turned towards ensuring the availability of systems and uninterrupted access to care in the face of cyber threats.

To adapt to these new challenges, health care providers (HCPs) need to build out their security assessment criteria to incorporate new considerations. Particularly when partnering with vendors, HCPs need to understand how they can remain operational in the case of a cyber incident with a vendor. This means HCPs should have a clear understanding of the course of action that enables them to resume normal operations if the vendor is offline, as well as the reassurance the vendor has implemented sufficient security measures to reduce the likelihood of incident in the first place.

In evaluating vendors, it's crucial to cut through rubber-stamp certifications and identify high-performing security teams. Smart evaluation methods involve assessing technical controls, operational practices, and the overall security culture within the vendor organization. Look for vendors who prioritize building a culture of security consciousness across their entire organization, respect the confidentiality of sensitive information, and demonstrate the ability to navigate the complex and dynamic cybersecurity landscape effectively.

By incorporating these net new criteria and adopting smart evaluation strategies, healthcare providers can enhance their cybersecurity posture,

safeguard patient data, and ensure uninterrupted access to care in an increasingly digitized healthcare environment.

To chat with us directly about your requirements, reach out today.

To learn more, visit ambiencehealthcare.com & zipsec.com.

About Zip Security:

Zip Security is an venture-backed cybersecurity start up with the mission to make security accessible to all. Zip integrates best-in-class security tools into a single user-friendly platform, empowering businesses to navigate the evolving cybersecurity landscape with confidence.

About Ambience Healthcare:

The mission of Ambience Healthcare is to supercharge clinicians with breakthrough generative AI technology. Leading health systems and provider organizations across North America partner with Ambience Healthcare to reduce clinician burnout, improve system efficiency, and enable high quality care. Founded in 2020 by Mike Ng and Nikhil Buduma, Ambience is headquartered in San Francisco, California, and has raised $100M in total funding from Kleiner Perkins, OpenAI Startup Fund, Andreessen Horowitz, Optum Ventures, Human Capital, Martin Ventures, AIX Ventures, AirTree Ventures, John Doerr, Jeff Dean, Richard Socher, Pieter Abbeel, Anne Wojcicki, Eren Bali, Jay Desai, Nish Bhat, Matt Mochary, and others.