Security is Table Stakes for Healthcare Start-ups

A Roadmap and Business Case for Security, Privacy, and Compliance for Healthcare Start-ups

Bottom Line Up Front

For many healthcare IT startups, the complexities of security, privacy and compliance present a blind spot that can be difficult to address. Resources are tight and the stakes are high. Regulatory mandates and customer requirements can be a barrier to client acquisition and present significant risk. The organization is tasked with not only having to prove their product solves an important problem, but also demonstrate to prospects that buying the product or services will not pose a security threat to their organization.

In this whitepaper we will present a security, privacy, and compliance roadmap for the healthcare IT startup to consider throughout the early stages of the organization's lifecycle. We will also discuss some strategies for arming your sales teams with the information and tools they need to remove doubt in the mind of prospective healthcare customers.

Contents

Let's Get Started

.

Shane Peden, Director of CISO Advisory
CISSP | CISA | HITRUST CCSFP
https://www.linkedin.com/in/speden/
404.519.8877

Background

Why This Matters

The healthcare start-up has made a commitment to their investors, employees, and customers to rapidly acquire market share and grow the company. The barriers to success in the healthcare sector are high. Your product must solve an important problem and you must be able to instill the confidence that using your (relatively unknown) product does not present a security and compliance risk to an organization. If you can do these two things, your business is likely to thrive.

The Roadmap to Success

In this whitepaper, we will propose information risk management strategies appropriate for each of the phases in a typical startup's lifecycle. Each strategy is based on personnel, time, and cash resource constraints we have experienced with our client base. By adopting these recommendations you can poise yourself to successfully win with new clients, spend less time and money on compliance, and rapidly scale your program as your product gains traction in the marketplace.

These lifecycle phases are as follows:

1. Minimum Viable Product (MVP) development and pre-revenue,
2. Initial rounds of funding and onboarding your first customers,
3. Gaining market traction and entering high growth mode.

Let's discuss each stage in some detail.

Stage One: MVP Development

In the early stages of a start-up's lifecycle the focus should be on building and architecting a product that ***clients want***. The bottom line is that even if you build the most secure platform on the planet, but clients do not want it, you will not grow a successful company.

The early stages of product development are foundational for future scalability. You certainly do not want to have to rebuild a half-baked product once a few customers are onboarded.

To avoid this, it is vital to consider future regulatory and customer requirements and make the best effort to architect the solution to account for these requirements. If you do not build a minimally secure and compliant product, you will have major problems onboarding any healthcare clients.

Here are the first things you should consider:

Focus on Product First

Risk3sixty is a security and compliance firm. We think security and compliance are among the most important things that any company can do. However, it must be reiterated that at this stage that you should focus on product-market fit. Focus on building a product that solves a huge problem.

If you have a great product, keep reading!

Identify Relevant Regulatory and Industry Requirements

As you are building your product, you should take time to consider which regulatory and industry requirements you will be beholden to. It is important to consider this up front because it will impact how you architect your product, what vendors you select to integrate with your product (e.g., HIPAA compliant partners), what data you may collect, and how your product will interface with prospective customers.

As a healthcare IT startup, you will likely encounter Protected Health Information (PHI) and Personally Identifiable Information (PII). You may be processing financial information or credit card information. You may collect or sell user data.

In each of those circumstances, common compliance requirements (HIPAA, PCI DSS, GDPR, CCPA, SOC 2, HITRUST) will be barriers to onboarding your first clients. If you understand what you may be up against, you can begin designing a future-proof and scalable system.

Make Smart (i.e. Compliant) Technology Architecture Choices

Are you going to build your system in the cloud? Which cloud and why? What technology partners will you work with to make engineering easier and faster?

Before making investments in what will comprise the technical foundation of your solution, ensure the infrastructure and third-party solutions you choose to build on meet all your compliance needs. This will save you from loss of time, cash, and sales opportunities in the future.

For example, most large cloud and SaaS providers (with a few notable exceptions) offer HIPAA-compliant solutions that your company can leverage to ensure compliance. The big three cloud infrastructure providers (Azure, AWS, GCP) offer compliance-conscious solutions that are also developer-friendly and allow for rapid solution development. These three should nearly always be in strong consideration.

To the best of your ability, ensure all downstream providers (source code repos, orchestration tools, data processors) and infrastructure providers meet as many of your future compliance needs as possible. This will likely mean purchasing the "HIPAA-Compliant" version of their product.

Having solid partners will allow you to stand on their maturity as the foundation of your story to prospective clients before you have your own to tell.

Prioritize These Security Requirements

With limited time, resources, and cash you will not be able to implement every security measure at once. As a result, you will need to prioritize the implementation of specific security and privacy requirements based on your industry and regulatory requirements.

If you are wondering where to start, here is a list of requirements you should focus on immediately:

Technical Security Requirements

- Encrypt all sensitive data at-rest and in-transit in any places where sensitive information may reside or be transmitted.
- Implement anti-malware scanning and monitoring technologies on all endpoints accessing production infrastructure.
- Enable system event and network event logging in the production environment and retain this information for at least six years.
- Implement network monitoring and/or agent-based anti-malware detection on servers within the production environment.
- Implement physical and logical access controls to limit access to sensitive information and systems controlling access to sensitive information. This includes network and user access controls.

Change Management and SDLC

- Segregate production and test environments as soon as possible.
- Avoid use of production data in testing as soon as possible.

Privacy Requirements

- Develop privacy notice and consent policies and make them available to the end users of the system.

HIPAA Specific Requirements

- Ensure you enter into a Business Associates Agreement with all third parties downstream who you might exchange PHI with.
- Develop a basic incident response and HIPAA breach notification process and be prepared to speak to it during due diligence with customers.
- Determine if you will need to obtain informed consent from patients as part of providing your services (not common, but important to determine early on).
- Ensure you are retaining all patient-related transactions and PHI for six years.

Stage Two: Venture Funding and Onboarding of Early Customers

Once the solution finds its place in the market, it will graduate from an MVP to a production solution with customers relying on it to do business.

Spending money on dedicated security, privacy, and compliance resources is difficult in this stage as growth sucks cash and every extra dime needs to go into R&D and sales. Every decision on spending needs to be tactical at this phase in the lifecycle.

Communicating your Security, Privacy, and Compliance Story to Prospective Clients

As you onboard more customers, they will begin asking very pointed questions about your security, privacy, and compliance program. This will manifest as an influx of due diligence questionnaires, requests for security certifications, and even on-site audits of your company.

The Vendor Transparency Report

At this point, a valuable tool you should consider to get ahead of these type of requirements is a "vendor transparency report". The vendor transparency report can be a valuable tool to share how your company manages security, privacy, and compliance. This may include links to security features your product offers, relevant policies, and even a pre-filled security questionnaire your client can reference.

A thoughtfully developed vendor transparency report can meet the following objectives:

- Arming the sales team and getting them on the same page,
- Creating clear and accurate communication of the organization's current security and privacy posture,
- Creating a temporary stop gap between having appropriate certifications (e.g. SOC 2, HITRUST) in place and having nothing at all.

Continue to Mature the Security Program

As you begin to gain traction in the marketplace, your organization will be expected to undergo independent audits and security reviews. This will likely manifest within customer contractual requirements or in due diligence questionnaires.

To prepare for the more formal audits, you will want to continue maturing your processes to meet these new and more stringent requirements.

Below is the next stage of technical and regulatory requirements your organization should consider in order to ensure you're poised for success.

Technical Security Requirements

- Develop an Information Security Policy that reflects reality**.** Do not over commit in your policies. Auditors audit against policies (especially the HHS Office for Civil Rights).
- Implement data backups and disaster recovery controls (e.g. failover or redundant infrastructure).
- Implement multi-factor authentication on systems and networks where sensitive data resides.
- Perform external and internal vulnerability scanning and integrate with the security patching protocol.
- Implement a media re-use and disposal policy and process and ensure it includes secure disposal of PHI.

Change Management and SDLC

- Develop change management and SDLC (secure development lifecycle) policies and procedures.
- Formalize change management and the SDLC for both practical reasons and to meet customer expectations and compliance requirements.
- Implement processes to tightly manage access authorization, provisioning and deprovisioning for both systems and people.
- Implement a security patching management protocol.

Privacy Requirements

- Begin mapping all internal and external data disclosures (e.g. data flow diagrams).
- Implement a process or method to allow patients/users of the system to authenticate themselves and obtain access to their private data.
- Implement a process or method to allow users to correct or update their private data that originated within your organization.
- Implement a process for handing data subject requests to delete their data.

HIPAA-Specific Requirements

- Consider identifying general or outside counsel with familiarity of HIPAA that can perform Business Associates Agreement (BAA) and service agreement reviews.
- Consider development of your own BAA with the assistance of general or outside counsel.
- Mature the incident response and HIPAA breach notification policies and procedures.
- Document the notification requirements defined in all customer BAAs and make sure your incident response and HIPAA breach notification processes can satisfy these.
- Formally assign security and HIPAA compliance responsibility within the organization.

Stage Three: Market Traction and Preparing for Scale

As you gain traction in the marketplace or begin to move into the enterprise space, clients will expect a comprehensive approach to security and compliance.

At this stage you will need to consider budget and resources for security partners, additional fulltime personnel, and toolsets.

During this transition period your organization may not have the know-how or budget to hire a full-time employee to manage these initiatives. In fact, due to the marketplace shortage for security and compliance professionals, there may not be any qualified candidates available who can single-handedly meet all your defined requirements.

Still, there is an undeniable need for someone to own the information risk management function within the organization. So, what should you do?

Maturing Your Program at Scale

Eventually the organization must outgrow a reactive approach and transition from compliance *"check-the-box"* exercises to strategic information risk management.

Here is the process risk3sixty has taken with many organizations:

Step 1: Identify an Appropriate Risk Management Framework

There is no shortage of potential frameworks for an organization to choose. In most cases, you will choose the framework that is most relevant to your organization based on the products and services you provide. As a starting point, we recommend considering ISO 27001, CIS CSC (a.k.a. CIS Top 20), and the NIST Cyber Security framework.

Each of these frameworks are well regarded and provide standards, guidelines, and best practices for implementing a world class information risk management program. Some benefits to be gained from adopting one over the other are as follows:

- Each of these frameworks can be mapped back to multiple regulatory requirements such as HIPAA (unified compliance approach).
- NIST CSF is preferred by government agencies and widely recognized by healthcare organizations in the USA. The OCR has issued a formal crosswalk/mapping between HIPAA and the NIST CSF, giving it additional validity in the healthcare industry.
- ISO 27001 is universally recognized as a leading industry standard and maps clearly to the NIST CSF. ISO 27001 is also the basis for HITRUST, a gold-standard certification for healthcare security.
- ISO has developed a series of complimentary standards to ISO 27001 that allow you to easily expand your program to other areas such as GDPR (27701), cloud security (27017), cloud privacy (27018), and risk management (27005).
- ISO 27001 is a certifiable standard, meaning an organization can obtain formal third-party certification.

Step 2: Perform a Current State Assessment Against the Framework of Choice

Once you have chosen a framework that best fits your organization, we perform a "current state assessment". The current state assessment is leveraged to measure your current maturity versus desired maturity. The gaps in the current state of operations are identified and a maturity roadmap is developed.

The maturity roadmap includes what will be done, who will do it, how it will be done, when it will be done, and the costs of implementation. This "strategic plan" gives top-level leadership everything they need to know about the future and progress of the security program.

The remediation roadmap also provides a vital benchmark to measure progress of your security program journey (Am I making progress against the roadmap, as planned?).

Step 3: Establish an Information Risk Council

Once your organization understands its current state and where it wants to go, it is vital that top-level leadership is bought into and has visibility into the security program.

To govern the security program and *ensure that program activities support the business' objectives,* we recommend establishing an information risk council.

The information risk council is a cross-functional group of company leadership that meets regularly to review risks and progress. Leaders are very busy, so meetings are designed to be efficient, impactful, and pointed. The information risk council drives strategy, measures progress, and hold individuals accountable.

Organizations typically formalize this in a charter and define roles and responsibilities in an Information Security and Privacy Management System and Policy.

Step 4: Develop and Mature Policies and Procedures

The information risk council typically oversees the development of a series of policies and procedures. The risk management framework chosen will drive policy and procedure content, as each requirement defined by the framework must result in a policy statement.

Do not treat policies as a formality. Policies are the written articulation of management's intent. They are essential for scalability, to formalize your expectations, and to limit the company's legal liability. Take them seriously!

Step 5: Develop Recurring Activities

Your information risk management program will require the operation of multiple controls and processes. Almost nothing is a one-time event, it must be "operationalized". Owners must be identified, and the elements of the program must be formalized and implemented.

Common recurring activities include:

- Information and third-party risk assessments
- Risk council planning and oversight meetings
- Security, privacy, and HIPAA training
- Logical and physical access reviews
- Incident response and handling process reviews and tabletops
- Technical continuity testing and tabletops
- Annual HIPAA risk assessments
- Penetration tests and vulnerability scans
- External audits

Step 6: Obtain Proof of Compliance

The final step is to obtain proof of compliance. Compliance can be demonstrated through internal efforts alone, but the majority of customers in the healthcare market are going to insist on formal certifications which may include SOC 2 Type 2, PCI DSS Level 1 certification, ISO 27001 certification, and HITUST certification.

The objective should be to develop an information risk management program that allows you to manage certifications with as much ease as possible. This is sometimes referred to as "test once, report many".

Cost vs. Benefit: Questions to Ask

If you are still on the fence about where to take your security program, ask yourself:

1. Does the risk of non-compliance exceed to cost of building a program? (e.g., regulatory, reputation, or contractual)
2. Does my current security and compliance posture hinder sales and growth? Is the loss of sales greater than the cost of a compliance program?
3. Am I on a timeline to meet these compliance requirements? Does building the program fast enough require external help?

If the answer is "yes" to these questions, then it might be time to consider building a security program and potentially seeking a partner to help.

Let's Get Started

Our vCISO Program:

If you are ready to get started and would like a guide, risk3sixty can help! Through our virtual CISO program we have:

- 100% certification and compliance success
- 100% three-year client retention
- 100% of clients are references

We also typically implement programs at 50% the cost of building programs internally

Speak with a Professional

Shane Peden, Director of CISO Advisory
CISSP | CISA | MCSE | GPEN
PCI ASV | HITRUST CCSFP
https://www.linkedin.com/in/speden/
404.519.8877

About the Author

Shane Peden is the Director of Information Security, Cyber Risk, and CISO Advisory Services. Shane focuses on assisting information technology firms with developing and implementing cyber security and privacy programs.

Shane's specialty is bridging the gap between the technical subject matter expert and organization leadership through effective communication of information risk within the business's context.