MedStack's Guide to:

Vendor Security Assessments

Everything you need to navigate the complicated world of VSAs.

MEDSTACK®

Table of Contents

MedStack's Guide to Vendor Security Assessments

Chapter One:

The Basics

MEDSTACK®

1.1

Introduction

Breaking into the digital health landscape can be challenging, even for vendors that have experience dealing with protected health information (PHI) or meeting HIPAA compliance requirements.

Unfortunately, many healthcare enterprises have experienced breaches in data due to third-party application leaks.

This has changed the vetting process of healthcare enterprises when onboarding digital health vendors, making it far more complex and thorough in recent years.

To avoid unnecessary risks to data integrity, third-party digital health solution vendors looking to partner with large healthcare enterprises are now asked to complete vendor security assessments before entering into any formal agreements.

But what are vendor security assessments, and why are they so critically important? Understanding how VSAs work, as well as finding ways to complete them quickly and efficiently, are vital for your success as a vendor within the healthcare industry.

What are VSAs?

Vendor security assessments, also known as 'third party risk assessments', 'security questionnaires', or simply VSAs, are a list of questions that are created by healthcare service organizations, typically by IT or Security Leads.

VSAs are seen by new vendors aiming to be integrated into existing systems of potential clients as a necessary burden of proof of their ability to protect patient data. They are sent in order to evaluate the privacy and security measures that the vendor currently has in place.

VSAs can be very extensive, often including hundreds of questions. This helps the enterprise get a well-rounded, holistic view of their vendors' current ecosystems, as well as their best practices.

Often, many of the questions found in these assessments are similar, but they tend to be worded uniquely based on the enterprise using them.

While this unique wording is standard practice, it can become very time consuming for the executives of vendors that need to fill out multiple VSAs.

1.2

Why are VSAs important?

At their core, VSAs are an effective method for streamlining the collection process for information that's necessary for large enterprises to ensure their protected health information remains secure.

They also help guarantee that all third-party vendors partnering with the enterprise have strong network security, and that they're meeting all the process requirements for auditing and compliance.

Proving HIPAA Compliance & Other Requirements

There are a number of security and privacy compliance requirements that you could be asked to verify in addition to HIPAA. Some of these may include:

- General Data Protection Regulation (GDPR)
- Payment Card Industry (PCI) Data Security Standards
- ISO 27001
- NIST
- Other Data Security Standards (DSS)

By guaranteeing ahead of time that HIPAA compliance requirements, as well as any other necessary compliance frameworks are being met, enterprises protect themselves from partnering with vendors that will increase their risk of confidential data breaches.

Adding Value for Startups

In addition to helping protect enterprises from potential data risks through third party vendors, VSAs hold value for startups.

If you're a startup that's only just begun working within your industry, or you're just starting to approach larger enterprise clients with your services, VSAs allow you to hone your own in-house resources for future applications.

It's vital as a vendor that you be able to provide accurate, concise information when requested by a potential customer, and VSAs allow you to create streamlined answers that can be converted for use in future applications.

Going through the VSA process also allows you to make sure that all the different parts of your business are working within your industry-specific regulations.

Understanding where there may be gaps in your own processes and compliance practices allows you to address them quickly, before they begin costing you the opportunity to partner with, sell to, and onboard healthcare enterprise clients.

Protected Health Information for Healthcare Enterprises

Of course, the most valuable aspects of a VSA relate to ensuring that protected health information remains protected, even after new third party vendors are able to access this confidential information.

It also puts processes into place to establish things like how the vendor will respond in the event of a potential data leak, or how their service will remain active in the event of an outage.

These protections give healthcare enterprises the peace of mind to be able to bring third party vendors into their secure networks and utilize their apps and services, without having to worry about putting valuable, secure information at risk.

MedStack's Guide to Vendor Security Assessments

Chapter Two:

Navigating the Process

MEDSTACK®

2.1

Introduction

Now that you know a bit about the basics of vendor security assessments, you're ready to begin preparing yourself for the submission process.

However, this is no small task.

VSAs can be long, time-consuming questionnaires to fill out. If you've never completed a VSA before, the process can be quite daunting.

What should you do to prepare?

What questions are they going to ask?

How can you show large healthcare enterprises that your organization is a safe, reliable vendor?

This chapter will walk you through more information about the process for approaching VSAs from healthcare enterprises.

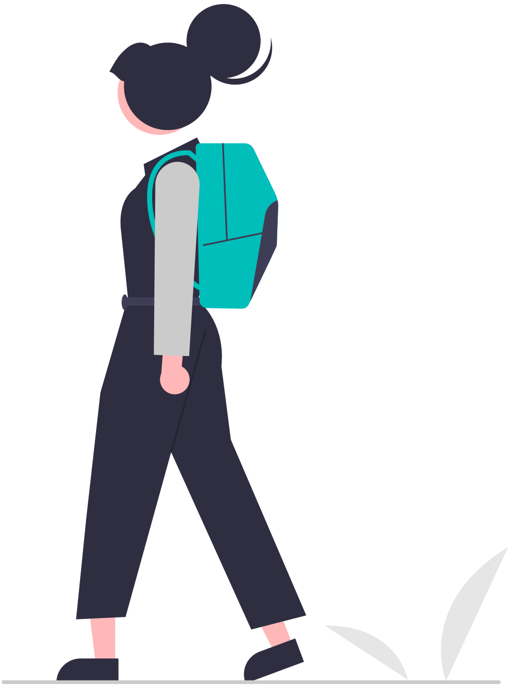
First Step After Recieving a VSA

Congratulations on receiving a VSA!

You should be excited if one of your potential clients has sent your business a VSA to fill out and submit.

Clients will only send a VSA to you if they're seriously considering doing business with you. This means you've already crossed the first hurdle, and the enterprise is interested in partnering with you.

Before you dive into the process of filling out the VSA, take a moment to congratulate yourself. You're on your way to securing a new customer.



2.2

How Often are Vendors Assessed?

Most vendors will receive a VSA to complete before a new enterprise client will consider them for a partnership.

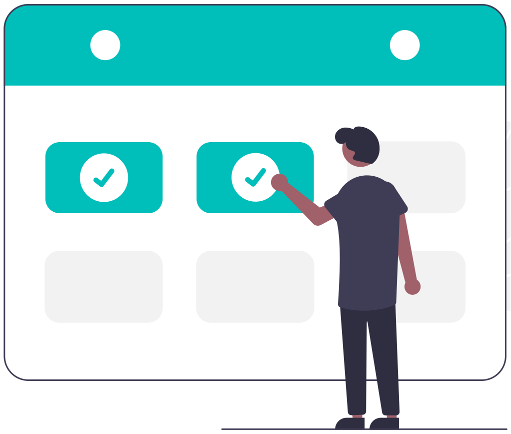
However, there is currently no set standard in place for vendors being asked to complete VSAs again in the future. Some organizations may ask vendors to complete a VSA each year, or every several years. They may only ask them to complete an initial VSA.

As long as you're prepared to complete VSAs efficiently at any time, you'll have no issue completing them whenever they're requested.

Proving HIPAA Compliance & Other Requirements

By hand, the first draft of a VSA could take dozens of hours to complete, with the final version taking weeks, or even months, depending on how prepared your business is to answer the questions.

Even if you're completing multiple VSAs simultaneously, you shouldn't use duplicate answers. While some questions may look the same at first glance, companies tend to use nuanced verbiage that may mean very different things.



Pre-Assessment Vendor Checklist

Before you jump into filing VSAs for your business, consider going through this checklist to ensure that you're prepared for all of the questions that you'll be expected to answer.

While these may not all relate to every VSA questionnaire, it's important that you understand the answers to all of these questions.

This way, you're prepared to answer in-depth questions about your company and its history, as well as the policies, procedures, and security measures you have in place.

2.3

Checklist Questions

You'll need to ask yourself questions such as:

- Are your cloud services configured for secure compliance?
- How is confidential information collected for your internal systems?
- Where is confidential information stored?
- What process is used to transmit data securely?
- Is all collected, stored, and transmitted data encrypted using the Advanced Encryption Standard's (AES) best practices? Including:
  - Established secure password access for all private information on all database servers
  - Protected access to internal servers
  - An established incident response, in the event of a data leak
- Antivirus & spam-blocking software to protect secure data from malware and phishing programs
- Protected web applications against cybersecurity attacks
- Is your business currently up-to-date on all necessary compliances, such as HIPAA policy?
- Has your business ever experienced a data leak in the past?

If so:

- How was it handled?
- Were there any repercussions resulting from the leak?
- What new security features have you put in place since the data breach?

- What are your internal privacy policies, and what software are you currently using to maintain network security for all your internal systems?
- What are your employee onboarding and offboarding security processes?
- How resilient are your current security systems?
- Could your current systems be improved prior to applying?

You will need to do a deep, thorough evaluation of all your business' internal processes, regulatory compliance practices, and security systems to ensure you're prepared for all of the potential questions that you're likely to be asked.

TIP: Answer all questions as clearly and concisely as possible. Never volunteer information or give more information than is being asked.

MedStack's Guide to Vendor Security Assessments

Chapter Three:

Best Practices for Answering VSAs

MEDSTACK®

3.1

Introduction

Now that you understand the basics of what a Vendor Security Assessment (VSA) is, as well as some tips for navigating the VSA process effectively, you're ready to complete your first VSA.

However, understanding the things you need to do and knowing the best practices you can use to complete them are two very different things.

Since VSAs range in length anywhere from 50 questions to over 250 questions, tackling one VSA successfully doesn't mean you're ready for all of them.

This chapter includes useful information that you can use to improve your practices for completing VSAs, which will not only save you time, but ensure the process is less stressful for you as well.

3.2

Tips for Proactively Preparing

Prepare Your Policies

Part of ensuring that you have all of the applicable information regarding your business processes starts with documenting the actual policies that you have in place.

Don’t have a policy in place to support a specific process? Now is the time to draft one and put it into effect. Otherwise, you might not be able to give honest, satisfactory answers when you complete the questionnaire.

The more specific policies you can quote alongside your business’ processes, the more credible and reliable your internal functions appear.

This helps add authority and confidence to your VSA, which also shows new enterprise clients that they can feel confident in partnering with you.
For example, when asked what kind of firewall your system is using, your answer would ideally be “not only do we have a firewall (and list its specs), but we are currently using this firewall policy [LINK]”.

Understand Your Own Processes

You can’t begin filing a VSA efficiently until you have a deep understanding of the processes that are used within your own company.

The enterprise wants to know that you have a formally writtenand documented process for any contingency that could arise.

Answering these types of questions accurately requires you to take time to understand all the details of the processes you currently have in place.

When answering questions about these processes, it’s crucial that you back up these claims with information regarding the policies you’ve put in place to support them.

Think About Your Audience

You should never try to duplicate answers from one VSA to another. The questions may be similar, but they may not be the same.

The more question-specific information you can give in your answers, the better. This also applies to relaying that information in a way that applies specifically to the enterprise considering your VSA.

Making this extra effort shows that you not only understand all the intricacies of your business, but you're taking the VSA process seriously. It will also provide better clarity for the people reviewing your VSA, which looks favorably on your submission.

Privacy & Security Professionals

These are the true gatekeepers. They're often understaffed and overworked, so they'll be looking for signs that your business fits their model of good security.

Third-party data breaches are one of the biggest concerns for any healthcare enterprise, so it's no surprise that HIPAA compliance and HIPAA security are such important considerations. These terms aren't mutually exclusive either, as many HIPAA requirements have some flexibility built into them.

However, remaining compliant means that at a minimum all of the required controls need to be implemented.

The privacy and security teams evaluating your VSA will be able to tell whether your systems are protected enough to consider allowing you access to their protected data.

If you've been considering instituting further HIPAA security measures, do it before you submit your VSA. That additional security could make all the difference.

Know how you protect each enterprise's Protected Health Information (PHI), and what specific tools are used to guarantee that protection.

Business Stakeholders

These are the people that want your app. They're interested in the things that your business can offer them, so you should remember that in their eyes you may already have what it takes.

For them, the VSA helps ensure that while your services benefit them, the risks that come along with bringing another third-party vendor into their systems are manageable and minimized.

Use Your Experts

Just because you can't answer a question efficiently or accurately in your questionnaire doesn't mean that you need to worry.

You should have people working in different departments of your business that you can reach out to for information when it comes to giving clear, concise answers.

Have experts on your team help give detailed answers about the privacy and security tools you're using.

For privacy and PHI, have them focus on areas like how you control access to data, whether clinicians can access that data, how you verify data is correct. how you handle patient requests, how your data flows (diagrams can help), and what you do if a patient's data is incorrect.

Security questions may be more high-level, but have those experts on your team look at what specific standards for security you're currently using. Do you have risk management or assessment programs? Do you do internal/external security audits? How is your network encrypted? You should also be prepared to share your security architecture diagram.

No single person has all the answers, and customers know that. However, it also is vital to consider the time and resource drain VSAs can be on your team, and find alternate solutions that are feasible for your company if possible.

Keep Answers Short & Sweet

Adding unnecessary or unclear information that isn't related to the question that's being asked makes your business look inexperienced – or worse, unreliable.

Always keep answers short and sweet whenever possible. Think about the phrasing they've used in their question and the specific examples (if any) that you can give to answer their question in a clear, concise way.

Never Give More Information Than Requested

Don't start offering up additional information that isn't being requested as part of the question.

Not only does that look poorly on your business from a communications perspective, it can also make you look disorganized.

Think of it this way: if your VSA answers imply you have difficulty following directions or maintaining clarity throughout an evaluation process, what is the likelihood that you can be trusted to ensure the continued privacy of health information?

Don't Leave Yourself Liable

Always be honest in a VSA. Never include misleading, false, or purposefully inaccurate information in your VSA, because you could be leaving your business open to serious liability issues.

If your privacy and security or privacy compliance practices aren't at the level they need to be, you can't fudge the truth to try and land a new client. Is your business missing something that's being requested by the enterprise?

That either needs to be properly addressed prior to submitting the questionnaire, or it needs to be reflected accurately in your VSA.

Even if it means you likely won't get this contract, lying on a VSA is never worth the risk. When you notice things that your business can't address or doesn't meet the criteria, make a note for yourself.

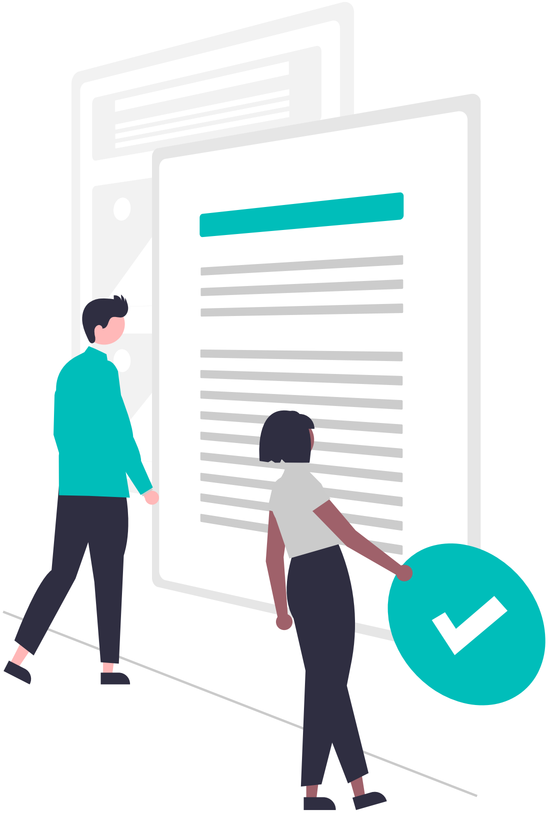
You may not get this client right now, but you can make adjustments to your planning, processes, and policies to ensure the next time a similar opportunity arises, you'll be prepared for it.

Ensure You're Fully Compliant

Maintaining unwavering health information privacy is the goal of every healthcare enterprise, but have you taken every step necessary to ensure your business is fully compliant?

It's also crucial to have all your compliance documentation in order and ready to reference, before you start completing the questionnaire. This way, if you are missing something or could improve your compliance practices, you'll have the opportunity to address them prior to submitting the VSA for evaluation.

Taking this step helps avoid overlooked compliance issues, and in turn, reduce the chances of receiving avoidable rejections from potential customers.



Keep Copies of Previous VSAs

Always keep copies of your previously submitted VSAs for future reference. Not only will this save you time and effort trying to source accurate high-level answers from other members of your team, but it will expedite the entire VSA filing process.

Just be sure to do a detailed evaluation of each answer before you utilize it in a new VSA, because your policies or procedures may have improved since your last VSA was completed.

You'll want to include any updated information, so each VSA is sent out with the most accurate, recent data.

You also want to avoid copying over any answers directly from old questionnaires, as the wording of the question in the new VSA may not match properly with that of the old one, which can lead to confusing or inaccurate answers.

Show How YouMaintain Privacy for Health Information

Ensure your NIST, ISO 27001, SOC 2, CIS, and HIPAA compliance practices are all up-to-date and all necessary information is readily available to prove that you're compliant with all relevant regulations.

Save yourself some headaches and be sure to have all the appropriate documentation available to you when you're completing a VSA.

This will save you time and energy preventing you from having to search for documentation in the middle of filing.

Talk to the Client

There's nothing wrong with asking questions to the client or requesting clarification about any of the questions that you're expected to answer on your VSA.

In fact, it can look responsible for you to request clarification, rather than make an assumption that could lead to a misleading or inaccurate answer.
If you believe your health information privacy standards may not meet those of the customer, ask them about their requirements.

Not only will this look good on you for ensuring your due diligence in research prior to filing your VSA, but it gives you time to make adjustments to your own policies, in case they aren't meeting the standards the customer needs.

In turn, this prevents avoidable rejections from customers, as well as gives you the opportunity to proactively improve your business' processes, which better prepares you for future VSAs.

Streamline your VSA Filing Process

If your process for filing VSAs or other important paperwork is just to sit down and tackle them one by one, you may want to consider instituting something more time efficient.

VSAs can take an extremely long time to fill out by hand, especially if you're not prepared. Consider how overwhelming that can become if you have multiple VSAs that you're trying to complete simultaneously. Take some time to create a process that reduces how much time you need to spend per questionnaire.

You can create a database of answers, which you can add to each time you submit a VSA. After a few, you'll notice trends in the questions you're being asked, as well as the answers you're giving. This will help you prepare to face other VSAs in the future.

Alternatively, you can turn to a company like MedStack. MedStack can alleviate a substantial portion of the time required for filing VSAs, and allow you to take back precious time and energy for other critical tasks like growing your business.

Our AI-powered proprietary answer library can answer up to 90% of compliance-related questions for you – and its adaptability is increasing every day. Our answers are pre-set by our pre-configured and industry-validated infrastructure security.

MedStack has already helped complete hundreds of assessments from major enterprises across North America, with the backing of our real-time updated, inheritable policies, as well as our built-in security and privacy controls.

Stop wasting your time, energy, and resources focusing on paperwork instead of your product. Let MedStack put your business on the fast track to growth and take your application from zero to healthcare hero.

Book a Free Discovery Call Today

@MedStack /MedStack medstack.co