Hushmail

GUIDE

Risk assessment for your practice

Risk assessment for your practice

Why you should conduct a risk assessment

“Risk assessment” is a term that often leads to anxiety, particularly for those managing a small practice. You may know that it’s something you should do, but not fully understand what it means. Or perhaps you worry you don’t have the resources to do it properly.

A risk assessment is the systematic analysis of a practice’s assets, the threats to those assets, and the potential consequences should any of those threats damage or otherwise compromise an asset.

There are several reasons why a small healthcare practice should conduct a risk assessment.

HIPAA compliance

First, the Health Insurance Portability and Accountability Act (HIPAA) requires the safeguarding of the confidentiality, integrity, and security of protected health information (PHI). Healthcare practices must have administrative, physical, and technical safeguards in place to ensure that PHI is protected from theft, leaks, breaches, cyber crimes, and other threats. The best way to ensure that you are implementing the appropriate safeguards, and demonstrating compliance, is to conduct and maintain records of regular risk assessments.

Best practice

Second, many health care practices use a risk assessment to create a clear picture of their practice’s assets and to pinpoint potential threats to those assets so they can be avoided or eliminated altogether. Such a process helps to strengthen the overall integrity of a practice.

Protect client information

Of course, most importantly, a risk assessment protects the security of your clients’ personal information. This consideration alone is crucial to the integrity of your practice.

Don’t be intimidated. Risk assessment can be simple.

It’s a common misconception that risk assessment is best left to the big medical practices with large IT departments and hefty security budgets.

It’s important for small practices to conduct risk assessments too. HIPAA compliance demonstrated with a thorough risk assessment is important if a security breach occurs and you are required to show that you put forth your best efforts to protect your clients’ information. Recovering from a breach when you can show compliance will be a far simpler and less damaging situation than if you’re caught unprepared.

Fortunately, a risk assessment isn’t as complicated or as costly as it sounds. There is no need to be intimidated.

Assign a security officer

It’s a good idea to assign a security officer so there is one person responsible for handling the risk assessment. If you have a small practice, that person might be you. When one person is knowledgeable about your practice’s security, it’s much easier to track down information when it’s needed.

Four simple steps

Risk assessment is common sense, and you can learn the basics in about 15 minutes from this guide. In the following pages, we’ll lay out four simple steps:

1. Identify your assets
2. Imagine the impacts
3. Consider and prioritize the threats
4. Reduce your exposure to risk

You will be guided through these steps one by one. If you follow along, then by the time you reach the end of this guide, you’ll have a clear picture of where your practice stands in terms of security risks and what you can do to reduce your exposure to them.

Step 1 - Identify your assets

The first step of a risk assessment is to identify your assets. Take a full inventory of anything of value that could be lost, stolen, leaked, or damaged. This includes any of the following that make sense for your practice:

- Client records and notes
- Accounting records
- Names and addresses of clients
- Equipment, including computers, fax machines, printers, scanners, etc.
- Computer records

Keep in mind that some of the assets listed above may be stored in the cloud through a third-party service. These assets are still your responsibility and should be included on the list.

It's up to you what qualifies as a separate asset. A good rule of thumb is to consider how the practice would be affected if that asset were stolen, lost, or damaged. If the effect is unique to that asset, then it should be listed separately.

Make a concrete list

Don't be tempted to list your assets in your head and leave it at that. Be sure to create a concrete list either in a file or on paper. Going through the effort of spelling out your assets in exact terms ensures that you're painting an accurate, complete picture of your practice. It also allows you to make connections you might otherwise miss.

An auditable record

Another reason to make a concrete list is that it creates an auditable record showing that you've gone through the risk assessment process. If the worst case scenario occurs, and you need to show that you've gone through the steps to protect your clients' information, you will have a record ready to go.

Step 2 - Imagine the impacts

Once you have a list of assets, go through it item by item and record what the impact would be if that asset were lost, stolen, leaked, or damaged.

Ask yourself these questions

- How would your practice be affected?
- How much revenue would you lose?
- Would the impact be an embarrassment and damage your reputation?
- How long would it take to recover?
- How might your clients be harmed?
- Would you be required by any laws in your jurisdiction to report the breach?

Play out the scenario in your head

For example, if you work in a private practice providing marriage counseling, and client records are lost, you run the risk of damaging your practice's reputation, losing clients, and losing revenue. The reputations of your clients might be damaged as well, and there could be legal consequences to consider. It could be very difficult to recover from such a scenario.

Thinking forward into the future about what could happen to your practice if an asset is compromised is a valuable exercise that puts you in a position to protect your practice before a damaging breach occurs.

Step 3 - Consider and prioritize the threats

The next step is to figure out *how* your assets might be lost, stolen, damaged, or otherwise compromised by a threat.

Examples of threats might include the following:

- A thief who steals your computers
- A cybercriminal who hacks your electronic health record (EHR)
- A fire, hurricane, or other natural disaster that destroys paper records
- An employee who unwittingly or purposefully discloses client information

Threat likelihood + impact = risk level

When you combine the likelihood of a threat with how damaging it would be to your practice, you get the risk level. By assigning a value to each threat reflecting the risk level, you can determine where to put your resources and protect your practice from the most likely and damaging scenarios.

Risk Level Matrix

The Risk Level Matrix is a simple tool that guides you through the process of determining the level of risk you're dealing with when it comes to each asset. Run each threat through the matrix below to figure out the risk level for each asset.

		Impact		
		Low	**Medium**	**High**
Threat likelihood	**High**	Low	Medium	High
	Medium	Low	Medium	Medium
	Low	Low	Low	Low

Impact

For example, when considering the threat of a cybercriminal hacking your EHR, you will consider the threat likelihood to be high if your data isn't encrypted. The impact this threat would have on your practice would also be high - losing patient information could be devastating to a

practice. Therefore the risk level of this threat is high and should be addressed as soon as possible.

Step 4 - Reduce your exposure to risk

Once you identify the threats with a high risk level, you will want to reduce your exposure to those threats. This is also referred to as “risk reduction.” Because you’ve gone through the process of listing your assets and threats and putting the threats through the Risk Level Matrix, you can prioritize your resources.

Assign priority

After the risk assessment you will likely find one or two threats with a high risk level that need to be addressed immediately. You might decide a few others with a medium risk level can be put off but should be addressed by the end of the year. The rest of the threats may be addressed when you have the time and resources or, if the risk level is low, may not need to be addressed at all.

Decide next steps

Next, you’ll decide what needs to be done to reduce the risk associated with the threats. This might include writing a new security policy, upgrading out-of-date equipment, or subscribing to services that are HIPAA compliant.

The following are some examples of ways you can reduce your risk:

- Require whole disk encryption that renders data on a hard drive unreadable without the proper password to decrypt the disk
- Review all of your third-party services for HIPAA compliance and ensure that your signed Business Associate Agreements (BAAs) are on file
- Create an onboarding process with a rigorous security segment for new practitioners or staff

How you choose to reduce your risk will depend on the threat and your resources.

Remember that any risk reduction is better than none, and understanding your threats in very clear terms will allow you to accurately plan and budget for reducing your exposure to them in the future.

Conclusion: it's not rocket science

As you can see, risk assessment isn't rocket science, and it's a good way to assess all areas of your practice at one time. During the risk assessment, don't be surprised if issues affecting multiple areas come to light that require action.

In a way, you can consider risk the measuring stick for the overall integrity of your practice. If you assess your risks and take the steps to reduce them, other parts of your practice will often fall in line as well.

How often should you conduct a risk assessment?

The short answer is once a year. However, if there's a major change in your practice, it's a good idea to conduct at least a mini assessment. Major changes might include the following:

- A move to primarily virtual services
- A geographical move
- A new EHR system or other new technology
- A change in leadership
- Anything that changes the way you manage your practice or care for your clients

If you're new at conducting risk assessments, for the first few years, we highly recommend you conduct at least an annual assessment. As you become more experienced with the process, and if your practice is stable, you can adjust the schedule to suit your own needs.

Take the plunge

Our hope is that by going through the steps in this guide, you will find the process much less intimidating and something you will happily conduct whenever you're feeling uneasy about security or HIPAA compliance.

While HIPAA requires risk assessment, it is simply a best practice. Once you make it a regular part of your practice, you'll wonder what you ever did without it.