A PHYSICIANS GUIDE TO SECURITY RISK ASSESSMENT

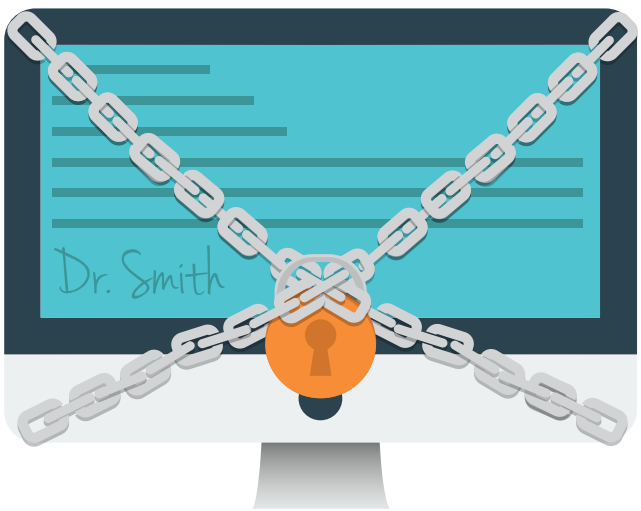
ISALUS HEALTHCARE

ISALUS HEALTHCARE

A PHYSICIANS GUIDE TO SECURITY RISK ASSESSMENT

TABLE OF CONTENTS

INTRO



As most of us know, the Health Insurance Portability and Accountability Act (HIPAA) requires healthcare providers handling protected electronic health information to regularly review the administrative, physical and technical safeguards they have in place to protect the security of the information they are managing. The premise is that by conducting these risk assessments, healthcare providers can uncover potential weaknesses in their security policies, processes and systems. The same risk assessments are also meant to help healthcare providers address vulnerabilities, thereby preventing potential breaches in the future.

Over the past several years, it's become more and more important for healthcare providers to perform these security risk assessments on a regular basis. Meaningful Use has made it mandatory for all providers to be in compliance, no matter how small or big your practice is. Any provider who is a Covered Entity under HIPAA is required to perform regular security risk assessments – especially if you want to receive EHR (electronic health record) incentive payments. Contrary to popular belief, this is much more detailed than simply installing a certified EHR. Essentially, the security requirements address all electronic protected health information, not just what is maintained in an EHR. However, it is important to note that your EHR vendor may be able to provide information, assistance and training on the privacy and security aspects of the EHR product. Nonetheless, it's the sole responsibility of the healthcare provider to have a thorough security risk assessment completed.

DO I NEED TO OUTSOURCE MY SECURITY RISK ASSESSMENT?

NO Some providers may believe this is an easy answer to performing an exhaustive audit that will ensure they are compliant but this is not necessarily the case. Many small to medium-sized practices are able to complete a security risk assessment by using helpful tools available to help measure the risk analysis and document the outcome; all in a simple and automated fashion.

THESE TOOLS CAN:

- Reduce costs and increase revenue
- Help your practice comply with Medicaid, Meaningful Use and the Department of Health and Human Services (DHHS)
- Protect your reputation and your patients' data

In fact, some of the tools available will make sure that your organization is always ready with the right documentation of the most current assessment of potential risks and vulnerabilities relating to the confidentiality, integrity and availability of electronic protected health information (e-PHI) in addition to the progress on remediation of those risks identified. These tools make the entire process much easier on the provider. Remember, the security risk assessment (SRA) is not a one-time deal. You must continue to review, modify and update your security processes on an ongoing basis. You must be prepared to produce a remediation plan and demonstrate reasonable progress towards remediation.

IS THERE A STEP BY STEP GUIDE I'M SUPPOSED TO FOLLOW?

NO The Office for Civil Rights (OCR) issued guidance to assist practices when identifying risks and implementing the appropriate remediation but there is not a specific step-by-step guideline you should follow. It's also important to note that you do not have to fully mitigate all risks before demonstrating your compliance for an EHR incentive program. You are only required to show you are correcting any deficiencies identified during the assessment during the reporting period as part of the risk management process.

WHAT AREAS SHOULD MY SRA ADDRESS

The HIPAA Security Rule identifies over **78** controls (in citation form), to include "*required*" and "*addressable*" controls. Make sure you look for a tool that has consolidated these with other industry best practices into a Common Control Framework that is aligned to with the HIPAA Security Rule.

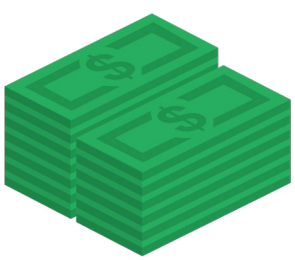
KEY AREAS ADDRESSED ARE:

- **Discover** – Learn the requirements and meet with the responsible parties
- **Evaluate –** Review the scope of current systems, audit trails and processes
- **Test –** Conduct IT penetration testing and ethical hacking to identify weaknesses
- **Analyze –** Review results to determine the applicable areas of focus
- **Update –** Implement systems & procedures then provide updates & reports.

WHAT TOOL IS BEST FOR ME TO USE?

There are a few important qualities you should seek when choosing the tool that's right for helping your practice complete a thorough security risk assessment. The right tool should be able to quickly and effectively self-assess your own environment's HIPAA compliance and provide ongoing remediation tracking, email reminders and automated reporting.

THREE MAIN CHARACTERISTICS ARE GOING TO BE:



Affordability

Automation

Simplicity

WHAT HAPPENS IF I DON'T COMPLY?

As a result of the changes driven by The HITECH (Health Information Technology for Economic and Clinical Health) Act, all Covered Entities and Business Associates must be compliant and completing a formal Security Risk Analysis is a crucial step in doing so. Enforcement of compliance has increased significantly over the last year and includes the following:

- Mandatory Audits
- Business Associates Must Comply With New Laws
- Subcontractors Must Comply With New Laws
- Non-Compliance Fines Are Being Enforced

- Stiffer Penalties
- Jurisdiction Provided To State Attorneys General To File Civil Actions Against Violators

Because of this, it is more important now, than ever before, to build your organization's risk management program methodically with a proven solution. All **78** Security Rule citations need to be addressed.

GETTING STARTED

Though a specific risk analysis methodology has not been presented as the standard to measure by, there has been a foundational element identified for the process of achieving compliance which sets multiple objectives to be achieved during whatever process you may choose. Let's take a detailed look at those objectives.

NO. 1 IDENTIFYING e-PHI

First and foremost, healthcare providers need to identify all e-PHI created, received, maintained or transmitted by the practice both inside and outside of the EHR. Again, all e-PHI is under scrutiny and must be evaluated for vulnerabilities and risks in their environments. This objective addresses not only the e-PHI created within your practice, but also health information you may have received from an outside source or have transmitted to an outside source. Start gathering and documenting the most obvious sources of health information and then audit any past or current projects by interviewing staff in charge of those projects to make sure e-phi does not exist in additional spaces. Staff should be questioned about their data collection processes and storage during the related projects.

NO. 2 DOCUMENTING OF RISK IS KEY

After you have identified and documented all e-PHI that exists in relation to your practice, you must begin breaking down each source and start analyzing it for risks and vulnerabilities. This includes identifying anyone who comes into contact with the information such as staff, vendors and consultants. Additionally, you must identify natural or environmental threats to the systems that contain e-PHI. Each organization will have risks that are exclusive to their practice that should be well-documented. Documentation should include an explanation of what would happen if any particular vulnerability was actually triggered creating the risk of inappropriate access to or actual leak of the e-PHI.

NO. 3 EVALUATE SECURITY PROCESSES

Once your practice has identified potential risks and vulnerabilities, it's time to evaluate the current guarantees you have in place as required by the Security Rule. Furthermore, you are also required to document whether or not those processes are set up properly and being used correctly. This will be a bit easier for a smaller practice to accomplish as they most likely have fewer vulnerabilities due to requiring less staff and interacting with fewer outside sources. This will, again, be particular to your individual practice as each practice has unique vulnerabilities and overall circumstances. You must also address staff administrative procedures and policies as part of the security umbrella.

NO. 4 DETERMINE THE PROBABILITY

So what are the actual chances of threat to the e-PHI of your practice? The Security Rule requires all practices to take into account the probability of potential risks. Then you must combine the initial list of vulnerabilities with the assessment of probability to determine and document which threats require protection because they are reasonably anticipated. Basically, the documentation will include all threat and vulnerability combinations with associated probability estimates that may impact the confidentiality, availability and integrity of the e-PHI of your practice.

FEELING CONFUSED YET?

SO ARE WE! So this is all a bit overwhelming and we still have several objectives to get through. Because this is enough to make your head spin, we wanted to stop and point out that there are tools to help you accomplish a detailed Security Risk Assessment in no time at all (here's one). If you're like most healthcare providers, what little time you have needs to be spent focusing on the care of your patients. Time-consuming requirements like the Security Risk Assessment can be limiting and result in inefficiency that effects the entire practice, in addition to your bottom line. Now let's get back to work.

NO. 5 ASSESSING POTENTIAL IMPACT OF THREAT

At this point, you've identified all sources of e-PHI in the practice; you've pinpointed every vulnerability and risk to the e-PHI; you've evaluated the security processes in place for those risks; and you have determined the probability of those risks actually being triggered. The next step to a thorough Security Risk Assessment requires that you determine or evaluate the actual impact of each potential risk to confidentiality, integrity and availability of e-PHI should it actually be triggered. In other words, what actual impact would that exposure have? When measuring this impact, you are required to use either the qualitative or quantitative method or a combination of both. As a result, your documentation should include all potential impacts associated with the occurrence of threats triggering or exploiting vulnerabilities that affect the confidentiality, availability and integrity of e-PHI within your practice.

NO. 6 ASSIGNING THE LEVEL OF RISK

After all the previous objectives have been completed, it is then time to evaluate the true risk level for each threat and vulnerability combination that has been identified during the risk analysis. For example, you could determine the level of risk by considering the values selected for the likelihood of threat occurrence and resulting impact of threat occurrence. The risk level determination might be performed by assigning a risk level based on the product of the selected likelihood and impact levels. As a result of this determination, your documentation should then include the assigned risk levels and a list of corrective actions to be performed to mitigate each risk level.

FINALIZING THE DOCUMENTATION

Interestingly enough, for all of the required objectives we've addressed, there is not a required format for the documentation of each step. Additionally, there's not a specific requirement for how often you conduct a risk analysis, only a requirement to document security measures and updates as needed. So does this mean you perform a Security Risk Assessment every year, every month or every week? In all fairness, the frequency will probably vary greatly from one entity to the next depending on variables such as size, specialty and environment. However, a truly complete risk analysis will be an ongoing one. The type of assessment that is always up to date and alerting you of any new vulnerabilities that may present themselves, along with making sure documentation is complete to remain in compliance.

Consider this, every time a new technology is introduced into the practice a Security Risk Assessment must be performed. Every time a new vendor comes into play, a risk analysis must be updated. Better yet, performing the risk analysis before the implementation of new technology or addition of new vendors is even better. This allows for potential high-impact risks to be avoided altogether. Ensuring that e-PHI is always protected and potential risks are safeguarded against is an ongoing process that really never stops. If you want to be compliant under the DHHS Security Rule, you will always be required to have a detailed understanding of the risks to the confidentiality, integrity and availability of e-PHI.

CONCLUSION

At the end of the day, this is a lot of work. Staying in compliance with the Security Rule is something that could become time-consuming, error-prone, and even result in added stress to your staff. One way to avoid this unhappy outcome would be to look towards an automated tool. As more and more regulations come down the pipeline, look for the help that technology can provide. It's the only real way you're going to be able to stay focused on patient care while remaining in compliance in order to receive the incentive payments needed to stay in practice.