Intraprise HEALTH™

Take a fresh look at your Annual Security Risk Assessment (SRA)

Organizational Resilience and Security Risk Assessments

The importance of a Security Risk Assessment is evident: it helps healthcare organizations ensure their physical, technical, and administrative safeguards are compliant with HIPAA requirements. It also highlights areas where an organization might be putting PHI and other sensitive information at risk.

All PHI and electronic PHI (ePHI) that a facility creates, receives, maintains, or transmits must be protected and a risk assessment is an essential part of this process.

As recent headlines have taught us, a security breach in healthcare—as in every industry—is not a matter of if, it's a matter of when. When your organization is hacked, your security professionals should only need to focus on the threat itself—and not be bogged down with administrative issues, such as when you last updated your software or when your vendors last updated their certifications.

The resilience of your organization is directly tied to the thoroughness of your Security Risk Assessments. The speed of the response to an attempted breach will directly impact your organization's ability to get back to business as usual. If you are unable to respond in a timely manner, or are unaware of a breach for months, or even years, you lose the confidence of your patients, customers, and all who do business with you.

According to the Annual Cost of a Data Breach Study by the Ponemon Institute, one of the most significant costs following a data breach is the loss of customers.

Lost customers equal lost revenue.

A thorough Security Risk Assessment increases your organization's resilience.

Here is a checklist that you can use as you interview Security Risk Assessment firms to ensure you receive the best service and guidance possible:

- ✓ Clearly understand your HIPAA/HITECH compliance mapped against the OCR Audit protocol
- ✓ Identify which security vulnerabilities exist in your internal and external network(s)
- ✓ Test your network's posture to withstand malicious penetration exploits and intrusion by hackers
- ✓ Assign severity ratings to assessment findings that pose risks to regulatory compliance, patient-care, and safety, as well as business operations
- ✓ Document the current state of your security controls against a nationally accepted, best-of-breed set of cybersecurity frameworks (e.g., NIST CSF, HITRUST CSF)
- ✓ Map your Report of Findings against HIPAA, NIST, HITRUST and OCR controls/requirements
- ✓ Meet Meaningful Use requirements associated with information security and compliance
- ✓ Evaluate the previous years' risk analysis program and remediation progress
- ✓ Understand which persistent trends pose high levels of recurring or systematic risk
- ✓ List potential solutions and remediation recommendations to enhance your risk management capabilities
- ✓ Establish a sustainable operating model for your information security management program
- ✓ Build trust and confidence with patients, providers, business partners, and the community through diligent assessment and remediation steps
- ✓ Advocate the reality that security is **NOT** an **IT** issue. It's an organizational and patient safety issue.

Secure with Vigilance™

What to look for in a Security Risk Assessment

Some hospitals and health systems shop around for their annual SRA firm with the goal of checking off the compliance box, while others pursue partners who will give them a fresh perspective on their information security program, policies, and best practices.

If it is time for your annual Security Risk Assessment, and you would like to make this assessment accurate and thorough, take a moment to look at our list of "must-haves" for what you should look for in an assessor:

1 CONDUCT A COMPREHENSIVE, COMPLIANCE-FOCUSED REVIEW

Your security risk assessor should conduct an accurate and thorough review of the potential risks to your confidentiality and integrity, as well as the vulnerability of your electronic protected health information (ePHI) and other sensitive information. It should be a compliance-focused assessment that relies on the best frameworks and regulations in the industry, including:

- HITRUST Common Security Framework (CSF)
- HIPAA/HITECH/Omnibus 2013 Final Rule
- Other authoritative sources - PCI-DSS, NIST Cybersecurity Framework, ISO 27001 and CIS Critical Security Controls

2 ASSESSMENT MUST BE RISK-BASED

Compliance does not equal security. That is not to say compliance isn't essential or required—because it is. Understanding where you stand against known and published regulations, laws and frameworks, is paramount to your ability to conclusively demonstrate security program maturity, vision, and road mapping. With that said, the real key to protecting your organization from disclosure or breach is to identify risk and prioritize the remediation and management of that risk. Using risk as the barometer for focus and prioritization will make allocating resources (time, people, money) an easier task. The assessment results will give you a clear starting line and an order in which to tackle problems. Furthermore, the HIPAA Security, in section 164.308 (a)(1)(ii)(A), requires covered entities and business associates to "conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information." *cont.*

What to look for in a Security Risk Assessment

3 CRITIQUE OF POLICIES, PROCEDURES, AND PROOF OF COMPLIANCE

Risk assessments should go beyond the “four walls” of the IT department and include a multi-tiered approach to identify vulnerabilities and their associated risk across the entire organization. This includes an administrative review and critique of policies and procedures, documentation, and implementation evidence, along with interviews with essential security program personnel.

4 ROBUST VULNERABILITY SCANS, CONFIGURATION REVIEWS, AND PHYSICAL INSPECTIONS

Your security risk assessor should highlight where your policies, procedures, technology, and documentation are strong, as well as alert you to the blind spots and weaknesses that may put your organization at higher risk.

Technical endpoint (including medical devices) and network vulnerability scans should be conducted alongside device configuration reviews. Equally important is carrying out physical walk-throughs of facilities, departments, data centers, and medical offices, inspecting physical access control measures and environmental hazard capabilities. You would be surprised at what we find when we do this!

5 SOCIAL ENGINEERING

Often a forgotten or underutilized tool in an assessment toolkit, social engineering is an effective way to see whether your policies, procedures, training, and awareness efforts are bearing fruit. Your assessment team should be utilizing techniques to enumerate sensitive information or gain access to secured areas. The results of these activities will demonstrate where you should focus your attention on closing those gaps.

6 TRUST BUT VERIFY

In the past, many healthcare risk assessment providers would provide questionnaires and conduct interviews to assess compliance and identify risk without actually validating whether the controls and safeguards exist. They would take what was given to them at face value. Unfortunately, this type of assessment (although inexpensive in some cases) provides a false sense of security for the assessed organization. Security technologies are the best example. An organization will purchase Data Loss Prevention (DLP) software but will not fully implement and manage the software. On a questionnaire, the organization is compliant—they have DLP. But is it as effective as it should be? As you can see, the actual value and the perceived value of that tool is not in line.

Robust and sufficient risk assessments will ask the right questions and require evidence to validate the existence and effectiveness of the controls. *cont.*

What to look for in a Security Risk Assessment

Return to the Checklist on the first page when interviewing your SRA firms.

7 COLLABORATIVE ASSESSMENT WITH REMEDIATION

Now that you know your risks—what comes next? Your security risk assessor should work side-by- side with you as an extension of your team, giving you a workable plan and recommendations for corrective action. Their support should continue as you take the first steps to remediate any gaps in your security.

Your assessment should address remediation priorities in a Report of Findings and a Briefing on Stakeholder Findings and Recommendations. Your security risk assessor should provide a corrective action plan (CAP) that contains specific remediation guidance.

At the end of your annual Security Risk Assessment, you should feel assured by the findings and confident in knowing the steps you should take to remedy the gaps.

8 MANAGE THE RISK

Unfortunately, risk identification and compliance assessments are the easy part. Mitigating the risks and filling the gaps is where the real work begins.

But, how can you implement a plan to manage risks? You may not be sure where to start or feel like you have enough staff or resources or expertise to take it on.

These are valid and real concerns that can be overcome with the right internal and external support. What's most important is your commitment to meet your organization's requirement to manage risk.

The HIPAA Security Rule requires explicitly organizations in 164.308 (a)(1)(ii)(B) that "Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306(a)."

There are **four** ways to manage risk:

- **Transfer the risk**
- **Accept the risk**
- **Remediate the risk**
- **Avoid the risk**

Within the healthcare industry, you typically would only see two of the four utilized: accept or remediate. Risk acceptance is a suitable way to address identified risk, but doing it formally with just reasoning is critical in protecting the organization in the case of a breach or audit.

About Intraprise Health

The Intraprise Health Security Services team has more than 30 years' experience in healthcare engineering, many annual assessments under our belts, and the ability to deliver a full suite of remediation and other security services after the assessment.

Learn more about our professional, qualified team of assessors, read our excerpt from the KLAS 2018 Information Security Report where we achieved a rating of 97.2* out of 100, or request an SRA proposal, by contacting Pamela Hayduk – phayduk@intraprisehealth.com.