# Expanded

## Security Risk Assessments

An introduction to the mandatory HIPAA SR assessment condition



## Summary


A Security Risk Assessment (SRA) is a requirement and a benefit for all medical practices. An SRA is a process that identifies security risks for a practice. The outcome of an SRA is a formal report which can be referenced by an auditor, confirmed by an affiliate, and more importantly, used by a practice to improve itself. Risk Assessments help HIPAA Covered Entities identify the location, risk, likelihood, and damage of data being violated.

This process can be performed internally by Practice staff, but a third party assessment is preferable. The process can be lengthy and requires both technical expertise and awareness of the latest expectations from the U.S. Department of Health & Human Services. An unbiased account of the security of a practice accompanied by an official certification will increase the likelihood of a favorable audit.

Reasons to have an SRA performed:

- The Health Insurance Portability and Accountability Act (HIPAA) Security Rule requires that covered entities and their business associates conduct a risk assessment of their healthcare organization.
- The Medicare Access and CHIP Reauthorization Act (MACRA) requires medical providers to “Conduct or review a security risk analysis in accordance with the requirements in 45 CFR 164.308(a)(1), including addressing the security (to include encryption) of ePHI data created or maintained by certified EHR technology in accordance with requirements in 45 CFR164.312(a)(2)(iv) and 45 CFR 164.306(d)(3), and implement security updates as necessary and correct identified security deficiencies as part of the MIPS eligible clinicians risk management process.”
- As of 2018, the Department of Health and Human Services has begun to issue fines starting at $10,000 for failure to have completed a Security Risk Assessment annually.
- Accountable Care Organizations are required to ensure its members have a certified SRA annually.

If a breach occurs, the auditor will request the most recent SRA audit to review your formal due diligence. We’ve observed auditors apply more leniency to practices that did their best to avoid ePHI threats leading up to the breach; the evidence is an SRA.

The act of performing requesting an SRA is the hardest part because the actual process can be done in less than 3 hours by ancillary staff. An SRA audit does not have a pass or fail out - it is merely a call to attention.

## The Purpose of a Security Risk Assessment

An SRA audit acts as a guide for establishing and evaluating the measures to ensure the security and privacy of the company’s electronic Protected Health Information (ePHI). It also works to inspect company assets, processes, resources, and devices that have contact with ePHI. The result is a controlled, high-quality assessment of the security of your operating environment. It focuses on sensitivity, threats, risks,and safeguards. The output is a series of corrective measures to alleviate threats, related exploitable weaknesses, and other associated affirmative attestation requirements.

1. Comply with the requirements of the HIPAA Security rule, which entails that all healthcare organizations under it run a comprehensive and precise risk assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI.
2. To assist healthcare organizations, recognize threatened areas where ePHI could be at risk, which in turn will help to assess the risk and vulnerabilities and take adequate measures to decrease it to a reasonable level, which are all seen as good practices in business.
3. To be able to benefit from meaningful utilization of the program, thereby receiving Medicare incentives after completion of the analysis and correcting security deficiencies and attesting it.

## Electronic Protected Health Information

As you have heard countless times, ePHI must be protected at all times. Each time this data is created, sent, received, and stored it's open to endless threats.

Common types of ePHI include:

- General information: Name, address, dates (birth/death date, admission/discharge date), phone numbers, fax numbers, and email addresses
- Care and insurance information: Social Security number, medical record number, health plan beneficiary number
- Personal identifiers such as finger or voice print and images.
- Certificate / license numbers
- Financial information: account number, credit or debit card number
- Any other unique identifying number, characteristic, or code
- Property information: car and devices identifiers or serial numbers

Any other unique identifying number, characteristic, or code that can identify a patient is considered ePHI. Some of the information seems irrelevant but recall when you forgot the password to your bank account, and the automated system asked you the name of your first pet, where you met your wife, or your favorite vacation spot - a hacker armed with those details could gain access to your accounts with only endless minutiae.

## Associated Threats

Turn on the TV or read the newspaper and you'll hear about significant breaches every day. The Michigan breach portal lists 20 recent significant breaches to organizations of whom you know. There are over 200 cases currently under investigation.

Threats are classified as:

1. Natural threats - threats which are disasters that cannot be avoided as well as are hard to predict, especially in the context of data protection. Typical examples are tornadoes, earthquakes, and storms.
2. Environmental threats - These threats refer to exposure to both internal and external environment, such as pollution, outages, chemicals, etc.... They are less common, but when they occur, the reach is often much further than one may expect
3. Human threats (the most common) - These refer to the type of risks that are caused by individuals. Deliberate acts such as with cyber-attacks, malware upload, computer and USBs theft, and medical ID theft. Non-deliberate actions include errors in data entry, unintended deletion, etc.…

A frequent human threat is a disgruntled employee, often a Manager, that steals ePHI intentionally and reports the breach to harm their former employer. On the Michigan breach portal, 20% theft and 40% are from hacking / IT incidents.

### Vulnerabilities of ePHI

Threats can exhaust specific vulnerabilities such as the computer monitors being visible or weaknesses in the organization's security procedures design or implementation. The fault may be technical, such as a laptop with no password or an open wireless network that gives free access to the system; alternatively, non-technical threats, such as missing internal policy and procedure manual or leaving the back office unobstructed. We've often found that most practices that have a policy and procedure in writing have no associated adherence.

## Importance of performing a Security Risk Assessment

Completing an SRA is not only the right thing to do, but also the HIPAA Security Rule and other formal Government acts require it. HIPAA states that all covered entities and their business associates must conduct such an assessment regularly. It is of utmost importance to assess the digital and physical security of your practice. Auditors want concrete evidence of a periodically occurring security assessment.

An SRA aids healthcare providers ensure they are compliant with HIPAA's administrative, physical, and technical safeguards. It also recognizes vulnerabilities that otherwise could expose ePHI, which if not resolved could expose your practice to cybercriminals, hackers and autonomous malware bots which are a growing threat facing healthcare clinics, and private medical practice owners globally. Your business and medical license are at risk even if the violator is an employee or a foreign person.

## Benefits of performing a Security Risk Assessment

Conducting an SRA will help clinics to strengthen security and reduce your risk to HIPAA breaches. In-depth evaluation offers many benefits which are priceless compared to the fines of a violation or absence of incentive program funds.

Common benefits are:

1. **Identify security vulnerabilities-** By considering external and internal threats, an SRA will highlight current security vulnerabilities, inadequacies, as well as non-compliances with standards for security policies of the entire system. The practice will have a list of specific security concerns prioritized by risk. You cannot manage what you cannot measure; an SRA a measurement.
2. **Creation of a security worklist -** With identified weaknesses an SRA will be able to determine the subsequent steps necessary to eradicate identified weaknesses and strengthen the system's security. Many of these requirements are free or require minimal time and energy to comply.
3. **Reduce financial risk-** Just a single fine from the OIG, HHS, CMS, MACRA, etc.… is enough to cripple a practice. Associated penalties average approximately $200,000 and could require that you close your practice. An SRA costs between $500 - $2,000 to perform so unless you're confident that your practice will never have a violation over 100

years then it makes good fiscal sense to have an SRA completed. MACRA has not only recouped funds from practices that lied about having an SRA performed, but they've also issued a $10,000 - $50,000 fine for the violation.

4. **Conduct smart purchases-**A risk assessment will be able to assist clinics with aligning the costs of security improvements with long-term financial benefits to prevent adverse events. Having a strategy which includes forethought is more cost-effective than placing endless bandaids on a risk. The assessment precludes an organization from overspending on a resolution.
5. **Document due diligence-** an SRA will validate the clinic's efforts to enforce proper security measures which, in turn, may act as evidence of due diligence to auditors and investigators.
6. **Employee Education-** Increasing employee awareness of security policy and risks creates more than a simple security benefit. Increased efficiencies will then lead to increased knowledge for the clinic and its employees. Employees will be more likely to use security best practices in daily operations. Most practices that have a high awareness of such vulnerabilities are self-correcting. It's rare that Administration truly knows the weaknesses of their practice from the perspective of the employees.
7. **Increased motivation**- For most clinics, the fact that an SRA is underway, will demonstrate to its employees that security is a significant concern. Armed with a renewed understanding of security risks, employees may feel an increased sense of motivation and productivity within their teams. By providing a purpose for a process, you encourage motivation for adherence.
8. **Improved communication and decision-making-** By starting a conversation about security, you open the doors for discussion of other subjects. Moreover, the detailed information provided by an SRA may assist to ease decision-making by removing some ambiguity of what is right or wrong. All methods that increase communication and teamwork will improve the practices ability to make and maintain better decision.

## Fundamental Protective Measures

Easy measures that practices should follow to protect ePHI are easy to implement and can decrease your risk significantly.

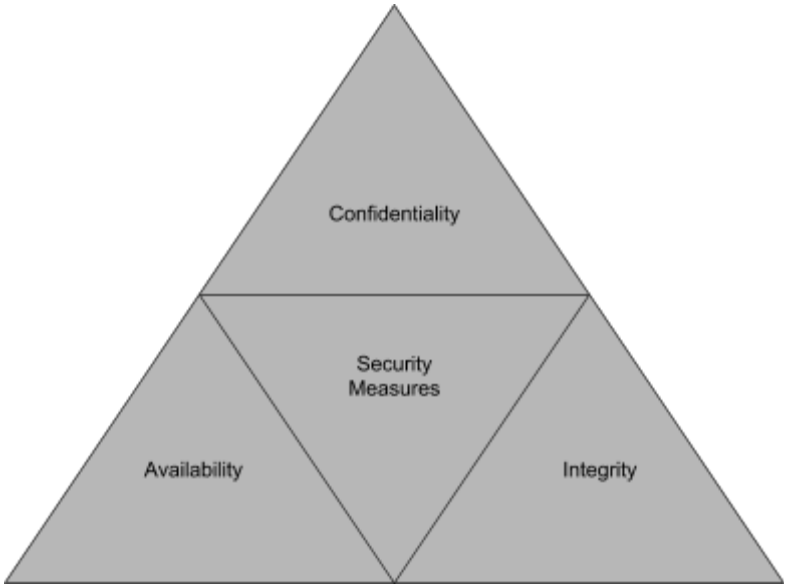
- Implement a server to secure workstation access by using centrally managed login credentials.
- Secure the use of the network by enabling encryption, installing a firewall, and using security software which often are free programs included in your workstation computers.
- You are securing mobile devices with a device policy hardcoded into phones that access data and employing the means to remotely wipe ePHI once the mobile device is no longer in use by using modern document management programs such as G Suite or Office 365.
- You are securing the internal network by removing the guest WiFi and adding a password.

It is important to note that all necessary security measures will not protect the organization from all and vulnerabilities, not even the best security measures will. There are automated systems which will routinely attempt to create a data breach regardless of who or where your practice is. Most of the threats discussed during an SRA are things you never considered, but once you

hear about them, it seems obvious. Internal and external threats will capitalize on that lack of consideration somehow someday, it's just a matter of time.

### Security Measure Core Components

To design a security measure you need to identify when and where a security risk exists and its potential impact. The recipe to make a security measure to protect ePHI has only three ingredients, confidentiality, integrity, and availability.




The Legal Information Institute states that **confidentiality** refers to who as well as to which process has the authorization to access the ePHI and for which method the data cannot be obtained.

**Integrity** refers to the data preservation with regards to quality (not altered) and quantity (not destroyed) from unauthorized events.

**Availability** speaks to accessibility as well as usability of the ePHI by an authorized person who is requesting it.

## Security Risk Assessment Process

To make an SRA, you need to hire a third-party vendor or perform the following:

1. Outline and describe the scope of the risk analysis, taking into account all the ePHI created, stored, received, as well as transmitted by the organizations. Locations may include 3rd party websites, emails, scans, offline data, etc.
2. Data needs to be collected, from where and how the ePHI originated to its storage, received, maintained, and transmitted.
    - Evaluate and execute past risk analysis
    - Conducting interviews and surveys in various departments
    - Reviewing the organization's policies and procedures

    - Cross-checking technical data
    - Running vulnerability scan
    - Pay an outside consultant to try and hack your system
3. Extend the reach of your methods of recognizing and documenting potential threats and vulnerabilities to ePHI.
4. Assess recent security measures to safeguard ePHI and the thoroughness of adherence. Primary safeguards are:
    - **Administrative safeguards** involve all the policies and procedures that are present to secure ePHI. These include risk analysis and management, assigned security responsibility, workforce security, security awareness training, information access management, contingency planning, security incident procedures, evaluation, business associate contracts, and other arrangements.
    - **Physical safeguards** refer to all the hard measures, policies, and procedures utilized to protect the practice's information from natural threats, environmental hazards, unauthorized access, facility access, workstation use, security, and device controls.
    - **Technical safeguards** are access control, audit controls, integrity controls, authentication, and transmission security. You should perform vulnerability testing, penetration testing, staff awareness tests, comparing your documents to others.
5. Determine the possible damage from an exploited vulnerability. The most significant harm should be assumed possible. Sometimes breaches cannot be controlled, but the level of damage often can be.
6. Determine the likelihood that a threat will occur if the current process is performed by the most vindictive person with the highest clearance or that an unreasonable natural disaster was to happen suddenly. When an adverse event happens, the worst possible outcome is always possible. Not a single practice on the public breach registry ever expected a threat to occur and the impact to be as severe.
7. Determine the risk level of each threat. By combining the chances and impact of threats and vulnerabilities that assists categorize risk as high, medium or low and prioritize how risk is addressed.
8. Produce a document that entails corrective measures to lower the risk (new policy, training staff).
9. Regularly review and update the risk analysis. Each time this occurs, the practice needs to have some formal certification outlining who was involved and what precisely happened. The minimum frequency for a review is annual. Any system-wide changes such as a new EMR or new office should trigger an immediate investigation.

Example:

An SRA is conducted like an interview initially. A standard SRA questionnaire may contain 200 core questions which have approximately 50 conditional questions that follow. Here's an example:

> Question: Who within your practice is responsible for developing and implementing information security policies and procedures?

Answer: The compliance officer is not formally named or otherwise identified in the policy.

Subsequent Questions: Who do people contact for security considerations if there is NO security officer? Who would an auditor speak to regarding an Audit? In your policies and procedures is anyone referenced as a point of contact? Are there any job descriptions related to information security? Who would be your last possible resort if you were forced to present a compliance officer?

That one question which led to numerous other items would create a summary such as this:

| **Section 3, Security & Workforce** | Risk Score: 53 % |
|---|---|
| Threats & Vulnerabilities | Risk Rating |
| Unqualified, uninformed, or lack of Security Officer | |
| Unqualified workforce or untrained personnel on security standards and procedures | Critical |
| Security policies not followed when not enforced | Critical |
| Misuse of audit tools, information systems, and/or hardware | Critical |
| Proliferation of unknown threats | Critical |
| Insider carelessness exposing ePHI | Critical |
| Unauthorized information disclosure (ePHI, proprietary, intellectual, or confidential) | Critical |
| Disruption of business processes, information system function, and/or prolonged adversarial presence within information systems | Critical |


## Conclusion

A Security Risk Assessment may seem like just one more new requirement to impede you from operating a successful medical practice, but it may save your practice just as well. Implementing the Meaningful Use measure about smoking cessation may have seemed like a bother, but the

quantity of smokers has swiftly declined since every doctor started to deliver the same message again and again. The MIPS incentive and value-based reimbursement model was perceived as a burden to practices slowly adopting the platform, but those same practices can see fewer practices and earn significantly more than their non-participating colleagues.

The first security risk assessment you need to consider is:

> Are my practice and my livelihood at risk if I don't have this security assessment performed?

The answer will always be yes. Practices that have violated or are negligent of performing an SRA received a fine higher than the price of having an SRA completed every year that the practice will be active. Breaches in ePHI are not only an embarrassment but cause irreparable finance damage to a practice. Each year, more incentive programs, more Government requirements, more organizations, and even more insurance companies are making a Security Risk Assessment mandatory.