ALTARUM

Security Risk Analysis (SRA)

Why Should I Assess the Security of My Medical Practice?

- Conducting an accurate and thorough security risk analysis is required under MACRA/MIPS, Promoting Interoperability/Meaningful Use, and HIPAA.
- Risks that are not identified and addressed can result in breaches, leading to patient harm, financial costs, and bad publicity.
- With constantly changing technology, emerging threats, and newly discovered vulnerabilities on a daily basis, security today is more challenging than ever before.
- Security in healthcare is in "critical condition" and needs to be improved at all levels, according to a recent U.S. government report.[1]
- 81% of patients are concerned about privacy and security, according to survey data, and many are willing to choose or change providers based on security.[2]
- Your patients are trusting you with their most personal data. Knowledge of your security posture is the first, essential step to keeping their trust, and their legally protected information, secure!

Be Aware of Your Practice's Security with a Security Risk Analysis

What is a Security Risk Analysis?

Security Risk Analysis is not only required under federal law, it is a critical step in ensuring patient safety and a valuable business investment. An accurate and thorough risk analysis critically examines threats and vulnerabilities facing an organizations' patient health information. It includes a complete look at how effectively this legally protected data is secured by the organization. Healthcare organizations that neglect to perform this task are putting their patients at risk and often fail federal compliance audits.

How We Can Help

Start building confidence with your patient base by ensuring their electronic information is protected. A member of the Altarum Quality Improvement Advisory Services (QIAS) Security Risk Analysis team will analyze the risks facing your practice, provide recommendations to improve security as well as the tools necessary to strengthen identified areas of weakness. Our Security Risk Analysis service includes:

- A comprehensive appraisal of your health care organization's information security practices.
- A dedicated Security Consultant to assess your security posture and provide recommendations.
- A summary report listing identified risks and a detailed corrective action plan to remediate risk.
- A security tool kit to assist with administration, staff education, and ongoing security maintenance.
- A set of information security policy and procedure templates based on HIPAA security requirements and industry best practices.

Quality Improvement Advisory Services
Solutions for providers, practices & hospitals

For further information, please contact:

Laura Bumgardner, Program Manager
Quality Improvement Advisory Services | Altarum
Laura.Bumgardner@altarum.org
888-MICH-EHR

[1] "Report on Improving Cybersecurity in the Healthcare Industry." *Health Care Industry Cybersecurity Task Force,* June 2017.

[2] "Third Annual Electronic Health Record Survey." *Xerox Corporation*, May 2012.

Network Security Evaluation

Why Should I Assess the Security of My Network?

Healthcare organizations are targeted by data thieves at an alarming rate: Hacking attacks against healthcare providers increased 320% in 2016.[3]

Theft of medical data is lucrative for criminals and costly for victims. The average cost of a medical record data breach is almost $400 per record to the breached organization, and over $5,000 to each victimized household.[4]

New and cunning threats to ePHI, such as ransomware, are constantly emerging and evolving, finding ways to efficiently exploit greater numbers of targets worldwide.

Any organization, from small medical offices to large healthcare enterprises, could be an easy target that can be seen and exploited by cyber criminals from any point in the world.

Do you know how secure your network is? The Altarum Quality Improvement Advisory Services (QIAS) Security Risk Analysis team can help you find out!

Be Aware of Your Network's Security with a Vulnerability Scan

What is a Vulnerability Scan?

A vulnerability scan surveys your network infrastructure, looking for technical vulnerabilities that hackers could use to gain unauthorized access to your information systems and data. The process yields a summary report that identifies actionable priorities for remediation to improve the security of your network.

Why have a Vulnerability Scan?

Many practice managers are not aware of the weaknesses within their practice's technical infrastructure. Everything in your network, including workstations, software, computing, and storage devices all have vulnerabilities, most of which are known and exploitable by hackers. Knowing the vulnerabilities you have is the first step to defending against their exploitation, getting a step ahead of attackers, and protecting the confidential information used in your practice. You will also be taking a critical step toward meeting the HIPAA requirements for evaluating your technical security.

The Altarum QIAS Security Risk Analysis Team Delivers

The team will produce a customized report for your practice, based on the specific findings of your vulnerability scan. This will be presented to you directly, with your dedicated QIAS Security Consultant available to discuss the results and answer your questions.

Your Security Consultant will help you understand the results, prioritize the most critical areas for your practice to address, and provide recommendations for mitigating identified vulnerabilities.

Upon reviewing the vulnerability scan results, you will have the roadmap for improving the security of your network, including detailed reports, easy-to-navigate summaries, a visual diagram of the scanned devices, and more. Continued vigilance is always necessary to ensure security and compliance on an ongoing basis.

[3] "U.S. Department of Health and Human Services Office for Civil Rights Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information." U.S. Department of Health & Human Services - Office for Civil Rights. N.p., n.d. Web. 19 July 2017.

[4] "Healthcare Cybersecurity Attacks Rise 320% from 2015 to 2016." HealthITSecurity. N.p., 15 Feb. 2017. Web. 19 July 2017.