THE VALUE OF AN INDEPENDENT SRA

Brought to you by: HTAA

WHY IS AN INDEPENDENT SRA NEEDED?

A security risk assessment makes sure your organization is compliant with HIPAA, CMS, and other state required data security and privacy safeguards. More importantly, it will help you identify critical technology risks and validate if your environment is as safe and secure as you think it is.

Healthcare organizations are often overwhelmed by day to day activities to just keeping the IT environment functioning. Performing patch management, keeping up with user accounts, remediating known security vulnerabilities, and reviewing system monitoring data are often postponed or not performed. Yet when IT staff or an outsourced IT vendor is asked by management "Is the organization's data secure?," they will most often say, don’t worry we have it covered.

What we have found in conducting SRAs for over 200 organizations is that often policies are out of date or not followed, and there is little to no evidence that critical data security and compliance procedures are practiced. ***SRAs we have performed uncovered missing policies and procedures, vendors who are not performing critical data security activities, hundreds of unpatched devices, and out-of-date or unsupported software***. Each of these represents an invitation to cyber criminals to hack or ransom these organizations.

Unfortunately, many healthcare organization leaders still end up just hoping everything to do with technology in their organization is fine.

An independently conducted, comprehensive security risk assessment should include a threat analysis, IT document review, risk analysis, vulnerability assessment, physical security walkthrough, report that details critical risk and action items, and a remediation work plan. It should identify critical environmental and human threats, key technology risks, physical security gaps, policies no longer up-to-date, and detail usable policies, procedures and plans, plus outline what key cyber security threats are likely. It should be conducted by an independent party who can be objective and unbiased, as well as constructive and solution focused.

Without this independent assessment, it is unlikely that staff or vendors--who may not want anyone to know what they are not doing--can objectively review and assess themselves.

WILL YOUR SRA HELP YOU FIX THE PROBLEMS?

Your SRA should not just highlight problems, but should also identify solutions and help you develop remediation plans. The process should be as simple and easy as possible, and help you bring together your entire team to understand and address key technology security risks. It should ensure you meet all regulatory requirements, and strengthen not only your security but your compliance as well..

WILL YOUR DATA STAY IN THE U.S.?

Any SRA provider must ensure all work is performed in the U.S. You can't afford to allow your PHI data to be accessed from countries with lax data security rules and enforcement. Or your patients' data could end up on the Dark Web.

Our SRA process is:

- Independent, comprehensive, and focused on helping you effectively address threats & risks
- Quick and easy for your staff--and we are with you every step of the way, providing guidance & support.
- Our legal, IT, audit and clinical expertise ensures environmental, cybersecurity, technology and privacy threats are identified and remediated.
- All our work is performed in the U.S.

CONTACT US

Contact us to make sure your organization is protected and HIPAA compliant.

Visit www.htaalliance.org for more information on our security risk assessment service.

Contact: Carlos Navarro

Email: carlos@htaalliance.org

Phone: 301-200-9776

Address:
11140 Rockville Pike,
Suite 400
Rockville, MD 20852