CLEARWATER COMPLIANCE

30-Minute Guide to Hiring The Best Risk Analysis Company

What to Look for in a HIPAA Risk Analysis Company & Solution

Introduction

We are often asked,

"How do I go about selecting a reputable firm to complete a bona fide Security Risk Analysis that will (a)meet the requirements of HIPAA and Meaningful Use; (b) satisfy the risk analysis component of an OCR Audit, OCR Investigation or CMS Meaningful Use Audit? and, (c) reduce our risks of a breach or investigation?"

This Clearwater Compliance Guide answers that question and provides an easy-to-use Security Risk Analysis Buyer's Guide Checklist to assist you in comparing alternative solutions and making your selection.

Over the years, we have assisted hundreds of customers create their evaluation criteria and make informed decisions about risk analysis solutions. Ultimately, the majority of them chose Clearwater to assist them to complete a comprehensive, bona fide security risk analysis.

Unfortunately, in today's healthcare market, unlike in the insurance marketplace, we do not have an A.M. Best, a Moody's, a Standard and Poor or Weiss Research publishing financial strength ratings on industry players. Nor do we have widely published customer service ratings for risk analysis work by a Powers & Associates in this industry. In fact, as a result, there are many charlatans and Johnny-come-latelies entering the Security Risk Analysis healthcare marketplace--some still spelling HIPAA with two Ps.

At the end of the day, when selecting a risk analysis partner, what you're seeking is ASSURANCE THAT:

- Your risk analysis specifically addresses all the elements a risk analysis must incorporate, as outlined in the HHS/OCR Guidance on Risk Analysis Requirements under the HIPAA Security Rule[1]
- Your risk analysis meets the requirements set out in the most current OCR Audit Protocol on Risk Analysis and Risk Management[2]
- Your risk analysis scope includes all information assets used to create, receive, maintain or transmit ePHI
- Your risk analysis process and reporting facilitates, more informed risk treatment decisions
- All reasonable and appropriate administrative, physical and technical controls are considered
- All relevant threat sources and threat agents for each media type are considered
- All relevant vulnerabilities for each media type are identified and evaluated
- Your risk analysis serves to identify, value and prioritize ALL risks to your information
- You have fast, easy, anytime, anywhere access to your overall risk management posture
- Your business risk management goals are being met
- Your risk analysis meets the CMS requirements for Meaningful Use
- Your risk analysis is being completed by certified information security professionals who have completed hundreds of security risk analyses for Covered Entities and Business Associates.
- Your risk analysis and risk management program actually works; that is, you are making informed decisions to reduce your compliance and cybersecurity risks.

"There are many charlatans and Johnny-come-latelies entering the Security Risk Analysis marketplace."

This guide is explicitly designed to help you navigate through a market where there are new consultants and service providers entering almost every week and simultaneously a growing number failed risk analyses. ePHI is more visible and valuable than ever, and at the same time more vulnerable than ever. To assist you in protecting this sensitive information, we have prepared these evaluation criteria/questions in the form of a due diligence checklist to ask candidate risk analysis partners.

SECURITY RISK ANALYSIS BUYER'S GUIDE CHECKLIST

Your ePHI is more valuable and visible than ever. At the same time, it is more vulnerable than ever. Make sure you hire the right firm that uses a proven, industry-standard methodology to complete a bona fide Security Risk Analysis. Use this HIPAA Risk Analysis Buyer's Guide Checklist to compare alternative solutions and make the best selection.

COMPETENCY – prospective service provider's technical and professional competence and ability to meet your requirements

	CRITERIA	CLEARWATER	VENDOR B	VENDOR C	VENDOR D
1	Will your risk analyses be conducted by qualified information security professionals who have conducted hundreds of Security Risk Analyses for Covered Entities and Business Associates?	✓			
2	Do the individuals performing your risk analysis have industry recognized credentials for understanding the information risk management process and information security requirements such as CRISC, CISSP and/ or HCISPP?	✓			
3	Does your prospective risk analysis solution partner have numerous reference-able customers from your industry segment for whom they have conducted a Security Risk Analysis?	✓			
4	Does your prospective risk analysis solution partner have specific experience with similarly-sized organizations in the same healthcare segment as your organization?	✓			
5	Is your prospective risk analysis solution partner an industry-recognized organization with a solid reputation for its healthcare industry skills, knowledge and experience performing security risk analysis and risk management work?	✓			
6	Has your prospective risk analysis solution partner earned industry awards, endorsements, and 'sole source provider' designations for its risk analysis and risk management work[3]?	✓			
7	Does your prospective risk analysis solution partner have deep healthcare industry experience in HIPAA Privacy, Security and Breach Notification compliance as well as information risk management?	✓			
8	Has your prospective risk analysis service provider's solution been subjected to and passed the scrutiny of OCR Auditors and Investigators, and/or CMS Auditors? If so, how many times?	✓			

CAPABILITY – prospective service provider's use of state-of-the-art technology to assure consistent, measurable, repeatable results

	CRITERIA	CLEARWATER	VENDOR B	VENDOR C	VENDOR D
9	Does the prospective risk analysis solution specifically address the nine (9) essential elements a risk analysis must incorporate as outlined in the HHS/OCR Guidance on Risk Analysis Requirements under the HIPAA Security Rule[4], satisfying both HIPAA and Meaningful Use?	✓			
10	Does the prospective risk analysis solution specifically meet the requirements set out in the OCR Audit Protocol on Risk Analysis[5]?	✓			
11	Does the prospective risk analysis solution provide an interactive, flexible software platform[6] on which you can manage your ongoing risk analysis and risk management program?	✓			
12	Does the prospective risk analysis solution drive workflow order, process, and discipline to your risk assessment and risk management efforts?	✓			
13	Does the prospective risk analysis solution readily and visibly highlight security control deficiencies and risk ratings by media and information asset for management reporting?	✓			
14	Does the prospective risk analysis solution calculate a risk rating for each risk to enable prioritization for risk management decisions?	✓			
15	Does the prospective risk analysis solution identify, value and prioritize ALL risks to your information assets to ensure you may then create a robust, prioritized risk management plan?	✓			
16	Does the prospective risk analysis solution permanently record the baseline for your current security risk profile and your subsequent risk profile as additional controls are implemented, information assets change, and future risk analyses are performed?	✓			
17	Does the prospective risk analysis solution provide for ongoing version management and control such that you can easily provide evidence of all risk analyses completed over the prior six (6) years?	✓			

CRITERIA		CLEARWATER	VENDOR B	VENDOR C	VENDOR D
18	Does the methodology, process and software being considered include key scalable, enterprise capabilities to support report roll-ups and risk analysis cascading? (i.e. Will your solution scale to support security risk analyses for all of your entities (e.g., hospitals, clinics, home health, etc.)	✓			
19	Should you choose to do so, does the prospective risk analysis solution equip and enable you to become self-sufficient and independent of outside, third-party consultants in completing the risk analysis and risk management process periodically as required by the HIPAA Security Rule?	✓			

COMMITMENT – prospective service provider's commitment to the healthcare industry, regulatory requirements and industry standards

CRITERIA		CLEARWATER	VENDOR B	VENDOR C	VENDOR D
20	Is the prospective risk analysis solution provider fully compliant with HIPAA Privacy, Security and HITECH Breach Notification Rules?	✓			
21	Will the prospective risk analysis solution provider sign a HIPAA Business Associate Agreement?	✓			
22	Does the prospective risk analysis solution follow the internationally-recognized standard methodology, cited by OCR, detailed in NIST SP800-30 Guide for Conducting Risk Assessments[7]?	✓			
23	Does the prospective risk analysis solution provide a complete, end-to-end process for including all information assets used to create, receive, maintain or transmit ePHI as required by regulations?	✓			
24	Does the prospective risk analysis process analyze all media that is used to create, receive, maintain or transmit ePHI?	✓			
25	Does the prospective risk analysis solution consider all reasonable and appropriate administrative, physical and technical controls to safeguard ePHI such as those found in NIST SP800-53[8]?	✓			
26	Does the prospective risk analysis solution ensure that all relevant threat sources and threat agents that may exploit vulnerabilities are considered for each asset / media type as required by NIST and other global standards?	✓			

	CRITERIA	CLEARWATER	VENDOR B	VENDOR C	VENDOR D
27	Does the prospective risk analysis solution identify all relevant vulnerabilities in protecting ePHI that should be evaluated for each asset / media type as required by NIST and other global standards?	✓			
28	Does the prospective risk analysis solution provider have a reputation for making a visible, positive contributions to the healthcare industry through white papers, educational events and participation in key industry associations such as AHA, CHIME, AEHIS, AHIA, AHLA and HCCA?	✓			

CUSTOMER SERVICE – prospective service provider's experience in the industry, surveys of customers, processes to ensure and measure customer satisfaction

	CRITERIA	CLEARWATER	VENDOR B	VENDOR C	VENDOR D
29	Does the prospective risk analysis solution provider maintain a formal customer satisfaction process including measurements, timely surveys, annual service and support reviews along with ongoing feedback?	✓			
30	Does the methodology, process and software being offered make it specifically clear what specific, tangible work products are delivered to you as the result of the engagement or use of the tools?	✓			
31	Is the prospective risk analysis solution provider well known in the industry for customer satisfaction?	✓			
32	Can the prospective risk analysis solution provider provide you with customer references regarding customer service, its customer community and any customer forums it facilitates?	✓			
33	Does prospective risk analysis solution provider offer free, unlimited and immediate ongoing support from information security professionals to help you throughout the security risk management process?	✓			
34	Is the methodology, process and software being considered transparent such that you are aware of specific work and/or activity that is being performed at every stage and every time period?	✓			
35	Does the prospective risk analysis solution provider's methodology, process and software make it specifically clear who will be supporting you to on a regular basis and how you will communicate?	✓			

Health Care Information Privacy, Security, Compliance and Risk Management Solutions from Clearwater Compliance LLC have earned the exclusive endorsement of the American Hospital Association.

[1] http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalintro.html
[2] http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html
[1] https://clearwatercompliance.com/company-news/senior-vp-of-the-american-hospital-association-praises-clearwater-solutions/
[4] http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalintro.html
[5] http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html
[6] https://clearwatercompliance.com/shop/product-category/compliance-software/
[7] http://csrc.nist.gov/publications/drafts/800-30-rev1/SP800-30-Rev1-ipd.pdf
[8] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

---

Clearwater Compliance LLC

Phone: 800-704-3394
Web: http://www.clearwatercompliance.com
Email: info@clearwatercompliance.com
Twitter: @ClearwaterHIPAA

About Clearwater Compliance LLC

Clearwater Compliance, LLC, helps hospitals, health systems and their business associates improve patient safety and quality of care by assisting them establish, operationalize and mature their compliance and cybersecurity programs. Led by veteran, C-suite health care executives, Clearwater's award-winning software, educational events and expert professional services provide scalable, cost-effective solutions for all sizes of organizations. Since 2009, the company has served hundreds of clients ranging from major health systems, hospitals, health plans and Fortune 100 companies, to medical practices and health care startups.

Find out more about Clearwater's compliance, cybersecurity and information risk management solutions at clearwatercompliance.com

IRM | Analysis™
Identify and Manage Priority Privacy and Security Risks

To learn more about our risk analysis solutions, visit:
https://clearwatercompliance.com/

For more information please contact:
Dan Pruyn
VP, Business Development
(615) 678-0370
800 704 3394
dan.pruyn@ClearwaterCompliance.com