Risk Analysis vs Risk Assessment

In discussions regarding HIPAA and risk determinations, each phrases “risk analysis” and also “risk assessment” are occasionally used correspondently. But bear in mind, according to HIPAA there is a difference between these phrases. Like many things under HIPAA, each and every single phrase possesses its own specific meaning and precision should be taken when applying or making reference to obligations. Each makes reference to a distinct requirement for covered entities and business associates under HIPAA.

The confusion that these phrases can produce is actually pervasive amongst individuals who deal with HIPAA. The difference was actually the topic of a debate on a medical lawyer listserv which I subscribe to. The fact that lawyers who actually focus their particular practices on HIPAA considered the necessity to debate the difference demonstrates the shortage of clarity in addition to the significance and need to carefully evaluate the differences.

Risk Analysis vs Risk Assessment

Under the HIPAA Security Rule, a “risk analysis” requires entities to “*conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate*.” 45 CFR § 164.308(a)(1)(ii)(A). The risk analysis is actually a required element for entities to perform in complying with HIPAA. While the definition of the risk analysis sets forth, the goal is to identify vulnerabilities and weaknesses in an entity’s systems. This in turn will assist the development of the entity’s security policies and procedures, which happens to be the next step in complying with the requirements of the HIPAA Security Rule. Accordingly, a risk analysis is an element of the compliance process.

By contrast, “risk assessment” presents itself in the HIPAA regulations under the definition of “breach” in the Breach Notification Rule. 45 CFR § 164.402. More specifically, a risk assessment is precisely what an entity must perform in an effort to determine whether there is a low probability that protected health information has been jeopardized, which informs whether or not the breach notification

6627 Valjean Ave.
Van Nuys, CA 91406
Phone: +888-959-0220
Fax: +818-356-7187
Email: info@camhipaasolutions.com
Website: www.camhipaasolutions.com

requirements will come into play. As set forth in the definition of a breach, a risk assessment consists of, at least, the following four elements: (i) the nature and extent of protected health information involved, (ii) the identity of the unauthorized person that accessed the protected health information, (iii) whether the protected health information was actually acquired and/or viewed, and (iv) the extent to which the risk to the protected health information has been mitigated.

As the regulating definitions show, both the requirements and framework concerning a risk analysis and a risk assessment vary. A risk analysis is an essential initial and ongoing action in establishing an entity's security policies, whereas a risk assessment is conducted to determine whether a violation of protected health information will be subjected to reporting requirements.

Whenever terms concerning art are created, they should be followed. Failure to consider the meaning attached to terms of art can easily lead to non-compliance or causing confusion. From a legal understanding, if a term of art is developed, then the meaning and requirements associated with that term will be brought up, even if the context is not right. Therefore, in the HIPAA context, carefully consider what needs to be done when stating whether a "risk analysis" or "risk assessment" is exactly what needs to occur. One sees an overarching assessment of an entity whereas the other is done in response to a suspected breach.

Hopefully this explanation was helpful in understanding the difference between a Risk Analysis vs Risk Assessment.

Feel free to give CAM HIPAA Solutions a call for any questions that you may have.

6627 Valjean Ave.
Van Nuys, CA 91406

Phone: +888-959-0220
Fax: +818-356-7187

Email: info@camhipaasolutions.com
Website: www.camhipaasolutions.com