Risk Analysis *versus* Risk Assessment

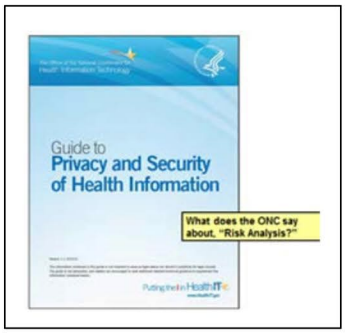
tw Security
Healthcare Information Security

Assessment – A judgment about something based on an understanding of the situation; a method of evaluating performance [high-level]

Analysis – The close examination of something in detail in order to understand it better or draw conclusions from it; the separation of something into its constituents in order to find out what it contains, to examine individual parts, or to study the structure of the whole [detailed]
Source: Encarta Dictionary

Risk Analysis – A systematic and ongoing process of identifying **threats**, **controls**, **vulnerabilities**, **likelihood** (or probability), **impact**, and an overall **rating of risk** *(If any of these steps (words) are missing – it's not a risk analysis.)*

Unfortunately, the federal government and others use the word "assessment" to often mean "analysis" which only adds confusion. This is something we commonly do in language. We refer to any gelatin dessert as "Jello," although it could be a different brand. We do the same with "Coke" and "Kleenex."



"Your first comprehensive security risk analysis should follow a systematic approach that covers all security risks. It should:

- Identify where ePHI exists …
- Identify potential threats and vulnerabilities …
- Identify risks and their associated levels (e.g., high, medium, low)"

(Guide to Privacy and Security of Electronic Health Information April 2015, pages 41 and 42)

HIPAA Security Rule - §164.308(a)(1)(ii)(A) Risk analysis *(Required)*
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].

Meaningful Use – Stage 1
Objective: *Ensure adequate privacy and security protections for personal health information*
Measure: *Conduct or review a security risk analysis in accordance per 45 CFR 164.308 (a)(1) and implement security updates as necessary and correct identified security deficiencies as part of its risk management process.*

Meaningful Use – Stage 2
Objective: *Protect electronic health information created or maintained by the Certified EHR Technology through the implementation of appropriate technical capabilities*
Measure: *Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1), including addressing the encryption/security of data at rest in accordance with requirements under 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 EP's risk management process.*

6108 W. 121st Street, Overland Park, KS 66209 I (o) 913-696-1573
CustomerCare@tw-Security.com I www.tw-Security.com