HEALTH
COMPLIANCE
PARTNERS

Comparison of HIPAA Security Compliance-Risk Assessment to Meaningful Use 15 Risk Analysis

By Ernie Hassell
Health Compliance Partners
July 2012

Abstract

This document presents a comparison of HIPAA Security Compliance-Risk Assessment to a Meaningful Use 15 Core Requirement Risk Analysis. HIPAA, ARRA-HITECH and Meaningful Use Core Measure 15 are contrasted. A summary and glossary is provided.

The content of this document is limited in scope and is not intended to be an exhaustive discussion about the subject area. The information presented is based on our experience in the healthcare industry and Risk Management, Risk Analysis, Risk Assessment of networks, systems and software.

Comparison of HIPAA Security Compliance-Risk Assessment to Meaningful Use 15 Risk Analysis

"Information is the lifeblood of modern medicine; health information technology is destined to be its circulatory system."
David Blumenthal, National Coordinator for Health Information Technology

Foreword

The list of terms and perceived definitions is seemingly endless. Risk Assessment? Risk Analysis? Compliance Assessment? Is it really compliance or is it simply conformance? Confusion continues to swirl around the differences among these terms. For the purposes of this paper, the emphasis is on comparing and contrasting HIPAA Security Compliance-Risk Assessment against Meaningful Use Core Requirement 15, Protecting Electronic Health Information. To provide the reader with meaningful use of this paper, it is first necessary to first wade into the regulatory waters and navigate through a basic description of HIPAA, ARRA-HITECH, and Meaningful Use regulations.

Introduction

This document is not intended to be an all-topic treatise on HIPAA Security and Meaningful Use 15. Terminology used in both of these regulations also varies somewhat, making interpretation a topic for ongoing discussion. Respect for the adage of 'the document speaks for itself' must constantly be kept in mind.

What this document is intended to provide is a basic description of key regulations and compare and contrast a HIPAA Security Compliance-Risk Assessment and a Meaningful Use 15 Risk Analysis. This paper provides reference to National Institute of Standards and Technology (NIST) guidance with respect to risk and analysis and assessment. It also provides guidance with respect to engaging consulting services when needing to comply with these regulations.

Background

Collectively, HIPAA, ARRA-HITECH and Meaningful Use regulations exist within the Code of Federal Regulations (CFR). The CFR contains the code of the general and permanent rules and regulations published in the *Federal Register* by the executive departments and agencies of the federal government. The combined CFR contains 50 broad topic areas. For discussion purposes, these 50 could be thought of as 50 volumes, or more precisely Titles, on a library shelf, with each Title having been assigned its own reference number.

Each of the regulations discussed in this paper exist within Title 45 of the CFR, Public Welfare.

As with any Title (or book), subtitles and subchapters are used to capture and convey the regulation.   So HIPAA Rules and Scope (broadly termed Administrative Simplification) is located within Subtitle A, Subchapter C of 45CFR160. HIPAA Security is located within 45CFR164.306 – 316. Privacy, as it relates to HIPAA, is more distributed, and is located across sections of 45CFR160 and 164. Privacy is also a topic that has been regulated earlier than security and is embedded in the Federal Privacy Act within the United States Code (USC). Discussion of it at that level is beyond the scope of this paper. HITECH (ARRA) is located within 45CFR164.412. Note too that cross reference to other regulations does occur within these cited regulations.

HIPAA was enacted before ARRA-HITECH and Meaningful Use. It is appropriate to explain its relevance to our discussion, and to keep in mind that as time passes, regulations change. HIPAA is no exception. Since the inception of HIPAA in 1996, modifications to the rules have been made. Other regulations have been 'dove-tailed' into HIPAA, such as HITECH. Now Meaningful Use Core Requirement 15, Privacy and Security of protected health information, relies upon HIPAA for foundation.

HIPAA – Health Insurance Portability and Accountability Act

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was enacted by Congress and signed into law on August 21, 1996. HIPAA consists of 5 Titles. Title 2, Administrative Simplification, requires the establishment of national standards for electronic health care transactions and national identifier for providers, health insurance plans, and employers. It is also under Title 2 that Security is embodied.

Within the context of this paper, Title 2 Administrative Simplification provisions touch each of the above cited regulations. One in particular, 45CFR164.306 is a key standard as it sets a foundational scope and requirement directly affecting the security and privacy of health related data. This 164.306 standard can be likened to standard rules. It addresses Confidentiality, Integrity and Availability (security); flexibility of approach, standards, implementation specification and maintenance.

Generally stated, the combined goal of each of the HIPAA standards is meant to improve the efficiency and effectiveness of the nation's health care system by encouraging the widespread use of electronic data interchange.

Administrative Simplification and the HIPAA Security Rule

The Final Rule on Security Standards was issued on February 20, 2003. It became effective on April 21, 2003 with a compliance date of April 21, 2005 for most covered entities and April 21, 2006 for "small plans”. The Security Rule complements the Privacy Rule. While the Privacy Rule pertains to all Protected Health Information (PHI) including paper and electronic, the Security Rule specifically addresses Electronic Protected Health Information (e-PHI).

The rule established administrative, physical, and technical safeguard (protection) requirements. Each standard within the Rule identifies various security safeguards that are to be in place. Each standard is further categorized as required or addressable. Within the context of HIPAA, 18 standards exist. Note that a similar approach was applied to Meaningful Use where the terms core and menu are applied. More about that topic is provided under Meaningful Use.

With respect to Required and Addressable specification, the following is offered. Required is simply that; a required rule is one that is mandated and must be in place (and working!). Addressable specifications are more flexible, enabling the individual entities to evaluate their own situation and determine whether or not to adopt one or more of the addressable rules. It must be noted that should an entity decide against implementing an addressable rule, they must document the reasoning and acceptance of associated risk. A form similar to a waiver may assist in this area.

It must be stressed that simply having policies and procedures is not adequate to meet compliance. They must be followed and following them must be accomplished in a manner that is ideally well documented and traceable.

HIPAA security rule categorically addresses safeguards. Safeguards are precautionary measures. By category, Administrative, Physical and Technical safeguards are defined in the rules.

- ***Administrative Safeguards*** – policies and procedures designed to clearly show how the entity will comply (and does comply) with HIPAA:
    - Covered entities (entities that must comply with HIPAA requirements) must adopt a written set of privacy procedures and designate a privacy officer to be responsible for developing and implementing all required policies and procedures.

  - The policies and procedures must reference management oversight and organizational buy-in to compliance with the documented security controls.
  - Procedures should clearly identify employees or classes of employees who will have access to electronic protected health information (e-PHI). Access to e-PHI must be restricted to only those employees who have a need for it to complete their job function.
  - The procedures must address access authorization, establishment, modification, and termination.
  - Entities must show that an appropriate ongoing training program regarding the handling of PHI is provided to employees performing health plan administrative functions.
  - Covered entities that out-source some of their business processes to a third party must ensure that their vendors also have a framework in place to comply with HIPAA requirements (Business Associates Agreement). Companies typically gain this assurance through clauses in the contracts stating that the vendor will meet the same data protection requirements that apply to the covered entity. Care must be taken to determine if the vendor further out-sources any data handling functions to other vendors and monitor whether appropriate contracts and controls are in place.
  - A contingency plan should be in place for responding to emergencies. Covered entities are responsible for backing up their data and having disaster recovery procedures in place. The plan should document data priority and failure analysis, testing activities, and change control procedures.
  - Internal audits play a key role in HIPAA compliance by reviewing operations with the goal of identifying potential security violations. Policies and procedures should specifically document the scope, frequency, and procedures of audits. Audits should be both routine and event-based.
  - Procedures should document instructions for addressing and responding to security breaches that are identified either during the audit or the normal course of operations.

- ***Physical Safeguards*** – controlling physical access to protect against inappropriate access to protected data
  - Controls must govern the introduction and removal of hardware and software from the network. (When equipment is retired it must be disposed of properly to ensure that PHI is not compromised.)
  - Access to equipment containing health information should be carefully controlled and monitored.

  - Access to hardware and software must be limited to properly authorized individuals.
  - Required access controls consist of facility security plans, maintenance records, and visitor sign-in and escorts.
  - Policies are required to address proper workstation use. Workstations should be removed from high traffic areas and monitor screens should not be in direct view of the public.
  - If the covered entities utilize contractors or agents, they too must be fully trained on their physical access responsibilities.

- ***Technical Safeguards*** – controlling access to computer systems and enabling covered entities to protect communications containing PHI transmitted electronically over open networks from being intercepted by anyone other than the intended recipient.
  - Information systems housing PHI must be protected from intrusion. When information flows over open networks, some form of encryption must be utilized. If closed systems/networks are utilized, existing access controls are considered sufficient and encryption is optional.
  - Each covered entity is responsible for ensuring that the data within its systems has not been changed or erased in an unauthorized manner.
  - Data corroboration, including the use of check sum, double-keying, message authentication, and digital signature is recommended to help ensure data integrity.
  - Covered entities must also authenticate entities with which they communicate. Authentication consists of corroborating that an entity is who it claims to be. Examples of corroboration include: password systems, two or three-way handshakes, telephone callback, and token systems among others.
  - Covered entities must make documentation of their HIPAA practices available to the government to determine compliance.
  - In addition to policies and procedures and access records, information technology documentation should also include a written record of all configuration settings on the components of the network because these components are complex, configurable, and always changing.
  - Documented risk analysis and risk management programs are required. Covered entities must carefully consider the risks of their operations as they implement systems to comply with the act. (The requirement of risk analysis and risk management implies that the act's security requirements are a minimum standard and places responsibility on covered entities to take all

reasonable precautions necessary to prevent PHI from being used for non-health purposes.)

Admittedly, interpretation of these requirements is frequently topic of discussion. To better help in this area, it is recommended that two other safeguards be added; one considered 'Operational' and the other, 'Best Practices.' Administrative, Physical and Technical could be considered grass roots while 'forest' level perspective should add Operational and Best Practices safeguards. Additional details concerning these safeguards are in the Conclusions section of this paper.

ARRA-HITECH
ARRA - AMERICAN RECOVERY AND REINVESTMENT ACT (ARRA) and the HITECH - HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH ACT (HITECH)

The American Recovery and Reinvestment Act (ARRA) is officially Public Law 111-5 signed on February 17, 2009. Within 45CFR164.412, Title XIII of ARRA was given the subtitle of the *Health Information Technology for Economic and Clinical Health Act* or HITECH. It is this section that deals with many health information communication and technology provisions as well as other related items. In many respects, HITECH could be thought of as an act primarily focused on closing gaps, expanding security and privacy coverage, and increasing penalties that were not adequately addressed within HIPAA.

Subtitle D of HITECH addresses the privacy and security concerns associated with the electronic transmission of health information. HITECH requires HIPAA covered entities to report data breaches affecting 500 or more individuals to Health and Human Services (HHS) and the media, in addition to notifying the affected individuals.

Interpretation of when it's necessary to report a breach is difficult. Language is used in the act that specifies "jurisdictions" (as a boundary). Jurisdictions are defined at the state level. The number of persons living within a jurisdiction whose data were breached also comes into play. This issue of breach and not having to report a breach is quite simply handled by encrypting the sensitive (e-PHI) data. There is a clause in the act that negates the need to report a breach if the data were encrypted.

HITECH also extends the complete Privacy and Security Provisions of HIPAA to business associates of covered entities. This includes the extension of newly updated civil and criminal penalties to business associates. These changes are also required to be included in any business associate agreements with covered entities. Penalties for violations vary. Under the old act (prior to HITECH), $25,000.00 per violation was the maximum. Under HITECH, that has been raised to $150,000.00.

Another significant change brought about in Subtitle D of the HITECH Act, is the new breach notification requirements. This imposes new notification requirements on covered entities, business associates, vendors of personal health records (PHR) and related entities if a breach of unsecured protected health information (e-PHI/PHI) occurs. For this purpose, a Business Associates Agreement (BAA) comes into play. The parent party that engages the secondary party for whatever purpose that provides that secondary party e-PHI/PHI to store, process, transmits or destroys PHI or e-PHI must be under a BAA.   Due to the complexities associated with BAA documents, the need for engaging a good healthcare attorney to respond to a BAA being provided or received is recommended.

Breach notification is also a key element in HITECH. Breach is a major issue, and the regulators take it seriously. Breach could be simply defined as a gap; a preverbal hole in the wall of security. As it relates to security, forensic analysis of a breach is requisite. An incident response plan is necessary to address this area.

HITECH also reduced the required timeframe for disclosing “requirements to information used to carry out treatment, payment….when using an EHR.” This new requirement limits the timeframe for the accounting to three years instead of six as it previously stood.

Meaningful Use

Another component of HITECH set the goal for Meaningful Use (MU) of interoperable Electronic Health Records (EHR) adoption in the health care system. HITECH established MU as a critical national goal and accordingly, incentivized EHR adoption. To be clear, the goal is not EHR adoption alone, but Meaningful Use of the adopted EHR and its clinical informatics capability. It is this MU that is planned to help providers achieve significant improvements in care.

Scope of Meaningful Use – Core and Menu Items

Attesting to Meaningful Use compliance promises maximum incentive payments for entities providing Medicaid billable services for those who adopt and use "certified EHRs". The maximum amount that may be received is $63,750 over 6 years provided use and attestation began in 2011. Eligible professionals must begin receiving payments by 2016 to qualify for the program. For Medicare the maximum payments are $44,000 over 5 years. To receive the EHR stimulus money, the HITECH act (ARRA) requires entities to show "meaningful use" of an EHR system. Note too that eligible amounts vary and specific dates are set for use and attestation definition purposes. Early adopters receive more incentives.

The Health Information Exchange (HIE) has emerged as a core capability for hospitals and physicians to achieve "meaningful use" and receive stimulus funding. HIE design and implementation state of HIE systems varies across the United States. This is in part due to the US Government providing limited standards with respect to design of the HIE. Consequently, no unified record-to-record transfer standard exists today of the HIE systems. This further compounds information exchange as well as the security and privacy of the information exchange issues. Healthcare system vendors use the HIE as a way to enable EHR systems to pull disparate data and function most typically on an interoperable local level, for example within the hospital. At the national level it compounds issues that are in process of being resolved.

Starting in 2015, hospitals and doctors will be subject to financial penalties under Medicare if they are not using EHR systems. Entities who do not adopt an EHR by 2015 will be penalized 1% of Medicare payments, increasing to 3% over 3 years. Similar penalty under Medicaid should also be presumed.

What is "Meaningful" within Meaningful Use?

So what really is meaningful use within the context of Meaningful Use? It is considered to be one or more of the following examples:

- The use of a certified EHR in a meaningful manner, such as e-prescribing.
- The use of certified EHR technology for electronic exchange of health information to improve quality of health care.
- The use of certified EHR technology to submit clinical quality and other measures.

Consequently, providers need to show and to attest to using certified EHR technology in ways that can be measured significantly in quality and in quantity.

In short, Meaningful Use was designed to:

- Improve care coordination

- Reduce healthcare disparities
- Engage patients and their families
- Improve population and public health
- Ensure adequate privacy and security

The full scope of Meaningful Use is being accomplished in phases, just as HIPAA was implemented in Privacy and Security stages. Meaningful Use is being implemented in three stages, with the last stage to occur in 2015. Stage 1 language and requirements has been finalized and continues to be implemented in the field; Stage 2 has been defined, however, not finalized. Stage 3 is still in formative development.

Meaningful Use Stage 1

The first steps in achieving meaningful use are to have a certified electronic health record (EHR) and to be able to demonstrate that it is being used to meet the MU requirements. In stage 1, entities were required to meet 15 core measures and five optional menu measures.

In total, Stage 1 contains 25 measures for Eligible Providers (EPs) and 24 measures for eligible hospitals. The measures have been divided into two sets; a core set and menu set. EPs and eligible hospitals must meet all measures in the core set (15 for EPs and 14 for eligible hospitals). EPs must meet 5 of the 10 menu-set items during Stage 1, one of which must be a public health objective.

Meaningful Use Stages 2 and 3

Both of these stages are a work in progress and continue to be a hot topic of discussion. At the time this paper was being written, Stage 2 continues to be discussed and argued. A ruling and final wording would need to come before August 2012 to provide sufficient time for entities to be able to comply with the proposed 2014 'on-line-and-operational' date.

With respect to Stage 3, let's get through Stage 2 first!

Meaningful Use Core and Menu Requirements

Core Requirements:

1. Use computerized order entry for medication orders.
2. Implement drug-drug, drug-allergy checks.
3. Generate and transmit permissible prescriptions electronically.
4. Record demographics.
5. Maintain an up-to-date problem list of current and active diagnoses.

6. Maintain active medication list.
7. Maintain active medication allergy list.
8. Record and chart changes in vital signs.
9. Record smoking status for patients 13 years old or older.
10. Implement one clinical decision support rule.
11. Report ambulatory quality measures to CMS or the State/s.
12. Provide patients with an electronic copy of their health information upon request.
13. Provide clinical summaries to patients for each office visit.
14. Capability to exchange key clinical information electronically among providers and patient authorized entities.
15. **Protect electronic health information (privacy & security)**

Menu Requirements:

1. Implement drug-formulary checks.
2. Incorporate clinical lab-test results into certified EHR as structured data.

3. Generate lists of patients by specific conditions to use for quality improvement, reduction of disparities, research, and outreach.
4. Send reminders to patients per patient preference for preventive/ follow-up care

5. Provide patients with timely electronic access to their health information (including lab results, problem list, medication lists, allergies)
6. Use certified EHR to identify patient-specific education resources and provide to patient if appropriate.
7. Perform medication reconciliation as relevant
8. Provide summary care record for transitions in care or referrals.
9. Capability to submit electronic data to immunization registries and actual submission.
10. Capability to provide electronic syndromic surveillance data to public health agencies and actual transmission.

Regulatory Summary

The United States Code relative to Privacy really sets foundation for each of the regulations cited in this paper. As a healthcare security practitioner, I'll give HIPAA credit for what it has achieved. I'll also give credit to the United States Code for setting the privacy foundation. In the decades between it and HIPAA, other regulations came into play. Clearly, HIPAA set the gold standard and HITECH borrowed from it to achieve Meaningful Use goals. It's a triad, a three legged stool.

So let’s borrow from the legs and construct a view of this paper’s subject, comparing a HIPAA Security Compliance-Risk Assessment against a Meaningful Use 15 Risk Analysis.

Risk Assessment and Risk Analysis

Evaluation of risk involves making assumptions and identifying uncertainties and clearly considering and presenting them. Part of the difficulty in risk management is that measurement of two of the quantities in which risk assessment is concerned - potential loss and probability of occurrence - can be very difficult. Subjective is the operative word. How many foresaw the likelihood of 9-11 occurring?

The chance of error in measuring either of these two in a compliance assessment or risk analysis is always at play. Materialized risk with a large potential loss and a low probability of occurring is often treated differently from the probability of risk materialization with a low potential loss and a high likelihood of occurring. In theory, both are of nearly equal priority, but in practice it can be very difficult to gauge as well as to manage when faced with scarcity of resources, especially finances and time.

Technically, when it comes to regulatory compliance of any type, three types of assessments may be completed:

1. Compliance Assessments answers questions such as: “Where do we stand with respect to the regulations?” and “How well are we achieving ongoing compliance?”
2. Risk Assessments (Analysis in HIPAA parlance) answers questions such as: “What is our risk exposure to information assets (e.g., PHI and e-PHI)?” and “What do we need to do to mitigate risks?”
3. Readiness Assessments answer questions such as: “Have we implemented adequate security and privacy safeguards?” Are we ready for an audit?

HIPAA Security Compliance-Risk Assessment

A thorough HIPAA Security Compliance Analysis broadly covers all aspects of the security portion of the act including all 18 Standards and 42 implementation specifications that comprise the Administrative, Physical and Technical Safeguards (CFR 164.308, 310, 312). Additionally, this analysis would cover CFR 164.314 and 316 related to Organizational Requirements, Policies and Procedures and Documentation. This type of analysis is a critical step and should be completed whether one is just starting a HIPAA Security Compliance program or rejuvenating one. The output of the work establishes a baseline against which overall progress can be measured by the executive team, compliance or risk officer, audit committee or board.

At the end of such an assessment, the deliverable should categorically cite each of the 18 standards and 42 implementation specifications. It should also report on related organizational requirements and Policies and Procedures documentation. Ideally, it should also factor in 'Operational' safeguards and industry best practices. It should also be considerate of Required versus Addressable.

HIPAA and Meaningful Use 15 – Common Ground

Both HIPAA and Meaningful Use 15 require a Security Risk Analysis. The implementation standard (subset) is referenced below:

A HIPAA Security Risk Analysis (§164.308(a) (1) (ii) (A)) is required by law to be performed by every Covered Entity and Business Associate. Additionally, completion of the Risk Analysis is a core requirement to meet Meaningful Use 15 requirements. Section 164.308(a) (1) (ii) (A) of the HIPAA Security Final Rule also states:

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 [organization].

Meaningful Use 15 Risk Analysis

As required by the HITECH Act, the Office of Civil Rights has issued final "Guidance on Risk Analysis Requirements under the HIPAA Security Rule". This guidance was published on July 8, 2010. The Office for Civil Rights (OCR) is responsible for issuing annual guidance on the provisions in the HIPAA Security Rule. The intent is to assist organizations in identifying and implementing the most effective and appropriate administrative, physical, and technical safeguards to secure electronic protected health information (e-PHI).

No specific methodology is indicated in that guidance, however it does describe nine (9) essential elements that a Risk Analysis must incorporate. Conforming to these 9 essential elements applies *regardless* of the risk analysis methodology employed. [We have designed a Risk Analysis methodology and tool kit that encompasses these elements with industry best practices]. The 9 essential elements of the Risk Analysis conform to NIST 800-30 with consideration for NIST 800-66. Further, OCR makes explicit recommendation concerning the use of NIST for guidance in performing this analysis.

Conducting a risk analysis is the first step in identifying and implementing safeguards that comply with and carry out the standards and implementation specifications in the Security Rule. A risk analysis is foundational. It's important to note too that even with what the OCR has provided with respect to guidance, it's not intended to provide a one-size-fits-all blueprint for compliance. What it does help to do is to clarify the expectations for meeting requirements. Perhaps most importantly, one must take into account the characteristics and organization of the environment as well as its size. A Risk Analysis is required; however, the safeguards are categorized as Required or Addressable.

The Importance of NIST

The National Institute of Standards and Technology (NIST), is a federal agency that publishes freely available material in the public domain, including guidelines. Although only federal agencies are required to follow guidelines set by NIST, the guidelines represent the industry standard for good business practices with respect to standards for securing e-PHI.

So, when it comes to HIPAA Security Compliance-Risk Assessment, think:

- Terminology – industry parlance for a HIPAA Security Compliance-Risk Assessment must include a risk analysis. And ideally, that risk analysis follows the guidance provided by NIST. Two NIST documents may be referenced for the analysis process, NIST 800-30 and NIST 800-66. Warning: NIST publishes many documents and it's very easy to get off track with choosing the right one.
- Overall compliance with the HIPAA Security Final Rule. This includes the implementation requirements for a contingency plan (Disaster Recovery Plan) as well as an Incident Response Plan.
- Establishing a baseline assessment for measuring progress. This involves the creation (if one doesn't already exist) of an ongoing Risk Register. The Register should capture the identified findings as a result of analysis that are being or are planned to be remediated. Auditors look for this register during audits.
- Asking: Have we documented appropriate policies and procedures? This is the largest single gap that we encounter. Typically, these documents don't exist, are out of date, or really aren't policies but are procedures. This is a hot button with auditors.
- Ask: Are we performing against our policies and procedures?

When it comes to HIPAA Security Risk Analysis, think:

- Every device (including all bio-medical devices beyond the normal user computers, fax machines, such as an MRI/CT-Scan and all mobile devices such as smart phones, iPads and similar that store, process, transmit or destroy e-PHI). Determine the view of each information asset with e-PHI
- Meeting a specific step in the overall compliance process
- Understanding implementation specifications in addition to current safeguards and controls in place
- Asking: What are our specific risks and exposures to information assets?
- Asking: What do we need to do to mitigate these risks?
- Asking: Who is tracking residual risk and how is it being managed and documented?
- Asking: What are we reporting to the board or supervisory committee about security, compliance and risk management on at minimum a quarterly basis? Are the meeting minutes capturing the full scope of discussions at this level?

The HIPAA Security Compliance-Risk Assessment combined with the HIPAA Security Risk Analysis are important and necessary steps on the HIPAA HITECH Security compliance journey.

Summary

A thorough HIPAA Security Risk-Compliance Assessment must address the 18 HIPAA Standards and 42 HIPAA Implementation Specifications. Performing the Risk Analysis based on NIST guidance is strongly recommended, as in the event of an audit, the results will show if this Risk Analysis requirement will have been met.

Unlike HIPAA, a Meaningful Use 15 Risk Analysis using the same NIST guidance is much less rigorous than a HIPAA Security Risk-Compliance Assessment and by no means ensures overall HIPAA compliance.

Anyone wishing to be fully compliant must ensure that the analysis or assessment performed encompasses all 18 HIPAA Standards and 42 Implementation Specifications in accordance with NIST guidelines.

GLOSSARY

Ask a group of people what the difference between a risk analysis and a risk assessment is and you'll get a variety of answers. For discussion sake, the following applies to this paper:

Contingency Plan A plan for emergency response, backup operations, and post disaster recovery in a system, as part of a security program, to ensure the confidentiality, integrity and availability of mission critical system resources and facilitate continuity of operations in a crisis.

Risk Analysis – The systematic use of information to identify sources and to estimate risk.   Risk analysis provides a basis for risk evaluation, risk treatment, and risk disposition. NIST 800-30 embodies this structure.

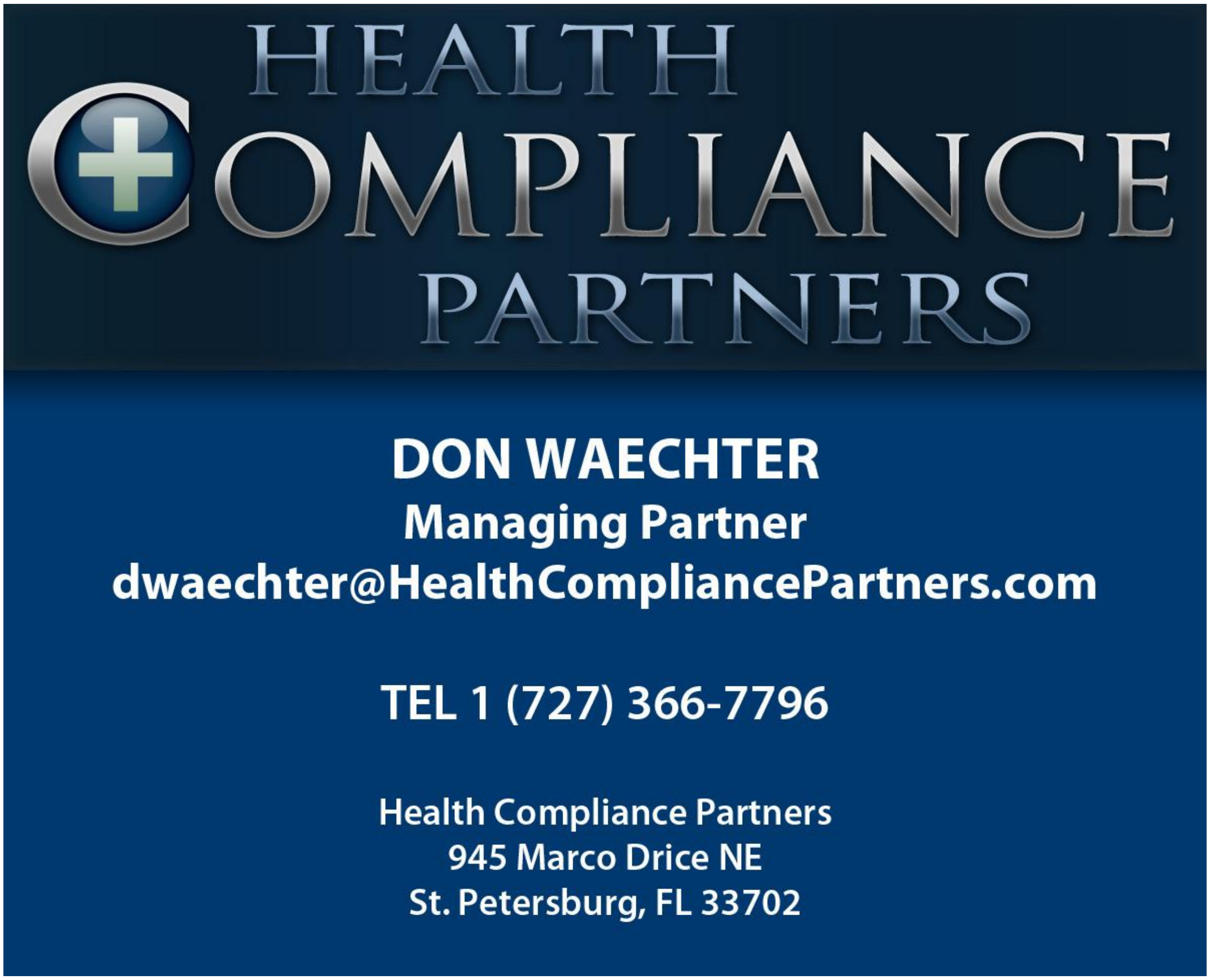
Risk Assessment is a step in a risk management plan or procedure. Risk assessment is the determination of quantitative or qualitative value of risk related to a situation and one or more recognized threats (also called hazards).

Risk Management The process distinct from risk assessment of weighing policy alternatives in consultation with interested parties that considering risk assessment and other legitimate factors, and selecting appropriate prevention and control options.

Threat Any circumstance or event with the potential to adversely impact an asset through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.

Questions or Comments

Please let us know what you thought about this article. Health Compliance Partners tries to bring what is thought to be relevant, timely and user beneficial information to market. Your insight is appreciated. Please contact:



HEALTH
COMPLIANCE
PARTNERS

DON WAECHTER
Managing Partner
dwaechter@HealthCompliancePartners.com

TEL 1 (727) 366-7796

Health Compliance Partners
945 Marco Drice NE
St. Petersburg, FL 33702

Health Compliance Partners
945 Marco Drive NE
St. Petersburg, FL
33702
Produced in the USA
07-12

Health Compliance Partners makes no representation or warranty regarding third party product or service including those under other names or designations.

Health Compliance Partners, the Health Compliance Partners logo, Compliance with Assurance, and Compliance Guardian are trademarks of Health Compliance Partners, LLC, in the United States and/or other countries.

All products referenced may be trademark registered or trademarks of their respective company.

Information about products is obtained from the manufacturers of those products or their published announcements. Health Compliance Partners has not tested those products and cannot confirm the performance, compatibility, or any other claims related to these products. Questions on the capabilities of products should be addressed to the suppliers of those products. Therefore, no assurance can be given that any system or individual user will achieve regulatory compliance or conformance equivalent to those stated herein.

Health Compliance Partners reserves the right to change specifications or other product information without notice.

Health Compliance Partners PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions.