McDermott Will & Emery

On the Subject

May 2, 2018

The Continuing Disconnect between the Health Care Industry and OCR on HIPAA's Risk Analysis Requirement

David Quinn Gacioch, Edward G. Zacharias, Amy C. Pimentel

The HIPAA Security Rule has long required every Covered Entity (CE)—and since September 2013, every Business Associate (BA)—to conduct a Risk Analysis.[1] And yet, lack of a sufficient Risk Analysis continues to be one of the most commonly alleged violations in the US Department of Health and Human Services (HHS) Office for Civil Rights' (OCR's) HIPAA enforcement actions, appearing in half of all the settlements OCR has announced in the last 12 months and in almost all of the $1 million-plus settlements during that time period.[2] In the same vein, OCR recently announced that its Phase 2 Audits of CEs and BAs conducted during 2016–2017 yielded the following results with respect to the Risk Analysis requirement:

Rating		% of Audited CEs Receiving	% of Audited BAs Receiving
1	"Audit results indicate the entity is **in compliance with both goals and objectives** of the selected standards and implementation specifications"	0%	7%
2	"Audit results indicate that the entity **substantially meets criteria**; it maintains appropriate policies and procedures, and documentation and other evidence of implementation meet requirements"	14%	12%
3	"Audit results indicate entity efforts **minimally address audited requirements . . .** entity has made attempts to comply, but implementation is inadequate, or some efforts indicate misunderstanding of requirements"	32%	37%
4	"Audit results indicate the entity made **negligible efforts to comply** with the audited requirements—*e.g.*, policies and procedures submitted for review are copied directly from an association template; evidence of training is poorly documented and generic"	33%	29%
5	"The entity **did not provide . . . evidence of serious attempt to comply** with the Rules and enable individual rights with regard to PHI"	21%	15%

1 45 CFR § 164.308(a)(1)(ii)(A); 68 Fed. Reg. 8,334 (Feb. 20, 2003); 78 Fed. Reg. 5,589 (Jan. 25, 2013).

2 https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html.

In more familiar terms, OCR's auditors gave no Covered Entity an "A" on the Risk Analysis requirement, and only 14% of the Covered Entity class received a "B." Fully a third of the Covered Entity class received a "D," and another fifth of the Covered Entity class received an "F" (totaling more than half of audited Covered Entities falling *below* a "C"). The results for Business Associates were similarly discouraging. Our personal experience in defending OCR investigations and negotiating several recent HIPAA settlements has been similar, with OCR frequently rejecting as insufficient risk analyses that clients had paid expert consultants (including other law firms and Big Four accounting firms) hundreds of thousands of dollars to design or conduct.

There remains significant confusion across the health care industry and among the professional advisors who support it as to what actually constitutes a Risk Analysis for purposes of the HIPAA Security Rule—confusion for which HHS is at least partly responsible. Indeed, on April 30, 2018, as we were finalizing this article, OCR issued its latest Cybersecurity Newsletter, titled "Risk Analyses vs. Gap Analyses – What is the difference?" which aims to address some of that confusion.[3]

This article discusses the distinction between a HIPAA Security Rule Risk Analysis and a HIPAA compliance gap analysis, reviews OCR's historical guidance on conducting a compliant Risk Analysis, and encourages CEs and BAs to consider carefully whether to conduct these reviews under attorney-client privilege. This distinction is critical for many reasons, not least of which is the fact that, in the enforcement context, OCR typically treats a CE's or BA's alleged failure to conduct an adequate Risk Analysis as at least a $1,000 per-day violation, spanning up to six years.

Terminology: Risk Analysis vs. Risk Assessment vs. . . .

First, let's get our terminology straight. The "Administrative Safeguards" provision of the HIPAA Security Rule (appearing at 45 CFR § 164.308) starts by directing every CE and BA to implement a "Security management process" that must include a "Risk Analysis"—defined as "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."[4] This is the legal requirement referenced in the prior section as appearing in half of OCR's recent HIPAA settlements and being scored so poorly on the Phase 2 Audits.

We have heard many stakeholders use "Risk Assessment" interchangeably with "Risk Analysis." That is entirely understandable, given that the Security Rule itself defines the required "Risk Analysis" as an "assessment" of risk and vulnerabilities. It is also understandable because National Institute of Standards and Technology (NIST) Special Publication 800-30 (titled "Guide for Conducting Risk Assessments"[5]) is referenced in OCR's 2010 guidance for conducting a HIPAA Security Rule Risk Analysis, and other official sources such as HealthIT.gov appear to use the phrase "Risk Assessment" specifically to refer to the Security Rule's Risk Analysis requirement.[6] This interchangeable use, however, creates confusion with the entirely different, multi-factor "risk assessment" contemplated by the HIPAA Breach Notification Rule for purposes of determining whether an unauthorized use or disclosure of protected health information (PHI) creates more than a low probability of compromise and thus constitutes a reportable breach.[7] Given this confusion about terminology, we recommend sticking with the Security Rule's own label of "Risk Analysis" when discussing an evaluation of the potential risks and vulnerabilities to electronic PHI (ePHI), as required by 45 CFR § 164.308(a)(1)(ii)(A).

What Does OCR Consider to Be a Compliant Risk Analysis?

As previously noted, the Security Rule's text defines Risk Analysis as "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."[8] In the preamble to the Initial Final Security Rule, HHS stated that a "thorough and accurate" risk analysis "would consider 'all relevant losses' that would be expected if the security measures were not in place. 'Relevant losses' would include losses caused by unauthorized uses and disclosures and loss

3 The newsletter was emailed to OCR's security distribution list, to which one can subscribe at https://list.nih.gov/cgi-bin/wa.exe?SUBED1=OCR-SECURITY-LIST&A=1. An archive of prior newsletters is available at: https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/cybersecurity-newsletter-archive/index.html.

4 45 C.F.R. § 164.308(a)(1)(ii)(A).

5 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.

6 https://www.healthit.gov/providers-professionals/security-risk-assessment

7 45 CFR § 164.402(2).

8 45 CFR § 164.308(a)(1)(ii)(A).

of data integrity that would be expected to occur absent the security measures."[9]

In 2010, drawing heavily from NIST recommendations, OCR expanded on that regulatory definition through sub-regulatory guidance[10] that remains "in effect" to this day.[11] While OCR recognizes that "[t]here are numerous methods of performing risk analysis and there is no single method or 'best practice' that guarantees compliance with the Security Rule," it lists nine "elements a risk analysis must incorporate, regardless of the method employed":

1. **Scoping** – to take into account all ePHI the entity creates, receives, maintains or transmits, regardless of medium, source or location
2. **Data Collection** – to "identify where the ePHI is stored, received, maintained or transmitted"
3. **Identification and Documentation of Potential Threats and Vulnerabilities** – to include any "reasonably anticipated" threats and any vulnerabilities "which, if triggered or exploited by a threat, would create a risk of inappropriate access **to or disclosure of ePHI"**
4. **Assessment of Current Security Measures** – to analyze current security measures (including technical and non-technical measures) implemented to minimize or eliminate risks to ePHI
5. **Determination of the Likelihood of Threat Occurrence** – leading to "documentation of all threat and vulnerability combinations with associated likelihood estimates that may impact the confidentiality, availability and integrity of ePHI"
6. **Determination of the Potential Impact of Threat Occurrence** – *i.e.* assessment of the magnitude or criticality of harm that potentially would result from each identified threat or exploited vulnerability
7. **Determination of the Level of Risk** – cross referencing the likelihood of occurrence of each threat or vulnerability exploitation with the magnitude of resulting harm
8. **Finalization of Documentation** – agnostic as to format
9. **Periodic Review and Updating** – with no specific frequency required, but a general call for "continuous risk analysis" that proactively responds to any changes in technology, business operations, ownership and/or key personnel[12]

OCR reiterated these "required" Risk Analysis elements in its April 30, 2018, Cybersecurity Newsletter. In OCR's view, the necessary starting point of this process is a complete and accurate inventory or map of where ePHI resides and how it moves through, into and out of the CE's or BA's IT environment.

If this all sounds like a time- and resource-intensive effort, that is because it is just that, notwithstanding OCR's previously stated estimate that it should take an average CE or BA fewer than 20 hours to complete a Risk Analysis and a Risk Management Plan and document all resulting Policies and Procedures.[13]

This guidance yields the following key takeaways:

- OCR does not consider a Risk Analysis to be compliant unless it takes into account *all* ePHI created, received, transmitted or held by the CE or BA.
- In OCR's view, a compliant Risk Analysis focuses on categories of ePHI and the practical threats and vulnerabilities that pertain to each category, rather than an entity's compliance with legal requirements.

All of this guidance clearly is important in that it explains how OCR, as the nation's lead HIPAA regulator, actually interacts with the Risk Analysis requirement and regulated entities' efforts to comply. It also is important, however, to remember that any such sub-regulatory guidance ultimately lacks the

9 68 Fed. Reg. 8,334, 8,347 (Feb. 20, 2003).

10 Guidance on Risk Analysis Requirements Under the HIPAA Security Rule (https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf).

11 In 2007, the Centers for Medicare and Medicaid Services (CMS) published sub-regulatory guidance titled "Basics of Security Risk Analysis and Risk Management" as part of its HIPAA Security Series (https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/riskassessment.pdf). On August 4, 2009, the Secretary of HHS delegated to OCR the authority to enforce the HIPAA Security Rule, which prior to that time had been the responsibility of CMS. 74 Fed. Reg, 38,630 (Aug. 4, 2009).

12 Id. at 4–7.

13 78 Fed. Reg. 5,566, 5,678 (Jan. 25, 2013).

force of law[14] (at least outside the confines of HHS's internal HIPAA adjudication process[15]) and is increasingly disfavored in US Department of Justice policy regarding civil enforcement.[16]

What Does OCR Clearly *Not* Consider to Be a Compliant Risk Analysis?

In our experience reviewing clients' historical Risk Analysis documents, we frequently encounter materials that focus not on categories/locations/types of ePHI and associated practical threats and vulnerabilities, but rather on the client's compliance with the range of HIPAA requirements. For example, we frequently see "Risk Analyses" that, rather than list ePHI stored on laptops issued to a client's traveling nursing workforce, and note risks such as theft or loss of such machines and associated mitigating controls (*e.g.*, hard drive encryption), instead list, *e.g.*, the Security Rule's requirement that each CE/BA establish and implement an emergency mode operation plan[17] and the Privacy Rule's requirement that each CE/BA develop and disseminate a Notice of Privacy Practices.[18] Such "Risk Analyses" then assess the subject entity's degree of (non-) compliance with those requirements—doing the same for each of the various requirements, standards and addressable specifications created by the HIPAA Privacy, Security and Breach Notification Rules. We regularly see this approach taken even now by many professional services firms that hold themselves out to be expert HIPAA consultants, sometimes based on contract work they have performed directly for OCR (*e.g.*, HIPAA audit design).

In our experience, and as OCR emphasized in its April Cybersecurity Newsletter, OCR calls this type of assessment a "gap analysis" and clearly distinguishes it from a Security Rule-compliant Risk Analysis. Therefore, an entity under OCR investigation that, when asked for a copy of its Risk Analysis, produces such a gap analysis faces potential scrutiny on multiple fronts.

First, OCR is likely to allege that the entity has failed to comply with the Risk Analysis requirement itself—potentially leading to a threat to impose penalties of $1,000 or more per day over the course of up to six years (including during the pendency of the investigation itself) for that alleged failure alone. Second, the entity has also handed OCR a roadmap to all of the other HIPAA Privacy, Security and Breach Notification Rule requirements with which the entity has not fully complied. OCR then can use the "Risk Analysis" not only as a roadmap for its investigation but also subsequently as evidence that the entity was on notice (at least as of the date of the analysis) that it was out of compliance, and that any failure in the meantime to come into compliance was a knowing or intentional one (triggering potentially larger per-violation penalties under HIPAA's Enforcement Rule).[19]

And OCR is not the only actor that can use such a document in this way. While HIPAA itself creates no private right of action, a privacy plaintiffs' bar has been developing for a few years now and is becoming both more sophisticated and more aggressive about using state law—from privacy-specific laws and UDAP (unfair or deceptive acts and practices) statutes to garden-variety negligence theories under various consumer protection laws—to bring claims for damages that are derivative of alleged HIPAA violations, and some state courts have recognized HIPAA as establishing a standard of care whose violation can establish a common law tort claim.[20] As privacy and cybersecurity issues increasingly dominate news headlines, this trend is likely to accelerate and grow into the areas of derivative, shareholder and business-to-business litigation.

Unfortunately, HHS itself has caused much of this problem. The "Security Risk Assessment Tool" that appears on HealthIT.gov—developed by the Office of the National Coordinator for Health Information Technology in partnership with OCR and HHS Office of General Counsel—is itself a "gap analysis" targeted at assessing an organization's degree of compliance with the administrative, physical and technical "safeguards" (more accurately, standards and implementation specifications) of the Security Rule. The tool does not help the user inventory the various categories of ePHI that the user's organization creates, receives, transmits and stores, then evaluate potential threats and vulnerabilities associated with those categories. This tool does not meet OCR's stated

14 Perez v. Mortgage Bankers Assoc., 135 S. Ct. 1199 (2015) ("The absence of a notice-and-comment obligation makes the process of issuing interpretive rules comparatively easier for agencies than issuing legislative rules...[b]ut that convenience comes at a price: Interpretive rules do not have the force and effect of law and are not accorded that weight in the adjudicatory process.") (citation and internal quotation marks omitted).

15 See 45 CFR § 160.508(c)(1)—whose validity has yet to be litigated.

16 See "Guidance on Guidance: DOJ Limits Use of Agency Guidance Documents in Civil Enforcement Cases," available at https://www.mwe.com/en/thought-leadership/publications/2018/02/doj-limits-use-of-agency-guidance-documents.

17 45 CFR § 164.308(a)(7)(ii)(C).

18 45 CFR § 164.520.

19 45 CFR § 160.404(b)(2)(iii)-(iv).

20 See, e.g., Byrne v. Avery Center for Obstetrics and Gynecology PC, SC 19873 (Conn., Jan. 16, 2018).

requirements for a compliant Risk Analysis, but its results do create a self-critical HIPAA compliance report card that is likely to be discoverable if sought by an investigating regulator or litigation adversary. As such, it should be treated with caution.

A Word on Privilege Issues

This is not to say that a HIPAA-regulated entity should not periodically perform a compliance gap analysis of some sort. To the contrary, in this era of increasingly aggressive HIPAA enforcement and derivative civil litigation threats, entities are well served to regularly assess the overall state of their compliance efforts as part of a continuous quality improvement (CQI) effort. But it is important to do so in a way designed to minimize the chance that a less-than-perfect result (which, let's be honest, is likely to result from most any entity's meaningful and realistic look into this particular mirror) can later be used against the organization by regulators or private litigants.

The attorney-client privilege is designed to facilitate exactly this sort of honest, self-critical communication. As a brief refresher, the privilege generally protects from compelled disclosure (whether to a regulator, a prosecutor or a private litigant) confidential communications whose primary purpose is for a client to seek legal advice from a lawyer or for a lawyer to provide such advice. It does not matter how relevant the subject communication may be to the matter being investigated or litigated; if the required elements of the privilege are established, the client generally has the right to decline to produce or otherwise reveal the content of the communication. The client also has the right to waive the privilege if desired, subject to limitations on selective waivers.

One key element of the attorney-client privilege: it only applies when a lawyer is being asked for, or is providing, legal advice. It does not protect expert advice from a non-lawyer consultant unless such advice is provided to a lawyer for the purpose of facilitating the lawyer's provision of legal advice to his or her client.[21] Therefore, if your organization wants to assess the state of its compliance with the HIPAA Rules, the right first step is to seek advice on that topic from a lawyer (in-house or outside) and let the lawyer help determine which, if any, other professionals are needed to facilitate such legal advice. By following that rule, and also the lawyer's direction with respect to confidentiality of the resulting communications and other materials, your organization can get a thorough, honest picture of its HIPAA compliance posture with minimal concern that a regulator or litigation adversary will end up using that assessment against you down the road.

All HIPAA-regulated organizations should also carefully consider conducting their Security Rule-required Risk Analyses under the attorney-client privilege, with engagements designed from the outset to facilitate a future limited waiver of the privilege if deemed appropriate in order to share the results of the analysis with a regulator, for example. This approach has pros and cons, but it is worth discussing with a lawyer before embarking on your next comprehensive Risk Analysis effort.

Bottom Line: What Should My HIPAA-Regulated Organization Do?

1. Determine now which document(s) you would provide if asked by OCR tomorrow to share a copy of your organization's most recent Risk Analysis.
2. Review those materials for the following:
    a. Methodology: Do they identify categories of ePHI and assess threats and vulnerabilities to that ePHI? Or do they instead focus on how and to what extent the organization complies with the various aspects of the HIPAA Rules?
    b. Scope: Do they address all known categories of ePHI the organization creates, receives, transmits and/or stores?
    c. Freshness: How recently was the analysis performed? Have any material operational, technological or personnel changes occurred in the interim?

    Based on that review, decide when a further Risk Analysis is needed and what aspects of the organization it needs to cover. Also consider whether further follow-up with previously engaged outside experts is needed to supplement their work.
3. When engaging outside experts to design or perform a Risk Analysis, ensure that they understand the differences

21 Most jurisdictions lack a more generalized privilege for "self-critical analyses" or the like, despite well-founded calls for such a privilege to be created.

between a Security Rule-compliant Risk Analysis and HIPAA "gap analysis," and that they know you are seeking the former for purposes of your organization's compliance with 45 CFR § 164.308(a)(1)(ii)(A)—and then document this as the deliverable work product in the Statement of Work or other engagement materials. Consider using a lawyer to drive the process, in order to maximize future optionality with respect to privilege protection.

4. Only conduct "gap analyses" or similarly self-critical analyses of your organization's legal compliance through a lawyer, under privilege, unless your organization has carefully evaluated the pros and cons and decided there is a compelling reason to create a self-critical assessment that may need to be produced to regulators and litigation adversaries.

5. Remember that, following the completion of the Risk Analysis, it is critical to prepare a written risk management plan that includes the CE's or BA's plan of action for mitigating any risks or vulnerabilities identified by the Risk Analysis.[22]

AUTHORS

For more information, please contact your regular McDermott lawyer, or:

David Quinn Gacioch
+1 617 535 4478
dgacioch@mwe.com

Edward G. Zacharias
+1 617 535 4018
ezacharias@mwe.com

Amy C. Pimentel
+1 617 535 3948
apimentel@mwe.com

For more information about McDermott Will & Emery visit
www.mwe.com

22 45 CFR § 164.308(a)(1)(ii)(B).

Office Locations

BOSTON
28 State Street
Boston, MA 02109
USA
Tel: +1 617 535 4000
Fax: +1 617 535 3800

BRUSSELS
Avenue des Nerviens 9-31
1040 Brussels
Belgium
Tel: +32 2 230 50 59
Fax: +32 2 230 57 13

CHICAGO
444 West Lake Street, Suite 4000
Chicago, IL 60606
USA
Tel: +1 312 372 2000
Fax: +1 312 984 7700

DALLAS
2501 North Harwood Street, Suite 1900
Dallas, TX 75201
USA
Tel: +1 214 295 8000
Fax: +1 972 232 3098

DÜSSELDORF
Stadttor 1
40219 Düsseldorf
Germany
Tel: +49 211 30211 0
Fax: +49 211 30211 555

FRANKFURT
Feldbergstraße 35
60323 Frankfurt a. M.
Germany
Tel: +49 69 951145 0
Fax: + 49 69 271599 633

HOUSTON
1000 Louisiana Street, Suite 3900
Houston, TX 77002
USA
Tel: +1 713 653 1700
Fax: +1 713 739 7592

LONDON
110 Bishopsgate
London EC2N 4AY
United Kingdom
Tel: +44 20 7577 6900
Fax: +44 20 7577 6950

LOS ANGELES
2049 Century Park East, 38th Floor
Los Angeles, CA 90067
USA
Tel: +1 310 277 4110
Fax: +1 310 277 4730

MIAMI
333 Avenue of the Americas, Suite 4500
Miami, FL 33131
USA
Tel: +1 305 358 3500
Fax: +1 305 347 6500

MILAN
Via dei Bossi, 4/6
20121 Milan
Italy
Tel: +39 02 78627300
Fax: +39 02 78627333

MUNICH
Nymphenburger Str. 3
80335 Munich
Germany
Tel: +49 89 12712 0
Fax: +49 89 12712 111

NEW YORK
340 Madison Avenue
New York, NY 10173
USA
Tel: +1 212 547 5400
Fax: +1 212 547 5444

ORANGE COUNTY
4 Park Plaza, Suite 1700
Irvine, CA 92614
USA
Tel: +1 949 851 0633
Fax: +1 949 851 9348

PARIS
23 rue de l'Université
75007 Paris
France
Tel: +33 1 81 69 15 00
Fax: +33 1 81 69 15 15

SEOUL
18F West Tower
Mirae Asset Center1
26, Eulji-ro 5-gil, Jung-gu
Seoul 100-210
Korea
Tel: +82 2 6030 3600
Fax: +82 2 6322 9886

SHANGHAI
MWE China Law Offices
Strategic alliance with
McDermott Will & Emery
28th Floor Jin Mao Building
88 Century Boulevard
Shanghai Pudong New Area
P.R.China 200121
Tel: +86 21 6105 0500
Fax: +86 21 6105 0501

SILICON VALLEY
275 Middlefield Road, Suite 100
Menlo Park, CA 94025
USA
Tel: +1 650 815 7400
Fax: +1 650 815 7401

WASHINGTON, DC
The McDermott Building
500 North Capitol Street, N.W.
Washington, DC 20001
USA
Tel: +1 202 756 8000
Fax: +1 202 756 8087