November 2018 – Vol. 34 No. 11
Published for Health Care Providers by ACA International
www.acainternational.org
pulse

Protecting Health Care Information

By Anne Rosso May

If you are a covered entity or business associate working under the umbrella of the Health Insurance Portability and Accountability Act, you should be pretty familiar with the expectation to document a risk analysis of your organization. The HIPAA Security Rule has required CEs and BAs to conduct risk analyses since 2003 and 2013, respectively, but confusion about what that means persists.

To wit: Last year, the Office for Civil Rights, which is responsible for issuing guidance on HIPAA Security Rule provisions, audited 41 BAs, a portion of which were debt collectors. In those audits, "OCR found that almost none of the business associates had what OCR evaluated as a competent or acceptable risk analysis policy," said David Holtzman, vice president of compliance strategies at CynergisTek, a cybersecurity firm.

To be fair, Holtzman, who is a former senior adviser to OCR for health information technology and the HIPAA Security Rule, noted that BAs were not alone—the CEs OCR surveyed also struggled to conduct appropriate risk analyses. (And of course, 41 is obviously not a large sample size considering the tens of thousands of BAs out there.)

But it might not be off-base to speculate that many CEs and BAs still haven't figured out what a risk analysis is, how it should be performed and what they should do with the findings. And this is a problem, especially if you consider that earlier this year, Fresenius Medical Care North America, a dialysis provider, agreed to pay OCR $3.5 million in part for failing to conduct a comprehensive risk analysis under HIPAA.

Of course, implementing a robust risk analysis will not only help insulate you from an OCR fine, it will also keep your clients and consumers happy—and your company out of the spotlight for a data breach.

The Essence of Your Analysis

A proper risk analysis, as defined in the HIPAA Security Rule, should identify any current or potential risks to the confidentiality and integrity of electronic protected health information (ePHI).

The good news is that there's no single defined way to conduct your risk analysis, so you are free to customize it to your specific organization. The bad news is that there's no single defined way to conduct your risk analysis, so it's up to you to figure out what it will entail.

To help companies get started, OCR put out guidance in July 2010 that's just as helpful now as it was then. In it, OCR laid out the nine essential elements it expects all risk analyses to contain. It wants you to:

1. Identify the scope of your analysis.
2. Collect data.
3. Identify and document potential threats and vulnerabilities.
4. Assess current security measures.
5. Determine the likelihood of a threat occurrence.
6. Determine the potential impact of a threat occurrence.
7. Determine the level of risk.
8. Finalize your documentation.
9. Periodically review and update your risk assessment.

These nine elements are so important that OCR released an update in April 2018 reiterating its expectations that organizations include these elements in their analysis.

Kevin Dunnahoo, associate director at Protiviti, a consulting firm, said that

continued on page 2

when he visits clients to help them tackle their risk analysis, he usually discovers that not only do they not understand those nine essential elements, most haven't even looked at OCR's guidance.

If this sounds familiar, pull up the OCR document (find it here: https://bit.ly/2tY9cgc) and compare it to your current documentation to get a better sense of whether or not you have hit these goals.

> "Many more recent OCR settlement agreements and enforcements have shown they will take a hard stance on organizations that have identified a risk but haven't put in appropriate management strategies."
>
> – Kevin Dunnahoo, associate director at Protiviti

OCR also poses three questions to help organizations start thinking about how they approach data security:

- Have you identified the ePHI within your organization? This includes ePHI that you create, receive, maintain or transmit.
- What are the external sources of ePHI? For example, do vendors or consultants create, receive, maintain or transmit ePHI?
- What are the human, natural, and environmental threats to information systems that contain ePHI?

If you haven't asked yourself these questions or feel your current risk analysis wouldn't hold up to OCR scrutiny, it may be wise to start fresh.

Dunnahoo suggested companies start by identifying the key stakeholders responsible for owning the analysis in both its current and future state, but to also make sure that other business units interacting with ePHI set aside time to provide input on how they are using it and potential threats to those uses.

OCR expects organizations to update their risk analysis "on a periodic basis," which is a pretty vague timeframe, but most experts encourage companies to at least minimally refresh it every year.

If, upon review, you find you don't need to update your risk analysis records, include an addendum explaining why things are staying the same for the time being—because if OCR comes calling, it will undoubtedly ask.

No Stone Unturned

Over and over again, OCR officials have stressed the importance of an enterprise assessment. In other words, if you're only looking at one aspect of ePHI in your business, say the strength of your firewall or how clients send you files, you're missing out on literally hundreds of other ways data could be compromised.

In its corrective resolution agreements and action plans for entities that have been found to violate HIPAA, OCR urges companies to develop a complete inventory of all facilities, electronic equipment, data systems and applications that contain or store ePHI and incorporate them into a risk analysis.

You'll want to look at how ePHI flows through your entire organization, which means examining your employee workstations, administrative controls, office equipment, server, physical security system, data security testing, compliance management system, website, vendors and more.

You've Identified Some Risks: Now What?

Catalog the risks you've uncovered, determine how likely they are to occur and calculate their potential impact. You'll want to put together a written plan to address the highest-risk items first, and gradually work your way down the list.

"Many more recent OCR settlement agreements and enforcements have shown they will take a hard stance on organizations that have identified a risk but haven't put in appropriate management strategies," Dunnahoo said. "If you can show you have identified it and are working through it that will put you in a much better light."

Your policies and procedures should address the purpose and scope of your risk assessment and detail how you are attempting to prevent, detect and correct security breaches.

When to Call for Help

There are many vendors and tools available that offer to help organizations with their HIPAA risk analysis.

Larger organizations will likely want to invest in an enterprise-wide information security risk analysis performed by a third-party, but smaller organizations can use online tools and guides to help structure their risk analysis.

"You can use a large risk management platform that can cost hundreds of thousands of dollars, but you can accomplish a lot of the same things in an Excel workbook as long as you are taking time to think through all the threats and vulnerabilities and controls in your environment," Dunnahoo said.

If you're wondering how your analysis would hold up to OCR scrutiny, you can cross-reference your plan against HHS' HIPAA audit protocols, which were just updated in July. (Find the protocols here: https://bit.ly/2Kn71Lz.)

Additionally, the Office of the National Coordinator for Health Information Technology's website (www.healthIT.gov) offers a downloadable risk assessment tool and the Information and Management Systems Society has an online risk assessment toolkit available (www.himss.org).

Still, OCR will be continuing its HIPAA enforcement program and related compliance reviews stemming from breach notification reports. If a report indicates the cause of the breach was due to how a BA handled ePHI, OCR will include that BA in its compliance review.

It's truly up to you to read up on OCR's expectations, examine your business, formulate a plan and see it through to the end.

Anne Rosso May is editor of Collector *magazine.*

Are You a Health Care Collection Expert?

ACA's Healthcare Collection Management designation can help you take your collection efforts to the next level.

By Irene Hoheusle

Does your agency collect health care debt? Do you consider yourself an expert in health care collections?

Do you feel the need for more education on health care collections?

If you answered yes to any of these questions, read on.

Those of us who collect medical debt understand that it's very different from any other type of debt.

Additional laws exclusive to the medical industry, such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and Health Information Technology for Economic Clinical Health Act (HITECH), as well as the Fair Credit Reporting Act when credit reporting medical debt, can be challenging.

There are a multitude of third-party payers that a health care collector needs to be familiar with to identify those deep pockets. Getting large third-party payments can benefit your agency, clients and consumers.

Commercial health insurance is just the icing on the cake. Your collectors need to learn about motor vehicles, premises liability, county liability and crime victims, just to name a few, according to Hoheusle. Additionally, with medical debt certain states hold spouses responsible, and there is always the question of who is responsible for minor children.

ACA has the resources to help health care collectors be their best. Earning ACA's Healthcare Collection Management designation (HCM) requires participants to complete three ACA Core Curriculum courses—Data Security and Privacy, Ethical and Professional Collections and Healthcare Collection Management—as well as the HCM Capstone Assessment.

The HCM webinar is presented in three afternoons, and covers the ins and outs of servicing health care accounts, the unique challenges of collecting health care accounts and the laws that affect health care.

Anita Manghisi, IFCCE, president of Independent Recovery Resources Inc., said she pursued the HCM designation for two reasons: to obtain the professional credentials and "to challenge myself, knowledge-wise, and improve upon any areas that I may not have known."

Manghisi also said she felt it helped her gain a first-party perspective so she can better understand what happens with health care accounts before they are turned to bad debt.

ACA's HCM designation is also a way to show your health care clients that you have gone the extra mile to learn their pain points so you can help resolve them.

Manghisi also noted that the HCM track "really challenges your knowledge of the entire process from day-one billing through the transfer to bad-debt."

Anyone collecting for the health care industry could benefit from taking the educational courses and receiving the HCM designation.

"I would encourage anyone in the health care space to take this track and ultimately achieve their designation," Manghisi said.

Irene Hoheusle, IFCCE, CCCO, is vice president of collections and education for Account Recovery Specialists Inc.

Visit https://www.acainternational.org/education/designations *to start working on your HCM designation.*

NEWS & NOTES

CMS Proposes Rules to Lower Compliance Burden on Health Care Providers

The Centers for Medicare and Medicaid Services is considering a rule to lower the burden on health care providers through changes to Medicare compliance requirements, according to a news release. The proposal is part of overall federal agency efforts to reduce burdensome regulations. Proposed Medicare updates would save health care providers approximately $1.12 billion each year. https://go.cms.gov/2PUEtY0

Consumers Face Bills from Out-of-Network Providers

A study of health insurance plans offered by large employers shows "a significant share of inpatient hospital admissions includes bills from providers not in the health plan's networks," according to the Kaiser Family Foundation. As a result patients typically have higher out-of-pocket costs and risk additional bills from their providers. For example, nearly 18 percent of inpatient admissions studied resulted in claims to out-of-network providers, according to the study. https://kaiserf.am/2BJy2of

We Want To Hear From You

Pulse is published for ACA health care collection agencies to provide current industry information for health care providers. ACA International welcomes article ideas and submissions for consideration in Pulse to the Communications Department at comm@acainternational.org.

For more health care collections news, visit ACA's Health Care Collections page at www.acainternational.org/pulse.

datawatch

Health Care Market Concentration

The Commonwealth Fund recently studied market concentration between health care providers and insurers in metropolitan statistical areas (MSAs). Overall, researchers found that concentration levels for providers fluctuated between highly concentrated (47.1 percent) and super concentrated (43 percent.) For insurers, however (MSAs) were in the middle categories of highly concentrated (54.5 percent) or moderately concentrated (36.9 percent).

		Health care provider market concentration				
		Unconcentrated	Moderately concentrated	Highly concentrated	Highly concentrated	Total
Health insurer market concentration	Unconcentrated	0/0%	0.6%	1.1%	1.9%	3.6%
	Moderately concentrated	0.0%	5.5%	16.5%	14.9%	36.9%
	Highly concentrated	0.3%	3.3%	27.5%	23.4%	54.5%
	Highly concentrated	0.0%	0.3%	1.9%	28%	5.0%
	Total	0.3%	9.6%	47.1%	43.0%	100.0%

Source: Brent D. Fulton, Daniel R. Arnold, and Richard M. Scheffler, "Market Concentration Variation of Health Care Providers and Health Insurers in the United States," https://www.commonwealthfund.org/blog/2018/variation-healthcare-provider-and-health-insurer-market-concentration To the Point (blog), Commonwealth Fund, July 30, 2018.

pulse is a monthly bulletin that contains information important to health care credit and collection personnel. Readers are invited to send comments and contributions to:

Communications Department
ACA International
P.O. Box 390106
Minneapolis, MN 55439-0106
comm@acainternational.org

Note: Requests for reprints or additional information on material herein must be made through the ACA International member who sponsored your receipt of this publication.

Do we have your correct name, title and address? Please advise your sponsor of any corrections.