HCCA HEALTH CARE COMPLIANCE ASSOCIATION

Compliance TODAY

April 2017

A PUBLICATION OF THE HEALTH CARE COMPLIANCE ASSOCIATION

WWW.HCCA-INFO.ORG

The mission of making Compliance an academic discipline

an interview with Ryan Meade
Director, Center for Compliance Studies
Loyola University Chicago School of Law

See page 16

> Compliance deals with speculative and practical ethics, organizational theory, psychology, finance, behavioral theory, and law. We need people who will help tie together the themes.

See page 18

ARTICLES

Compliance TODAY

EXECUTIVE EDITOR: Roy Snell, CHC, CCEP-F, CEO, HCCA
roy.snell@corporatecompliance.org

NEWS AND STORY EDITOR/ADVERTISING: Margaret R. Dragon
781-593-4924, margaret.dragon@corporatecompliance.org

COPY EDITOR: Patricia Mees, CHC, CCEP, 888-580-8373
patricia.mees@corporatecompliance.org

DESIGN & LAYOUT: Pete Swanson, 888-580-8373
pete.swanson@corporatecompliance.org

PROOFREADER: Briana Ring, 888-580-8373
briana.ring@corporatecompliance.org

PHOTOS ON FRONT COVER & PAGE 16: David Joel

Compliance Today (CT) (ISSN 1523-8466) is published by the Health Care Compliance Association (HCCA), 6500 Barrie Road, Suite 250, Minneapolis, MN 55435. Subscription rate is $295 a year for nonmembers. Periodicals postage-paid at Minneapolis, MN 55435. Postmaster: Send address changes to *Compliance Today*, 6500 Barrie Road, Suite 250, Minneapolis, MN 55435.

VOLUME 19, ISSUE 4

by Frank Ruelas

Analyzing the 2017 OIG Work Plan, HIPAA, and your annual work plan

» The OIG Work Plan identifies focus points related to data security and HIPAA.
» Focus points can be used to create an organizational work plan.
» The OIG Work Plan describes Meaningful Use audits and Security risk analyses.
» Data security is an ongoing challenge as described in the OIG Work Plan.
» Penetration testing is a tool that may prove useful against hackers.

Frank Ruelas *(francisco.ruelas@dignityhealth.org) is a Facility Compliance Professional with Dignity Health in Phoenix.* *bit.ly/in-FrankRuelas* *@Frank__Ruelas*

OK, you've read the email that announced that the Health and Human Services (HHS) Office of Inspector General's (OIG) Work Plan is posted and available for downloading.[1] Perhaps you even took the time to download a copy and keep it on file along with your copies of the 2016 OIG Work Plan, the 2015 OIG Work Plan, and so on. So now what? Is there additional value in the OIG Work Plan that compliance professionals may be overlooking, particularly those who are looking to draft a compliance work plan for their organization?

Ruelas

Given the comprehensive nature of the OIG's Work Plan, it can appear quite daunting and even intimidating to try to identify how it may provide input in the drafting of a work plan at the organizational level. This is one reason I like to review the OIG's Work Plan to get a sense of some of the key areas the OIG is focusing on. It gives me the opportunity to see how these focus points may apply directly or indirectly to my organization. Then I am in a better position to draft a compliance work plan that may address some of the same or similar issues that the OIG is planning to assess in the upcoming year.

There is increased attention directed to the Health Insurance Portability and Accountability Act (HIPAA). This may be due in part to the ongoing Office for Civil Rights (OCR) HIPAA Audit Program and ongoing challenges in dealing with security issues related to malicious software such as ransomware. Keeping this in mind, one might do a quick electronic search of the OIG Work Plan using the term "HIPAA" and see that there are no occurrences of it within the OIG's Work Plan. If one is focused primarily on HIPAA privacy or security, it would be reasonable to conclude that the 2017 Work Plan does not have much to do with HIPAA, much less with information privacy or security.

Not so fast!

By searching for the terms "security" and "privacy," one does indeed find several hits that are related to HIPAA. For those who are focused on HIPAA privacy and security, let's

sift through the OIG Work Plan and see what we can take away that may help us identify possible focus areas, which we can also use to develop our own, individual work plans.

Before moving on, please note that though I am presenting this analysis with respect to possible relationships with HIPAA, the same approach may be used for other focus areas listed within the OIG Work Plan that compliance professionals may find useful. For example, the OIG Work Plan has information related to compliance in the areas of billing and coding, claims management, and medication management to name a few. Consider several of your top focus areas, and then review the Work Plan for related content that you may find useful in developing your work plan.

In presenting the following sections from the OIG Work Plan, I included a brief restatement or paraphrase of a particular section along with page numbers where it is listed in the PDF version and in the text based version of the OIG Work Plan. The "Overview" section provides a quick summary of some of the high points I read in that section. The "Applicability" section describes ideas that I had when considering how I could apply what was explained in the Overview description to my organization. The "Takeaway" section lists possible action items for consideration.

Mandatory reviews of MACs

(PDF version: Pg. 24
Text-based version: Pg. 39)
Overview: Medicare Administrative Contractors are required to have independent evaluations of their security plans completed and for the OIG to report the results of these evaluations to Congress.[2]

Applicability*:* There may be review requirements that are prescribed by contracts or other agreements such as in Business Associate Agreements. These may include types of reviews or audits done to determine how effectively third parties, such as business associates, are protecting the privacy and security of PHI.

Takeaway: Check for any audit schedules or other documents that may identify if any reviews are needed. If reviews are needed, get them scheduled so as to complete them in a timely manner. Include any findings or some type of comprehensive summary report at the next scheduled Compliance Committee meeting or similar forum.

Breach notifications by state Medicaid agencies

(PDF version: Pg. 45
Text-based version: Pg. 60)
Overview: State Medicaid agencies and their subcontractors are required to comply with the breach notification rule (Subpart D, Part 164 of the HIPAA regulations). The OIG plans to review the breach notifications procedures of the state Medicaid agencies and their contractors and will also review past breaches of unsecured PHI.[3]

Applicability: Covered entities and business associates are required to comply with the Breach Notification Rule. If a breach is identified, the breach notifications are triggered and must be completed within the timeframes identified in the HIPAA regulations. In addition, the OCR HIPAA Audit protocol lists elements (#162 and #164)[4] that assess processes and procedures to provide affected individuals with timely breach notifications.

Takeaway: Review identified breaches and see that documentation is available to show that the organization provided breach notifications as required by the Breach Notification Rule. Take steps to ensure that the documentation is readily available to show when the risk assessments of incidents were determined

to not represent breaches. These documented risk assessments could be requested during an OCR HIPAA audit as described in the audit protocol (#170).[5]

CMS oversight of security controls

(PDF version: Pg. 45
Text- based version: Pg. 60)

Overview: Previous OIG reviews reported that state Medicaid information systems lacked sufficient security features. The lack of such features could put the PHI of Medicaid beneficiaries at risk for unauthorized access. The OIG is going to review some of these information system controls and use its assessment tools to evaluate the security of the information systems of selected state Medicaid agencies.[6]

Applicability: Under the HIPAA Security Rule, there are a number of implementation specifications, some required and some addressable, that are focused on providing administrative, technical, and physical safeguards to protect the security of PHI. A subset of the OCR Audit protocol (elements #90 – #161)[7] is also dedicated to security, some or all of which may be assessed during an OCR HIPAA audit or in response to a complaint investigated by the OCR.

Takeaway: Consider collaboration with the Information Technology (IT) or similar department within the organization to determine if the Security Rule implementation specifications are applied in accordance with the HIPAA Security Rule. Also identify if there are any addressable implementation specifications that were not implemented and, if so, documentation to support why not and what the organization did to provide an equivalent security measure.

Certified EHR technology and incentive payments

(PDF version: Pg. 52
Text-based version: Pg. 67)

Overview: The OIG will be reviewing covered entities to determine if they are protecting PHI maintained by their certified electronic health record (EHR) technology. To receive incentive payments under Meaningful Use, eligible providers and hospitals were required to conduct a Security risk analysis (SRA) to include their certified EHR as described by federal regulations.[8]

Applicability: If the organization has received incentive payments from CMS under the Meaningful Use program, the organization may get audited, including a likely review of the SRA that was used to support its attestation that was submitted as part of the process to receive Meaningful Use incentive dollars.

Takeaway: Identify the location of the SRA used as part of the attestation process under Meaningful Use so that it can be retrieved if a Meaningful Use audit occurs. The SRA is also identified in an element (#93) listed within the OCR HIPAA audit protocol that may be reviewed during an audit. Having the SRA readily available is helpful in meeting the response timeframe that may be applied in providing documents to the OCR in preparation for an audit or in response to an OCR's investigation of a complaint.

FDA's response for networked medical device compromise

(PDF version: Pg. 62
Text-based version: Pg. 76)

Overview: The OIG will review the Food and Drug Administration (FDA) in how it monitors the safety and effectiveness of networked medical devices. This includes reviewing how the FDA communicates and addresses a medical device's cybersecurity compromise. Medical devices continue to evolve in their complexity as they are able

to perform a number of functions, which may include receiving or sending network data that may include PHI.[9]

Applicability: Determine if medical devices that are connected to the organization's network are included in the organization's most current SRA. Also identify if the person designated to receive FDA notices, including notices related to cybersecurity issues as they apply to medical devices, is receiving notices in a timely manner.

Takeaway: Review the SRA to identify if networked medical devices are listed as assets that create, maintain, receive, or transmit PHI. If there are devices listed, review the administrative, technical, and physical safeguards that are identified in the SRA, which are in place to provide an acceptable level of security to the identified PHI as determined by the organization.

HHS compliance with FISMA

(PDF version: Pg. 80
Text-based version: Pg. 95)
Overview: The OIG will review HHS and selected HHS operating divisions on their compliance with the Federal Information Security Modernization Act (FISMA) requirements. FISMA requires adequate security on systems that collect, process, transmit, store, or disseminate information.[10]

Applicability: HIPAA has a focus on applications and processes that create, maintain, receive, or transmit PHI. This may present an opportunity for the designated individual, identified in the Administrative Requirements under the Security Rules, to conduct an inventory to work with IT or others to make sure that applications that collect, maintain, receive, or transmit PHI are accounted for. After this accounting, a review of the SRA can be completed to see if these identified applications are included in the most recent SRA.

Takeaway: Given OIG's focus on applications that seem to mirror similar functions that are identified within HIPAA as they relate to FISMA, this presents an opportunity to make an effort to validate that programs and applications that process PHI are adequately identified and assessed as called for in the HIPAA regulations.

Penetration testing

(PDF version: Pg. 80
Text-based version: Pg. 95)
Overview: Hackers use penetration tests to identify potential ways to gain unauthorized access to information systems. The OIG will conduct penetration tests to determine the level of security of HHS systems and their susceptibility to hackers.[11]

Applicability*:* Covered entities and business associates are required to comply with the HIPAA Security Rule. In doing so, there is a need to assess the level of security of those applications and programs that are associated with PHI. Penetration testing may present an organization with a more complete or accurate profile of the security of its information systems.

Takeaway: Penetration testing may not be something that is done by the organization. This type of test may contribute to a more accurate assessment of the security of an information system. It may also help prevent or minimize opportunities that may be exploited by a hacker who is trying to gain unauthorized access to the organization's information system. If penetration testing is not currently done, engage the IT department or similar department in a discussion to consider the use of penetration testing in the ongoing assessment of the security of the information system.

Summary

The overview, applicability, and takeaway approach used here is one of many ways to review and dissect the OIG Work Plan to analyze how the activities of what the OIG is planning to do may have some applicability at the organizational level. Given the amount of information that the OIG is privy to and its work with HHS, CMS, OCR, and other units that deal with compliance-related issues across the federal healthcare delivery system and its programs, the OIG very likely has a keen sense of some of the challenging areas across the compliance spectrum. In turn, there may be sections within the OIG's Work Plan that organizations can use to identify how some of these challenging areas may also exist within their organizations.

Although the OIG Work Plan assesses the compliance landscape on a macro level, it can also be used to identify meaningful focus points that on a micro level can help compliance officials develop work plans for their own organizations. This aspect can be very useful in providing the organization's leadership team with information on how this year's work plan was developed. This may also provide very useful in supporting requests for resources to support the timely implementation and management of the organization's work plan.

1. HHS: Office of Inspector General: Work Plan archive. Available at http://1.usa.gov/1g9X7oi
2. HHS: Office of Inspector General: OIG Work Plan 2017. Available at http://bit.ly/2j2lUoB, Pg 24.
3. Idem, Pg 45. http://bit.ly/2j2lUoB
4. HHS.gov: Health Information Privacy: Audit Protocol – Updated April 2016. Available at http://bit.ly/2biNxRL
5. Idem.
6. Ibid, Ref #3.
7. Ibid, Ref #4.
8. Ibid, Ref #2, Pg 52.
9. Ibid, Ref #2, Pg 62.
10. Ibid, Ref #2, Pg 80.
11 Idem.