HIPAA AND MEANINGFUL USE AUDITS AND THE SECURITY RISK ANALYSIS NEXUS

By Daniel F. Shay, Esq.

Alice G. Gosfield & Associates, PC
2309 Delancey Pl.
Philadelphia, PA 19103
215-735-2384
215-735-4778
agosfield@gosfield.com
www.gosfield.com

Accepted for publication in the Health Law Handbook, 2015 Edition.
Alice G. Gosfield, Editor. © Thomson Reuters.
A complete copy of the Health Law Handbook is available from Thomson Reuters by calling 1-800-328-4880 or online at www.legalsolutions.thomsonreuters.com.

1 Introduction

Computer software is changing the administrative aspects of the practice of medicine. With the advent of electronic medical records, computerized order entry, and electronic prescribing, physicians and physician practices are finding new ways to improve practice efficiency and increase practice income. At the same time, many practices are taking advantage of federal incentive programs, such as the Meaningful Use program, to bring in yet more money. However, physician practices are discovering that, while the use of these electronic tools can improve a practice's performance, it also imposes burdens on the practice to monitor a range of reporting responsibilities to qualify for Meaningful Use incentive payments.

Recognizing the popularity of the Meaningful Use program, as well as the need to ensure that it gets its money's worth, the federal government has instituted an auditing program examining the information supporting a physicianôs attestation of being a ñmeaningful userò within the definition of the program. If the physician fails the audit, he or she must return the *entirety* of the Meaningful Use payments received for the reporting year, and will face payment adjustments, beginning in 2015. As of this writing, it is estimated that over 257,000 eligible providers (EPs) ï more than half of those who reported ï face Meaningful Use penalties of 1% Medicare payment reductions incurred as a result of failures to effectively report in 2013.[1]

At the same time, the federal government has also determined that its enforcement of HIPAA has been lax, particularly with respect to the Security Rule, which governs electronic protected health information (ñPHIò). Accordingly, federal regulators have begun conducting separate HIPAA audits, as well as increasing enforcement of HIPAA against physician practices. If a physician practice falls short of meeting its requirements under HIPAA, it may face stiff fines, and may be required to enter into a settlement agreement with the federal government ï which itself can require a wide range of corrective actions.

Given the newness of both their electronic systems and these audit programs, physician practices may find themselves unprepared or caught flat-footed. Yet at the same time, many practices continue to disregard their obligations, leaving themselves exposed. This chapter explores the background of the two auditing programs (under meaningful use and the HIPAA Security Rule), including a brief history behind these enforcement and auditing efforts, and where those efforts stand at the time of this writing. It then explores the grounds on which federal regulators have enforced these rules. Finally, the chapter turns to the steps that physician practices can take to protect themselves and begin meeting their obligations, with a particular eye towards helpful resources provided by federal administrative agencies.

2 Background Information

To understand the current efforts towards enforcement, it is helpful to have a general sense of how we arrived at this point. Towards this end, this section explores the history behind the HIPAA and Meaningful Use audit programs, and the regulatory and enforcement steps that led to

[1] Mace, Scott, ñMeaningful Use Payment Adjustments Begin,ò Health Leaders Media, December 18, 2014, available at http://www.healthleadersmedia.com/page-1/TEC-311416/Meaningful-Use-Payment-Adjustments-Begin.

their beginning. It also provides general information on the current auditing process for each program, and what audited providers can expect.

2.1 HIPAA Audit Program

Passed into law in 1996, the Health Insurance Portability and Accountability Act has seen several regulatory schemes published over the last nineteen years.[2] The major highlights include the Privacy Rule, which was published in December, 2000[3]; the Security Rule, published in February, 2003[4]; the Enforcement Rule, published in final form in 2006[5]; the Breach Notification Rule, published in August, 2009[6]; and the Ominbus Rule, which modified aspects of the previous Rules, published in January, 2013[7].

The Department of Health and Human Services' Office of Civil Rights ("OCR") has enforced HIPAA's regulations since April 14, 2003 -- the date of compliance for the Privacy Rule. Interestingly, the OCR did not begin to enforce the Security Rule until July 27, 2009, over four years after the April 20, 2005 compliance date.[8] For several years, the OCR primarily targeted its enforcement activities against larger covered entities, such as hospitals and health systems. However, this changed in April, 2012, when the OCR enforced against Phoenix Cardiac Surgery, P.C., a two-physician practice, following a complaint that ePHI had been erroneously posted online.[9] Whereas the OCR had previously focused the bulk of its enforcement efforts on "big fish," this enforcement action demonstrated that they would now target "little fish," as well.

Under the Health Information Technology for Economic and Clinical Health Act of 2009 ("HITECH"), itself a part of the American Recovery and Reinvestment Act of 2009 ("ARRA"), the OCR was required to perform "periodic audits."[10] Accordingly, beginning in November,

[2] For additional information on HIPAA, see the Office of Civil Rights' website at www.hhs.gov/ocr/privacy/hipaa/administrative/index.html.

[3] 65 Fed. Reg. 82462, December 28, 2000. Revisions were published at 67 Fed. Reg. 53182, August 14, 2002.

[4] 68 Fed. Reg. 8334, February 20, 2003.

[5] 71 Fed. Reg. 8390, February 16, 2006. Revisions were published at 74 Fed. Reg. 56123, October 30, 2009.

[6] 74 Fed. Reg. 42740, August 24, 2009.

[7] 78 Fed. Reg. 5566, January 25, 2013.

[8] http://www.hhs.gov/ocr/privacy/hipaa/enforcement/index.html.

[9] The practice in question posted clinical and surgical patient appointments on a publicly accessible Internet-based calendar. The practice was fined $100,000 and required to rectify the deficiencies discovered after the OCR investigated the practice over a three-year period. See, ñHHS Settles Case with Phoenix Cardiac Surgery for Lack of HIPAA Safeguards,ò HHS Press Release, at http://www.hhs.gov/news/press/2012pres/04/20120417a.html. The full resolution agreement is available at, http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/pcsurgery_agreement.pdf.

[10] HITECH Act, Sec. 13411.

2011, the OCR launched its Audit Pilot Program ï a roughly year-long program where the OCR conducted privacy and security audits of a selected group of covered entities.[11] The primary purpose of the program was "to examine mechanisms for compliance, identify best practices and discover risks and vulnerabilities that may not have come to light through OCRôs ongoing complaint investigations and compliance reviews."[12] The program targeted a total of 115 covered entities including hospitals, group health plans, nursing care facilities, health care clearinghouses, physician practices, and even a dental practice.[13] Notably, the results of these initial audits found that smaller entities ï such as physician practices and community or rural pharmacies ï had difficulty with Privacy, Security, and Breach Notification Rule compliance.[14]

The Audit Pilot Program led to the Audit Evaluation Program, wherein the OCR evaluated the results of the audits it had conducted between November, 2011 and December, 2012, and examined feedback from the covered entities who had been audited.[15] The Audit Evaluation Program was designed to determine the effectiveness of the audit protocol established by the OCR as well as the auditing process itself, to understand what activities and resources had facilitated the auditing program, and to help understand the barriers and any problems that might have been encountered in the program.[16] Towards this end, the OCR reviewed audit data, conducted a confidential online survey with audit participants, and conducted interviews with some participants.

Based on the results of the Audit Pilot Program and the Audit Evaluation Program, the OCR began "Phase 2"[17] of its Audit Program in October, 2014.[18] The "Phase 2" audits target

[11] http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/auditpilotprogram.html.

[12] http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/auditpilotprogram.html.

[13] http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/listofentities.html. The initial group of covered entities was limited to 20 to test the original audit protocol, and was then expanded to 95 further covered entities to test a modified audit protocol. See, Sanches, Linda, "HIPAA Privacy, Security and Breach Notification Audits -- Program Overview & Initial Analysis," HCCA 2013 Compliance Institute, April 23, 2013, p.2, at www.hcca-info.org/Portals/0/PDFs/Resources/Conference_Handouts/Compliance_Institute/2013/Tuesday/500/504print2.pdf.

[14] Sanches, Linda, "HIPAA Privacy, Security and Breach Notification Audits -- Program Overview & Initial Analysis," HCCA 2013 Compliance Institute, April 23, 2013, p.9.

[15] http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/evaluation.html.

[16] Sanches, Linda, "OCR Audits of HIPAA Privacy, Security and Breach Notification, Phase 2," HCCA Compliance Institute, March 31, 2014, p. 10, at http://www.hcca-info.org/Portals/0/PDFs/Resources/Conference_Handouts/Compliance_Institute/2014/tue/710print2.pdf. This powerpoint presentation also includes descriptions of the audit subjects' reactions to the process, and the areas where the OCR believes it could improve the process.

[17] The Audit Pilot Program is considered "Phase 1." See, Sanches, Linda, "OCR Audits of HIPAA Privacy, Security and Breach Notification, Phase 2," HCCA Compliance Institute, March 31, 2014.

[18] The OCR did pause the Audit Program in September, 2014, while it upgraded certain technology to allow for better audits. McGee, Marianne Klbasuk, "HIPAA Audits: A Revised Game Plan," Healthcare Info Security, at http://www.healthcareinfosecurity.com/hipaa-audits-revised-game-plan-a-7296. Audits have since resumed.

approximately 350 covered entities, as well as their business associates.[19] The covered entities were notified that they had been selected for auditing in fall, 2014, followed by requests for data. Whereas previous audits were conducted by outside contractors, these audits are performed by the OCR itself, using its internal staff.[20] Business associates of the audited covered entities are being audited in 2015. Among covered entities, providers make up 2/3 of the projected audit targets for Phase 2, with IT-related business associates expected to make up 70% of the 50 business associates that the OCR expected to audit.[21]

While the OCR will perform on-site audits where possible, most Phase 2 audits are conducted as "desk reviews," wherein the covered entity is notified that it has been selected for an audit by the OCR, certain documentation is requested from the covered entity, and the covered entity must respond within two weeks and provide the requested information to the OCR auditors; the OCR does not visit the covered entity's location and all requested materials are submitted electronically. After reviewing the submitted material, the OCR issues a draft of its findings, which are reviewed by the covered entityôs management. Finally, the OCR issues its formal report on the audit results for the covered entity.

The OCR has offered advice to covered entities faced with a desk audit. For example, the OCR points out that only timely-submitted data is assessed by auditors. Moreover, the documentation provided must be current as of the date of the request. The documentation should also be as complete and accurate as possible. Auditors typically will not contact the covered entity to ask for clarification or additional supporting information, and information extraneous to that which is requested may actually make the auditor's assessment more difficult.[22] Finally, a failure to submit documentation may result in the audit being referred to compliance review.

2.2 Meaningful Use Audit Program

The Medicare EHR Incentive Program (also known as "Meaningful Use") was created as part of the HITECH Act, with a goal of spurring the effective use of electronic health record ("EHR") technology by "eligible practitioners" (or "EPs") participating in Medicare and/or Medicaid.[23]

[19] Sanches, Linda, "OCR Audits of HIPAA Privacy, Security and Breach Notification, Phase 2," HCCA Compliance Institute, March 31, 2014, p. 17. However, a prior notice from the OCR indicated that the total number of audits could be as high as 1,200. 79 Fed. Reg. 10158, February 24, 2014.

[20] Sanches, Linda, "OCR Audits of HIPAA Privacy, Security and Breach Notification, Phase 2," HCCA Compliance Institute, March 31, 2014, p. 18. Previous audits were performed by KPMG, based on information developed by Booz Allen Hamilton in 2010-2011. The evaluation of the audit program was performed by Price Waterhouse Cooper, LLP in 2013. Id, p. 2.

[21] Sanches, Linda, "OCR Audits of HIPAA Privacy, Security and Breach Notification, Phase 2," HCCA Compliance Institute, March 31, 2014, p. 18.

[22] Sanches, Linda, "OCR Audits of HIPAA Privacy, Security and Breach Notification, Phase 2," HCCA Compliance Institute, March 31, 2014, p. 20.

[23] In fact, the Health Resource and Services Administration notes that the Meaningful Use program is not designed to spur adoption of EHRs, but rather to spur the effective use thereof. http://www.hrsa.gov/healthit/meaningfuluse/MU%20Stage1%20CQM/mu.html. The Meaningful Use program is also available to Eligible Hospitals, but they are not the focus of this chapter. For more information on the

The Centers for Medicare and Medicaid Services ("CMS") published regulations governing the Meaningful Use program in 2010.[24] Modifications to the regulations were published in September, 2012, and again in September, 2014.[25]

Under the program, EPs can receive up to almost $44,000 total over a period of up to five years, for participating in three stages of the program requiring EPs to satisfy increasingly difficult criteria for payment through the use of certified EHR software.[26] Stage 1 of the Meaningful Use program began in 2011, with Stage 2 launching in 2014, and Stage 3 expected to premiere in 2016. In general, Stage 1 is designed to capture reported data by EPs and share the information with patients and/or other providers. Stage 2 requires that EPs begin to perform certain "advanced clinical processes," and Stage 3 is intended to lead to improved outcomes. All EPs begin the process in Stage 1, but incentive payments are not available for EPs who began reporting after 2014.[27] For those who met the Stage 1 criteria for between two and three years (those who began participating in 2011 or 2012, and continued to participate in subsequent years), EPs were required to meet the criteria for Stage 2.

By April, 2012, approximately *$4.5 billion* in incentive payments had been distributed to EPs and hospitals, with $339.9 million directed to EPs alone.[28] To ensure that incentive payments were being properly awarded, and as required under the HITECH Act,[29] CMS and its contractor, Figliozzi & Co.,[30] began post-payment audits of EPs that same year.[31] Any EP who receives an

Meaningful Use program generally, see Shay, Daniel, ñPQRS and Its Penumbra,ò Health Law Handbook¸ 2012 ed., pp. 87-119.

[24] 75 Fed. Reg. 44314, July 28, 2010.

[25] 77 Fed. Reg. 53968, September 4, 2012; 79 Fed. Reg. 52910, September 4, 2014.

[26] Although EPs who begin participating in later years receive less money, since incentive payments are scheduled to end in 2016. Thus, an EP who began reporting in 2014 would only receive a maximum of $23,520. See, Medicare and Medicaid EHR Incentive Program Basics, at http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Basics.html. In addition, due to a sequestration order issued by President Obama on March 1, 2013, the total amounts payable under the Meaningful Use program were reduced by up to $300 per year. For more information, see ñAn Introduction to: Medicare EHR Incentive Program for Eligible Professionals,ò at http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Getting_Started.html. For a current list of certified EHRs, see the Office of the National Coordinator for Health Information Technology ("ONCHIT" or simply "ONC") list, at http://oncchpl.force.com/ehrcert?q=chpl.

[27] ñAn Introduction to: Medicare EHR Incentive Program for Eligible Professionals,ò p.16. Separate from the incentive payment portions of Meaningful Use, and beginning in 2015, EPs who fail to meet reporting criteria (or who simply decline to participate at all) will face payment reductions, also known as ñpayment adjustments.ò

[28] Mosquera, Mary, "CMS EHR Incentives Reach $4.5B," Government Health IT, April 20, 2012, at http://www.govhealthit.com/news/cms-ehr-incentive-payments-reach-45b.

[29] HITECH Act, Section 13411; 42 USCA 17940.

[30] http://www.figliozzi.com/.

[31] Plank, Kendra Casey, "Meaningful Use Participants Begin Receiving Audit Letters from Contractor," BNA Health IT Law & Industry Report, July 25, 2012, at http://www.bna.com/meaningful-participants-begin-

EHR incentive payment may be selected as the subject of an audit.[32] In 2013, CMS announced that it would begin *pre-payment* audits of EPs.[33] This development actually represented a reversal by CMS, which had previously taken a position against pre-payment audits.[34]

To assist participating EPs, CMS has published several documents that describe the audit process, and outline the kind of information that must be supplied. Current audits begin with a notification letter from Figliozzi & Co. (but listing a CMS email address), sent electronically to the email address provided during registration for Meaningful Use.[35] A sample letter has been posted on CMS' website.[36] The letter includes an information request list, supplied as an attachment to the letter itself. The information requested may be submitted electronically as per instructions attached with the letter, or by mail, and must be supplied by a deadline stated in the letter.

Initial reviews of submitted information are desk reviews, although CMS describes that additional information may be requested, and an onsite review might be required to demonstrate the EP's certified EHR system.[37] Following the audit, the EP receives an Audit Determination Letter from the auditor, which states whether the EP was successful in meeting the Meaningful Use requirements for their reporting year and stage. When the EP is determined to have not met the requirements, the *entire* Meaningful Use payment must be returned.

n12884910824/. The article notes that, at this time, CMS had not formally announced that it had begun auditing EPs, but news was reported on law firm Ober Kaler's website, at http://www.ober.com/publications/1882-figloiozzi-company-begin-meaningful-use-audits-cms-designee. At the same time, CMS did post a FAQ on its website, identifying Figliozzi & Co. as its contractor for Meaningful Use audits, which remains available today at https://questions.cms.gov/faq.php?id=5005&faqId=7361.

[32] http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/RegistrationandAttestation.html.

[33] EHR Incentive Programs Audits Overview, at www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/EHR_Audit_Overview_FactSheet.pdf.

[34] In an October 9, 2012 response to recommendations by the OIG that CMS implement pre-payment audits, then-Acting Administrator of CMS Marilyn Tavenner stated that "The CMS does not believe prepayment audit is necessary at this juncture...To change [the attestation and review] process and implement pre-payment audits could significantly delay payments to providers." Early Assessment Finds That CMS Faces Obstacles in Overseeing the Medicare EHR Incentive Program, p. 30, available at www.oig.hhs.gov/oei/reports/oei-05-11-00250.pdf.

[35] EHR Incentive Programs Supporting Documentation for Audits, February 2013, available at www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/EHR_SupportingDocumentation_Audits.pdf.

[36] www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/SampleAuditLetter.pdf. A similar sample audit letter has been published for Eligible Hospitals and Critical Access Hospitals, available at www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/EHR_SupportingDocumentation_AuditsEHCAP.pdf.

[37] EHR Incentive Programs Supporting Documentation for Audits, February 2013, available at www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/EHR_SupportingDocumentation_Audits.pdf.

3 Where Practices Fail

In this new environment of HIPAA and Meaningful Use audits, physician practices face significant penalties for failing to meet their compliance obligations. It is better, therefore, to proactively comply rather than to be required to do so by Federal enforcers, while also under financial burdens from penalties, fines, or repayments. Designing an effective compliance approach for both HIPAA and Meaningful Use, however, is difficult without an understanding of likely problems for each area of compliance.

3.1 HIPAA Failures

The OCRôs Audit Pilot Program provided valuable information regarding which areas the OCR determined to be the most problematic for purposes of compliance with HIPAAôs Privacy, Security, and Breach Notification Rules. In April and May of 2013, and again in March of 2014, the OCR published slide decks from PowerPoint presentations outlining their findings.[38] First, and perhaps most noteworthy of these findings from the 2012 audits, was that small providers had trouble with all three areas.[39] Of the total range of audit subjects, small providers accounted for the largest number of findings.[40] Collectively, breach notification and privacy accounted for 40% of the findings; security issues, on the other hand, accounted for 60% of the total findings.[41]

[38] Sanches, Linda, "HIPAA Privacy, Security and Breach Notification Audits -- Program Overview & Initial Analysis," HCCA 2013 Compliance Institute, April 23, 2013, at www.hcca-info.org/Portals/0/PDFs/Resources/Conference_Handouts/Compliance_Institute/2013/Tuesday/500/504print2.pdf; Rinker, Verne, JD, MPH, ñHIPAA Privacy, Security and Breach Notification Audits -- Program Overview & Initial Analysis,ò 2013 NIST / OCR Security Rule Conference, May 21-22, 2013, at http://csrc.nist.gov/news_events/hipaa-2013/presentations/day1/rinker_day1_215_hipaa_privacy_security_breach_audits.pdf; Sanches, Linda, "OCR Audits of HIPAA Privacy, Security and Breach Notification, Phase 2," HCCA Compliance Institute, March 31, 2014, at http://www.hcca-info.org/Portals/0/PDFs/Resources/Conference_Handouts/Compliance_Institute/2014/tue/710print2.pdf. The May 21-22, 2013 presentation provides some of the most helpful information, given that the slide deck is in color. The two presentations from Linda Sanches are in greyscale, which can result in some slides being difficult to decipher, due to confusingly similar color schemes in pie charts, bar graphs, and the like. Accordingly, the remainder of this chapter references the Rinker presentation in May, 2013, which contains a slide deck identical to the one from the Sanches presentation in April, 2013. The March presentation from Ms. Sanches contains similar information, but is not identical, and is therefore included in the citations.

[39] Rinker, Verne, JD, MPH, ñHIPAA Privacy, Security and Breach Notification Audits -- Program Overview & Initial Analysis,ò 2013 NIST / OCR Security Rule Conference, May 21-22, 2013, p. 18; Sanches, Linda, "OCR Audits of HIPAA Privacy, Security and Breach Notification, Phase 2," HCCA Compliance Institute, March 31, 2014, p. 4.

[40] Of the four different levels of covered entities audited, Level 4 (small providers) accounted for 41% of the total findings during the audit process. Rinker, Verne, JD, MPH, ñHIPAA Privacy, Security and Breach Notification Audits -- Program Overview & Initial Analysis,ò 2013 NIST / OCR Security Rule Conference, May 21-22, 2013, p. 19; Sanches, Linda, "OCR Audits of HIPAA Privacy, Security and Breach Notification, Phase 2," HCCA Compliance Institute, March 31, 2014, p. 5.

[41] Breach notification accounted for 10%, while privacy represented 30%. Rinker, Verne, JD, MPH, ñHIPAA Privacy, Security and Breach Notification Audits -- Program Overview & Initial Analysis,ò 2013 NIST / OCR Security Rule Conference, May 21-22, 2013, p.21; Sanches, Linda, "OCR Audits of HIPAA Privacy, Security and Breach Notification, Phase 2," HCCA Compliance Institute, March 31, 2014, p. 5.

From these findings alone, it is reasonable to expect that small providers will likely be targeted more by the OCR in the future; the OCRôs data shows that small providers like physician practices are more likely to have problems maintaining compliance with HIPAA. Moreover, these small providers are most likely to have problems specifically with compliance under the Security Rule, although the Privacy and Breach Notification Rules also present a challenge to such small providers. The OCR has provided more granular information on these areas, and how covered entities failed to meet their compliance requirements.

Given that Breach Notification Rule issues represented only 10% of the total issues found, it seems that the OCR may be less concerned (for the time being) with Breach Notification Rule compliance than with other areas. Still, with respect to this Rule, the OCR found that covered entities had problems with: providing notification to individuals, the timeliness of notification, the method of notification used, and the burden of proof in demonstrating that notification had been provided or that no breach had occurred.[42] Small providers represented the majority of covered entities that had difficulties in these areas (58%, 57%, 63%, and 52%, respectively).[43]

As with Breach Notification Rule issues, small providers alone represented over half of the number of Privacy Rule problems found.[44] Small providers faced the most difficulty with uses and disclosures of PHI (accounting for 43% of the findings for small providers in this area), followed by problems with notices of privacy practices (20%), administrative requirements (19%), access to PHI by individuals (16%), and right to request privacy protections (2%).[45] For administrative issues, the OCR noted that the largest number of problems arose from policies and procedures.[46]

[42] Rinker, Verne, JD, MPH, ñHIPAA Privacy, Security and Breach Notification Audits -- Program Overview & Initial Analysis,ò 2013 NIST / OCR Security Rule Conference, May 21-22, 2013, p.30; Sanches, Linda, "OCR Audits of HIPAA Privacy, Security and Breach Notification, Phase 2," HCCA Compliance Institute, March 31, 2014, p. 8.

[43] Rinker, Verne, JD, MPH, ñHIPAA Privacy, Security and Breach Notification Audits -- Program Overview & Initial Analysis,ò 2013 NIST / OCR Security Rule Conference, May 21-22, 2013, p.30; Sanches, Linda, "OCR Audits of HIPAA Privacy, Security and Breach Notification, Phase 2," HCCA Compliance Institute, March 31, 2014, p. 8.

[44] Rinker, Verne, JD, MPH, ñHIPAA Privacy, Security and Breach Notification Audits -- Program Overview & Initial Analysis,ò 2013 NIST / OCR Security Rule Conference, May 21-22, 2013, p.24.

[45] Rinker, Verne, JD, MPH, ñHIPAA Privacy, Security and Breach Notification Audits -- Program Overview & Initial Analysis,ò 2013 NIST / OCR Security Rule Conference, May 21-22, 2013, p. 23.

[46] Although, problems were also noted with training, complaints, and sanctions. Rinker, Verne, JD, MPH, ñHIPAA Privacy, Security and Breach Notification Audits -- Program Overview & Initial Analysis,ò 2013 NIST / OCR Security Rule Conference, May 21-22, 2013, p.25.

However, by far the most problematic area was compliance with the Security Rule. Of 59 providers audited, 58 had at least one problem relating to Security Rule compliance.[47] Of these providers, 47 had no complete security risk assessment.[48] Small providers represented over 50% of the total number of findings in each of the areas audited by the OCR: risk analysis (68%), access management (71%), security incident procedures (55%), contingency planning and backups (74%), media movement and destruction (67%), encryption (69%), audit controls and monitoring (65%), and integrity controls (67%).[49]

It is no surprise, therefore, that the OCR announced that its Phase 2 audits would be heavily focused on Security Rule compliance. Moreover, given how highly represented small providers were in the Phase 1 audit findings with regards to all levels of compliance, the OCR can reasonably be expected to focus its auditing and enforcement efforts on small providers for the foreseeable future. It appears that many small providers, including physician practices, have been lax in their duties with respect to maintaining compliance with these Rules. However, the OCR has noted that the most common reason for the bulk of its findings was that the covered entity being audited was simply unaware of its obligations, rather than a flagrant disregard for them.[50]

The focus on Security Rule compliance can also be seen in several resolution agreements (ñRAsò).[51] Fact patterns leading to RAs included lost or stolen thumb drives and laptops[52], and

[47] Rinker, Verne, JD, MPH, ñHIPAA Privacy, Security and Breach Notification Audits -- Program Overview & Initial Analysis,ò 2013 NIST / OCR Security Rule Conference, May 21-22, 2013, p.27.

[48] The problem was not limited to providers alone ï 2/3 of all entities surveyed had no complete security risk assessment. Rinker, Verne, JD, MPH, ñHIPAA Privacy, Security and Breach Notification Audits -- Program Overview & Initial Analysis,ò 2013 NIST / OCR Security Rule Conference, May 21-22, 2013, p.27.

[49] Rinker, Verne, JD, MPH, ñHIPAA Privacy, Security and Breach Notification Audits -- Program Overview & Initial Analysis,ò 2013 NIST / OCR Security Rule Conference, May 21-22, 2013, p.29.

[50] Approximately 30% of all compliance failures by audited entities were the result of lack of awareness of the requirement, which can be further broken down by Rule: 39% Privacy Rule, 27% Security Rule, and 12% Breach Notification Rule. Other reasons for non-compliance were incomplete implementation, lack of application of sufficient resources, and complete disregard. Rinker, Verne, JD, MPH, ñHIPAA Privacy, Security and Breach Notification Audits -- Program Overview & Initial Analysis,ò 2013 NIST / OCR Security Rule Conference, May 21-22, 2013, p.31.

[51] While it is true that the auditing efforts and enforcement efforts are not directly tied together, as a general matter, RAs represent an excellent source of information to see how the OCR actually enforces HIPAA, and what types of fact patterns lead to enforcement under the different Rules, as well as the settlement amounts that entities were required to pay, and the remedial steps the entities were required to take to satisfy the OCR. These can be found at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/index.html.

[52] See, Lowes, Robert, "Physician's Stolen Laptop Leads to $1.5 Million Settlement," Medscape Medical News, September 21, 2012, located at http://www.medscape.com/viewarticle/771348. For the full resolution agreement and HHS press release, see, "Massachusetts Provider Settles HIPAA Case for $1.5 Million," at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/meei-agreement.html. See also, Thuerk, Sarah, ñDerm Practice Pays $150K Settlement for Stolen Patient Data,ò Dermatology Times, January 7, 2014, at http://dermatologytimes.modernmedicine.com/dermatology-times/content/tags/dermatology/derm-practice-pays-150k-settlement-stolen-patient-data?page=full. For the full resolution and HHS press release, see http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/apderm-agreement.html. See also, Conn, Joseph,

even improperly configured servers such that ePHI was made public online, and would even appear in Google search results, as well as posting patient appointments on public, Internet-based calendars.[53] Typically, these cases resulted in the disclosure of thousands of patient records[54], which required the covered entities to report the incidents to the OCR as breaches. The breach notification, in turn, prompted an investigation by the OCR, which revealed a variety of faults.

The most common issues included: a total failure to conduct a security risk analysis as required by the regulations (or an ineffectively conducted analysis)[55]; ineffective or non-existent risk management plans to address security risks and vulnerabilities[56]; and, failure to (or ineffectively) implement policies and procedures to prevent, detect, contain and correct security violations.[57] Other issues included failures to document reasons why ePHI was left unencrypted, and failure to implement physical safeguards.[58]

ñUnencrypted-Laptop Thefts at Center of Recent HIPAA Settlements,ò Modern Healthcare, April 23, 2014, at http://www.modernhealthcare.com/article/20140423/news/304239945. For the full resolutions and press release, see ñStolen Laptops Lead to Important HIPAA Settlements,ò at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/stolenlaptops-agreements.html.

[53] See, Friedman, Lauren F., ñHospital to Pay Millions After Embarrassing Data Breach Put Patient Info on Google,ò Business Insider, May 9, 2014, at http://www.businessinsider.com/new-york-presbyterian-columbia-hipaa-settlement-2014-5. For the HHS press release and resolution agreement, see ñData Breach Results in $4.8 Million in Settlements,ò at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/jointbreach-agreement.html. See also, ñHHS Settles Case with Phoenix Cardiac Surgery for Lack of HIPAA Safeguards,ò HHS Press Release, at http://www.hhs.gov/news/press/2012pres/04/20120417a.html. The full resolution agreement is available at, http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/pcsurgery_agreement.pdf.

[54] See, the New York-Presbyterian and Columbia University settlements, involving approximately 6,800 records, at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/jointbreach-agreement.html; the Massachusetts Eye and Ear Institute settlement, involving 3,600 records, at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/meei-agreement.html; and the Adult & Pediatric Dermatology settlement, involving 2,200 records, at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/apderm-agreement.html. However, the number of disclosed records that prompt enforcement can even be as low as 148, as in the QCA Health Plan settlement, at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/stolenlaptops-agreements.html.

[55] See, the New York-Presbyterian and Columbia University settlements, at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/jointbreach-agreement.html.

[56] See, the Massachusetts Eye and Ear Institute settlement, at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/meei-agreement.html.

[57] See, the QCA Health Plan and Concentra Health Services settlements, at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/stolenlaptops-agreements.html. See also, the Phoenix Cardiac Surgery settlement, at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/pcsurgery_agreement.html. Phoenix Cardiac Surgery failed in numerous areas, including failing to establish a business associate agreement with the entity that provided the Internet-based calendar where ePHI was stored, failing to establish administrative and technical safeguards to prevent workforce members from transmitting ePHI over personal email accounts, failing to identify a security official, and failing to conduct an accurate and thorough risk assessment.

[58] The circumstances involved a laptop stolen out of one of Concentraôs physical therapy facilities. Presumably, this would not have been possible, had Concentra complied with the requirements to maintain physical security of ePHI, including measures relating to facility access and workstation use and control, under 45 CFR 164.310. Moreover,

Settlement amounts ranged from a low end of $100,000[59] all the way up to $3.3 million[60], with several covered entities paying approximately $1.5 million.[61] Remedial efforts imposed by the OCR typically included requiring the covered entity to: conduct (or in some cases, re-do) a security risk analysis that accounted for the entityôs entire IT infrastructure; develop risk management plans, in some cases including specific timelines to complete remedial actions; review existing policies and procedures, and revise them to address issues such as information access management, device and media controls, and the development of security awareness training programs.

Performing a security risk analysis *after* the incident does not protect the covered entity from the imposition of monetary penalties, nor OCR oversight. Adult & Pediatric Dermatology, for example, conducted a security analysis almost a full year after the reported breach, and was still fined $150,000 and required to re-do their security risk analysis, develop a risk management plan, and revise their policies and procedures relating to security, all of which had to be submitted to the OCR for review.[62] Similarly, Concentra Health Services conducted a full security risk analysis and the start of remediation actions in June, 2012 ï seven months after it reported the theft of a laptop containing unencrypted ePHI ï but still was required to pay $1.7 million, conduct another security risk analysis, develop a risk management plan, and provide the OCR with evidence of all of its implemented and planned remediation actions for the risks it discovered.[63]

Concentra had encrypted 434 out of 597 laptops, but had not documented why some laptops remained unencrypted nor how it had reached the decision to leave them unencrypted. See, the Concentra RA, at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/concentra_agreement.pdf.

[59] As in the case of Phoenix Cardiac Surgery. See, the Phoenix Cardiac Surgery RA, at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/pcsurgery_agreement.pdf. Similarly, Adult & Pediatric Dermatology, which involved an unencrypted thumb drive stolen from an employeeôs car, resulted in a $150,000 penalty. See, the Adult & Pediatric Dermatology RA, at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/concentra_agreement.pdf.

[60] As in the case of New York-Presbyterian Hospital, where approximately 6,800 patient records were made searchable on Google. See, the New York-Presbyterian Hospital RA, at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/ny-and-presbyterian-hospital-settlement-agreement.pdf.

[61] Massachusetts Eye & Ear Infirmary paid three installments of $500,000 each. See, the Massachusettes Eye & Ear Infirmary RA, at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/meei-agreement-pdf.pdf. Columbia University paid a total of $1.5 million for its involvement in the New York-Presbyterian Hospital case. See, the Columbia University RA, at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/columbia-university-resolution-agreement.pdf. Concentra Health Services paid over $1.7 million. See, the Concentra Health Services RA, at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/concentra_agreement.pdf.

[62] See, the Adult & Pediatric Dermatology RA, at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/concentra_agreement.pdf.

[63] Because Concentra had identified that it maintained unencrypted ePHI as early as October, 2008, and had otherwise failed to document a reason for not encrypting the data, it also had to provide information on its encryption status, including the percentage of devices and equipment that had been encrypted 120 days after signing its RA, and proof that all new devices purchased had been encrypted. It also had to provide an explanation for the

3.2 Meaningful Use Failures

There is no "partial credit" under the Meaningful Use program; failure to comply with the full requirements for successful participation means that the EP failed to qualify for the incentive payment, or avoid a payment adjustment. Thus, for EPs who have already attested that they successfully participated, a single improper attestation will invalidate their entire payment, and the EP will have to return the money. Unfortunately, enforcement of the Meaningful Use program and collection of incentive payments has not been as widely publicized as the OCR's efforts regarding HIPAA enforcement have. As a result, there are fewer public records available to provide guidance on the types of errors that participating EPs and hospitals have made. Still, there is some information to be gleaned from both enforcement efforts and voluntary repayments of Meaningful Use funds that have been publicized in one form or another.

One area where both small practitioners and larger institutions have faced difficulties is with respect to the certification of the EHR software itself. The Office of National Coordinator for Health Information Technology (ONCHIT) certifies EHR software for use in the Meaningful Use program.[64] This certification is a prerequisite for participation in the Meaningful Use program.[65] Even if an EP successfully meets the other requirements for the Meaningful Use program, if the requirements were not met using certified software, the EP failed to qualify for the Meaningful Use payment.

In one particularly high-profile case, Health Management Associates (HMA) reported repaying $31 million in incentive payments, for improper Meaningful Use attestations for 11 hospitals.[66] According to the press release, after conducting an internal review, HMA determined that "it had made an error in applying the requirements for certifying its EHR technology under these programs" for payments received between July 1, 2011 and June 30, 2013. The company voluntarily repaid the amounts (determined as $8.3 million in 2011, $17.3 million in 2012, and $5.4 million for the first half of 2013), and had to restate its financial statements for the years ending on December 31, 2010, 2011, and 2012, and the quarters ending March 31 and June 30, 2013.

percentage of devices *not* encrypted, and conduct security awareness training. See, the Concentra Health Services RA, at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/concentra_agreement.pdf.

[64] For general information on the certification process, see http://www.healthit.gov/policy-researchers-implementers/about-onc-hit-certification-program. For a list of currently certified EHR software, see http://www.healthit.gov/policy-researchers-implementers/certified-health-it-product-list-chpl.

[65] See generally, 42 CFR 495.6. Many of the core measures for EPs, hospitals, and critical access hospitals require the use of certified EHR technology.

[66] "Health Management Associates Announces Restatement of Financial Statements," MarketWatch.com, November 5, 2013. http://www.marketwatch.com/story/health-management-associates-announces-restatement-of-financial-statements-2013-11-05?reflink=MW_news_stmp.

Some hospitals and physician groups have sued their EHR vendors for failing to obtain Meaningful Use certification for their software.[67] This area also is likely to become more problematic for Meaningful Use attestation under the 2014 Stage 1 requirements. At the time of this writing, the ONCHIT list of certified EHR products lists 3,808 individual entries for certified software for the 2011 edition of the Stage 1 requirements for ambulatory practice types (as opposed to inpatient practice types); the 2014 edition lists 1,237.[68] While it is likely that ONCHIT will certify more software in the future, the list of available certified software may still be smaller for the 2014 edition and beyond, as compared to the list of software certified for the 2011 edition. As a result, EPs may have to engage in the costly, and time consuming process of switching software suites, or forego payment incentives and face the penalties imposed under the Meaningful Use program.

Other failures may arise from technical problems with the software itself that prevent the EP from meeting requirements. For example, our firm represented a client who faced a repayment of the incentive payments it had received, because its software was unable to function as described by the software vendor. Although the vendor stated it would be capable of doing so, the software was unable to electronically submit prescriptions to pharmacies.[69] In addition, the vendor failed to obtain certification for the software. As a result, the client was required to return *all* of the incentive funds it received for the year, although it was able to meet the reporting requirements in the following year.

One of the most prominent and problematic risks, however, is that associated with security risk assessments. Under the Meaningful Use program, for both Stage 1 and Stage 2, an EP must have conducted a security risk assessment in accordance with the requirements of 45 CFR 164.308(a)(1).[70] As with all other Meaningful Use requirements, failure to satisfy this core measure means the EP is ineligible for incentive payments, and will be subject to penalties in 2015 and beyond. Given the glaring problems relating to security risk analyses by the OCR's HIPAA audits, this issue could prove a double-whammy, especially for physicians and physician practices. Not only do they face exposure under HIPAA, but they may also have to repay whatever incentive payments they have received to date.

[67] Conn, Joseph, "Montana Hospital Sues Developer Over Electronic Health-Record Certification," Modern Healthcare, January 7, 2014, http://www.modernhealthcare.com/article/20140107/NEWS/301079958. In this case, Mountainview Medical Center sued NextGen Healthcare Information Systems for failing to provide a certified EHR system in a timely manner. Bandell, Brian, "Class Action Lawsuit in Miami-Dade Targets Allscripts," South Florida Business Journal, January 3, 2013, http://www.bizjournals.com/southflorida/news/2013/01/03/class-action-lawsuit-in-miami-dade.html?page=all. In this case, the plaintiff claimed that approximately 5000 small group physicians were sold defective software by Allscripts, with part of the claim resting on the fact that Allscripts said it would obtain Meaningful Use certification, but failed to do so because of the software's defects.

[68] Note that these numbers reflect only the individual entries counted on the certification list. Some software may be certified using multiple configurations, or for use with specific mixes of other required software, meaning that there may be even fewer actual EHRs available for use, and that the numbers are inflated due to the options for different configurations of those EHRs.

[69] Required as a core measure for Stage 1. 42 CFR 495.6(d)(4).

[70] For Stage 1, 42 CFR 495.6(d)(14); for Stage 2, 42 CFR 495.6(j)(16).

4 **Practical Guidance**

The risks posed by both HIPAA and Meaningful Use audits are significant. Physicians can face repayments of Meaningful Use incentives, and the imposition of Meaningful Use payment adjustments. Likewise, physicians can face fines for HIPAA violations, and may have to undertake time-consuming and costly remedial steps under the watchful eye of federal enforcers. However, there are preventive steps that physician practices can take to avoid these problems. This section discusses several of these steps, focusing on the security risk analysis, and explores the guidance offered both by the OCR and by CMS with respect to HIPAA and Meaningful Use audits and compliance.

4.1 The Security Risk Analysis

The importance of the security risk analysis to both HIPAA and Meaningful Use compliance cannot be overstated. With respect to Meaningful Use, it is a core measure; as discussed above, a failure to meet any of the core measures required under the program means that the EP (1) was not a meaningful user during the reporting year, and therefore cannot be eligible for payment of incentives, and (2) faces penalties during the penalty phase of Meaningful Use.

With respect to HIPAA, the security risk analysis is even more important: it is the keystone of the entirety of a covered entity's Security Rule compliance efforts.[71] Without an effective security risk analysis, all of the steps the covered entity takes to comply with HIPAA's Security Rule are suspect. If the covered entity has not conducted a security risk analysis of all of its ePHI, it cannot know, for example, whether it has implemented "security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level" to comply with HIPAA requirements[72]; it cannot determine the appropriate manner of protecting health information transmissions[73]; nor can it effectively decide whether and how to use encryption.[74] The OCRôs audit program results demonstrate that it is aware that many covered entities have not performed a security risk analysis, especially physicians and physician groups. Likewise, the OCRôs enforcement efforts with respect to security-related incidents frequently determine that no security risk analysis had been conducted prior to the incident, or that what had been conducted was ineffective and/or incomplete. It is therefore reasonable to expect that physicians and physician practices will be subject to increasing scrutiny on this issue.

[71] The OCR describes the risk analysis as "foundational," and as the first step in identifying and implementing safeguards that comply with and carry out the requirements of the Security Rule. "Guidance on Risk Analysis Requirements Under the HIPAA Security Rule," p.1, July 14, 2010, at www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf.

[72] 45 CFR 164.308(a)(1)(ii)(B).

[73] 45 CFR 164.312(e)(1).

[74] 45 CFR 164.312(a)(2)(iv) and (e)(2)(ii).

While it is not required under either HIPAA or Meaningful Use, an "outsourced" security risk analysis can be extremely helpful, rather than a physician office "self-diagnosing." Security risk analyses require a particular kind of thinking that incorporates both an understanding of the legal requirements, and technical knowledge regarding a wide range of technology (including EHR software functionality, network architecture, and electronic security standards). A consultant experienced in these areas will likely be far more effective at conducting a thorough analysis than a physician practice's compliance officer or whichever individual is responsible for IT issues. For that matter, the consultantôs expertise will likely outstrip an attorneyôs when it comes to technical matters. For example, one issue a consultant may examine that many attorneys may be totally unaware of is the degree of security applied to wi-fi networked printers, which can be an entry point for hackers to access a physician practiceôs IT infrastructure. However, the analysis should be conducted in coordination with an attorney. The attorney will have a better sense for the contours of the regulatory requirements, understanding the grey areas in how the regulations can be interpreted. In addition, if the attorney engages the consultant to conduct the analysis on behalf of the physician client, then the results of the analysis may be protected as attorney work-product. While the value of asserting attorney work-product privilege over information ï some of which may be required to be disclosed in response to a HIPAA or Meaningful Use audit ï may be questionable, it is better to be able to argue that the material is privileged and ultimately have to disclose, than to not be able to make the argument because an attorney was never involved.[75]

The analysis itself need only be conducted on a periodic basis. Based on guidance posted by ONCHIT on HealthIT.gov, this means that the analysis should be reviewed and updated when an EHR is obtained, or when changes to practice electronic systems occur.[76] While the Meaningful Use program requires that a *review* of the security risk analysis be conducted for each reporting period, it does not require a full security risk analysis be performed each year. Moreover, all risks need not be mitigated before submitting an attestation under Meaningful Use; rather, the program requires that deficiencies identified during the risk analysis be corrected during the reporting period, as part of the risk management process.[77] CMS has further elaborated on this, explaining that,

[75] In the preface to the 2002 Privacy Rule final rule, HHS responded to a comment that the requirement at 45 CFR 164.504(e)(ii)(I) that business associates ï including attorneys ï make information relating to the use and disclosure of PHI available to the Secretary of HHS could jeopardize attorney-client privilege. HHS stated that ñThe Privacy Rule is not intended to interfere with attorney-client privilege. Nor does the Department [of HHS] anticipate that it will be necessary for the Secretary to have access to privileged materials in order to resolve a complaint or investigate a violation of the Privacy Rule.ò However, given that it is also a regulatory requirement that a security risk analysis be conducted ï and the necessity of being able to prove that to HHS ï it is unclear how far privilege would extend with respect to a security risk analysis. At the very least, a final report for the analysis would likely not be privileged, however, communications with the consultant and other documentation associated with the analysis might remain privileged.

[76] "Top 10 Myths of Security Risk Analysis," HealthIT.gov, at http://www.healthit.gov/providers-professionals/top-10-myths-security-risk-analysis.

[77] "Top 10 Myths of Security Risk Analysis," HealthIT.gov, at http://www.healthit.gov/providers-professionals/top-10-myths-security-risk-analysis.

> "These steps may be completed outside of the EHR reporting period timeframe, but must take place no earlier than the start of the EHR reporting year and no later than the provider attestation date. For example, a EP who is reporting Meaningful Use for a 90-day EHR reporting period may complete the appropriate security risk analysis requirements outside of this 90-day period as long as it is complete no earlier than January 1st of the EHR reporting year and no later than the date the provider submits their attestation for that EHR reporting period."[78]

The documentation supporting a practice's policies and procedures relating to its Security Rule compliance efforts must be maintained for six years, for both HIPAA and Meaningful Use purposes.[79]

The OCR has published guidance that addresses certain basic elements that must appear in all security risk analyses.[80] For example, the scope of the analysis must address the potential risks and vulnerabilities to all of the ePHI created by a covered entity[81], including all forms of electronic media, ranging from hard drives to PDAs, and individual workstations to local computer networks. The analysis must also identify and document potential threats and vulnerabilities to the covered entity's ePHI.[82] However, this and other guidance makes it clear that there is also no single prescribed form that a security risk analysis must take.[83]

This offers consultants and attorneys some flexibility with respect to what the final security risk analysis document looks like, and when one can state that such an analysis has been performed. For example, if an EP is nearing a deadline for Meaningful Use attestation and needs to have the

[78] CMS Frequently Asked Question: "How can a provider meet the 'Protect Electronic Health information' core objective in the Electronic Health Records (EHR) Incentive Programs?", at https://questions.cms.gov/faq.php?faqId=10754.

[79] 45 CFR 164.316(b)(2)(i).

[80] "Guidance on Risk Analysis Requirements Under the HIPAA Security Rule," July 14, 2010, at www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf.

[81] The OCR guidance refers to "organizations," which includes both covered entities and their business associates. "Guidance on Risk Analysis Requirements Under the HIPAA Security Rule," p. 1. Given that this chapter is focused primarily on physicians and physician practices, it refers to covered entities to avoid confusion.

[82] Other elements include documenting the method by which the covered entity determined where ePHI is stored, received, maintained, or transmitted; assessing current security measures; determining the likelihood of threats occurring and the potential impact on such threats; and assigning risk levels to all identified threats and vulnerabilities.

[83] "Guidance on Risk Analysis Requirements Under the HIPAA Security Rule," p. 6. See also, "Top 10 Myths of Security Risk Analysis," HealthIT.gov, at http://www.healthit.gov/providers-professionals/top-10-myths-security-risk-analysis. With respect to Meaningful Use, CMS has published a document titled "Security Risk Analysis Tipsheet: Protecting Patients' Health Information." In addition to addressing the same "Top 10 Myths," the Tipsheet includes some security areas that EPs should consider and offers examples of potential security measures that can be taken to address them. It is available at, www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/SecurityRiskAssessment_FactSheet_Updated20131122.pdf.

analysis completed prior to attesting, an informal report could be generated prior to the consultant producing a longer, more thorough report, to allow the EP to attest in time. In these circumstances, the analysis would still be complete in time, even if the longer-form final report was not completed prior to attestation, as long as the analysis allowed the EP to begin to correct identified security deficiencies and develop a risk management plan. According to CMS, the report must at least document the procedures performed during the analysis and the results, should be dated prior to the end of the reporting period, and should include evidence to demonstrate that it was generated for the EPǿs system (such as an NPI number, provider name, practice name, etc.).[84]

The risk to EPs with respect to failing to conduct a security risk analysis also implicates provisions of the Fraud Enforcement Recovery Act of 2009 (FERA), as well as provisions of the Patient Portability and Affordable Care Act of 2010 (PPACA) that apply to retention of overpayments as applied to the Federal False Claims Act (FCA). FERA modified the FCA to make the ñimproper retentionò of overpayments a false claim; PPACA further modified this to establish that an ñimproper retentionò occurs when the entity retaining the overpayment knew or should have known that the monies paid were an overpayment, and that overpayment is retained for longer than 60 days once identified.[85] As applied to Meaningful Use payments, this means that if an EP attested that it qualified for Meaningful Use in a given reporting period, any monies paid as a result of that attestation constitute an overpayment if the EP has not actually conducted a security risk analysis. Similarly, as applied to the penalty phase of the Meaningful Use program, attestation to avoid the imposition of a penalty would mean that any monies paid which were higher than what would have been paid if the penalty had been imposed would constitute an overpayment. In other words, *all* of the EPǿs Medicare payments would be impacted, since the penalty phase imposes up to a 2.0% reduction of all of the EPǿs Medicare payments.

4.2 Additional MU Practical Advice

With respect to compliance with Meaningful Use requirements, CMS has published several helpful documents. Much of the information on CMSô EHR Incentives Program web page relates to the process of registration, attestation, etc., and is not directly related to security risk analyses nor to Meaningful Use audits, although it is still extremely helpful for EPs looking to navigate the program.[86] However, CMS has published two guides that provide information on the Meaningful Use audit process.

[84] ñEHR Incentives Program Supporting Documentation for Audits,ò p.4.

[85] PPACA § 6402.

[86] The main page is located at, http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/index.html?redirect=/ehrincentiveprograms/. The Educational Resources page can be found at, http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/EducationalMaterials.html. The Educational Resources page also includes documents regarding objectives and clinical quality measures for Stage 1 and Stage 2, FAQs, registration guides, etc. For EPs and attorneys with questions about the program, the website may prove quite helpful.

The EHR Incentive Programs Audits Overview provides general information about the Meaningful Use audit process, describing the steps that are involved in an audit[87]; CMS has also posted a sample audit letter from Figliozzi & Company.[88] More useful, however, are the two documents relating to the supporting documentation that will be required to respond to an audit for Stage 1 or Stage 2.[89] The key takeaway from these publications relates to documentation retention. As discussed above, supporting documentation must be retained for six years following attestation.[90] Much of the documentation is typically in the form of a report generated by the EPôs certified EHR. If the EHR cannot produce such a report, other documentation may be required. CMS advises that ñProviders who use a source document other than a report from the certified EHR systemé should retain all documentation that demonstrates how the data was accumulated and calculated.ò[91]

The ONC and CMS have both emphasized that EPs should not rely on or assume that their EHR vendor is taking care of managing these issues for them.[92] Instead, an EP should address these issues prior to attestation and/or an audit, taking into account the functionality of their EHR. For example, the EP should determine whether its EHR can print the kind of reports necessary for attestation, and if not, should create periodic screenshots or printouts to capture this information. The task for maintaining this documentation should be assigned to one or two individuals in the practice (or more, depending on the EP's practice size) with a good understanding of what

[87] Available at, http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/EHR_Audit_Overview_FactSheet.pdf

[88] Available at, http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/SampleAuditLetter.pdf.

[89] ñEHR Incentives Program Supporting Documentation for Audits,ò and ñStage 2 EHR Incentive Programs Supporting Documentation for Audits,ò available at http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/EHR_SupportingDocumentation_Audits.pdf and http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/Stage2_AuditGuidance.pdf, respectively.

[90] 45 CFR 164.316(b)(2)(i).

[91] ñEHR Incentives Program Supporting Documentation for Audits,ò p.3. This publication also describes the minimum information that will be required, including numerators and denominators for measures, time period covered by the report, and evidence to support that the information was generated for that EP based on NPI number, provider name, etc. With respect to Stage 2 documentation, the EP should also be able to produce evidence that the report was generated by the certified EHR system, such as a screenshot of the report before it was printed from the system. ñStage 2 EHR Incentive Programs Supporting Documentation for Audits,ò p.3.

[92] A fact reiterated in publications both from CMS and from ONC. Both documents address the misconception that the EHR vendor has taken care of Security and Privacy Rule compliance, by responding that "Your EHR vendor may be able to provide information, assistance, and training on the privacy and security aspects of the EHR product. However, EHR vendors are not responsible for making their products compliant with HIPAA Privacy and Security Rules. It is solely your responsibility to have a complete risk analysis conducted." "Top 10 Myths of Security Risk Analysis," HealthIT.gov, at http://www.healthit.gov/providers-professionals/top-10-myths-security-risk-analysis; "Security Risk Analysis Tipsheet: Protecting Patients' Health Information," p.4, at, http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/SecurityRiskAssessment_FactSheet_Updated20131122.pdf.

information is being attested to, and the documentation requirements for that attestation. Even if the EP's EHR can produce the required reports automatically, it still may be beneficial to retain backups throughout the year, both in electronic and hard copy. These steps should all be decided early in the reporting period, and internal audits can be conducted periodically to determine whether the EHR is properly capturing and reporting data, and whether the individuals are retaining hard and electronic copies of whatever information the EHR does not itself report. By adopting these measures early in the process, the EP should be able both to effectively attest meaningful use, and to respond to an audit.

If the EP is audited and receives a negative determination, all hope may not be lost. CMS has established an appeals process for EPs to challenge certain adverse determinations relating to Meaningful Use.[93] In general, the type of information that may be included in an appeal of a failed audit must not be information already submitted to Figliozzi & Company.[94] The type of documentation that may be submitted includes proof of certified EHR possession, dated reports from the EHR that validate a range of measures and procedures performed for a security risk analysis, dated screenshots from the EHR taken during the attestation reporting period, and dated letters or emails verifying that a security risk analysis has been performed and the actions take in response to the findings or from a vendor verifying certified EHR possession or other measures.[95]

Unfortunately, the appeals process is not governed by regulations, and in fact, CMS declined to reduce the process to regulations. In the Final Rule for Stage 2 of Meaningful Use, CMS stated,

> "...After review of the public comments and the appeals filed as of the writing of this final rule, we believe the administrative review process is primarily procedural and does not need to be specified in regulation...We believe such an informal reconsideration process may be included in procedural guidance, rather than in our regulations."[96]

CMS' decision was partially influenced by the HITECH Act's restriction on administrative and judicial review of standards and methods used to determine eligibility and payment.[97] CMS does not view the Meaningful Use appeals process as permitting challenges of the standards and methods themselves, but rather permitting challenges of whether an EP met the standards. While

[93] The appeals process also permits appeals of negative determinations relating to eligibility for participation in the Meaningful Use program, and for failures to report meaningful use. See, "Eligible Professional (EP) Appeal Filing Request," available at http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Appeals.html. This page also includes an appeals form for eligible hospitals.

[94] In fact, the instructions for the appeals for explicitly prohibit resubmitting documentation previously requested by or submitted to an auditor. "Eligible Professional (EP) Appeal Filing Request," p.3.

[95] See, "Eligible Professional (EP) Appeal Filing Request," p.4.

[96] 77 Fed. Reg. 54112, September 4, 2012.

[97] 42 CFR 495.110.

it may seem a fine hair to split, it provides EPs with the best and only available method to challenge adverse determinations.

4.3 Additional HIPAA Practical Advice

Physicians and physician practices can best prepare for a HIPAA audit by preemptively achieving compliance. Towards this end, both physicians and the attorneys who advise them should avail themselves of the educational materials published by the federal government. Fortunately, there exists a wide range of such materials, which offer practical advice for establishing HIPAA compliance with the Security Rule as well as with the Privacy and Breach Notification Rules.

The HealthIT.gov website represents an excellent starting point for physicians attempting to comply with the various HIPAA Rules; the site includes a trove of regulatory guides, tools, and educational materials relating to Privacy and Security Rule compliance.[98] Two resources in particular offer guidance relating to Security Rule compliance: ñReassessing Your Security Practices in a Health IT Environment: A Guide for Small Health Care Practices,ò and ñCybersecurity ï 10 Best Practices for the Small Healthcare Environment.ò[99]

The first is geared towards practices of 10 or fewer health care providers[100], and includes examples of administrative, physical, and technical safeguards[101], as well as questions the practice can ask itself to help assess risks regarding and identify safeguards for EHRs and other health IT.[102] The types of questions posed help orient physician practices towards both the complexities relating to Security Rule compliance, as well as the fact that much of compliance in this area depends upon practical and technical considerations.

The second document offers a list of best practices, including explanations for each practice and checklists to implement these practices. For example, one such best practice addresses the use of

[98] http://www.healthit.gov/providers-professionals/ehr-privacy-security/resources.

[99] Available at http://www.healthit.gov/sites/default/files/smallpracticesecurityguide-1.pdf, and http://www.healthit.gov/sites/default/files/basic-security-for-the-small-healthcare-practice-checklists.pdf, respectively.

[100] ñReassessing Your Security Practices in a Health IT Environment: A Guide for Small Health Care Practices,ò p. 3.

[101] ñReassessing Your Security Practices in a Health IT Environment: A Guide for Small Health Care Practices,ò pp. 5-6.

[102] ñReassessing Your Security Practices in a Health IT Environment: A Guide for Small Health Care Practices,ò pp. 7-9. Examples of such questions include: Should all employees with acces to EHRs have the same level of access?ò, ñHow will I know if an EHR, or the electronic health information in the EHR, has been altered or deleted?ò, and ñHave I configured my computing environment where electronic health information resides using best-practice security settings (e.g., enabling a firewall, virus detection, and encryption where appropriate? Am I maintaining that environment to stay up to date with the latest computer security updates?ò

passwords, and advises that they be ñstrong passwords,ò[103] and advising that the passwords be changed frequently (at least quarterly) or that multi-factor authentication ï such as an electronic fob or fingerprint scanner.[104] The checklist for implementing this best practice includes more basic advice, such as passwords not being reused, not appearing on screen, not written down elsewhere, and not shared with others.[105] Other best practices include practical, technical advice such as using a firewall and virus protection software, limiting electronic and physical access to ePHI and the devices on which it is stored, and protecting and encrypting ePHI stored on mobile devices.

In both documents, the guidance is written in laymanôs terms, and is presented in a clear and straightforward fashion. This information can be coupled with ñhow not to do itò examples drawn from RAs (e.g., data on mobile devices should be encrypted, so as to avoid the fate of those covered entities who had unencrypted laptops and thumb drives stolen), to provide an overall context for Security Rule compliance.

Another useful resource for information as to the OCRs plans regarding future enforcement can be found in the OCRôs required reports to Congress.[106] These documents report on enforcement efforts by the OCR for the reporting period, but also address enforcement efforts that the OCR plans to take. For example, a 2009-2010 report noted that the OCR was in the process of developing audit protocols and establishing a pilot auditing program.[107] The 2011-2012 report noted that, facing increasing numbers of HIPAA-related complaints and unchanging resources, the OCR would ñwork smarter,ò by providing technical assistance and early intervention, rather than conducting full investigations. Investigations would be more focused on cases presenting ñcompliance issues that are pervasive in the health care industry or other serious allegations,ò especially in so-called ñhigh-impact cases,ò that involve investigations and compliance reviews that would result in ña substantial industry impactò so as to encourage compliance.[108] By reviewing this information, especially when considered alongside the OCRôs other enforcement

[103] Defined in the document as being at least 8 characters in length, including a mix of upper and lower-case characters, and not include words from the dictionary ï even with numbers swapped as letters, such as ñ4ò for ñAò or ñ7ò for ñTò ï and that they not include personal information such as a birthday, names, etc. ñCybersecurity ï 10 Best Practices for the Small Healthcare Environment,ò November 22, 2010, p. 8.

[104] ñCybersecurity ï 10 Best Practices for the Small Healthcare Environment,ò November 22, 2010, p. 8-9.

[105] ñCybersecurity ï 10 Best Practices for the Small Healthcare Environment,ò November 22, 2010, p. 25.

[106] The OCR is required under the HITECH Act to provide annual reports to Congress regarding its enforcement efforts. HITECH Act, Section 13424(a) for Privacy and Security Rule reports; HITECH Act, Section 13402(i) for Breach Notification Rule reports. The OCR reports may be found at, http://www.hhs.gov/ocr/privacy/hitechrepts.html.

[107] ñAnnual Report to Congress on HIPAA Privacy Rule and Security Rule Compliance For Calendar Years 2009 and 2010,ò August 11, 2011, p. 20, available at, http://www.hhs.gov/ocr/privacy/hipaa/enforcement/compliancerept.pdf.

[108] ñAnnual Report to Congress on HIPAA Privacy Rule and Security Rule Compliance For Calendar Years 2011 and 2012,ò May 20, 2014, p. 20, available at, http://www.hhs.gov/ocr/privacy/hipaa/enforcement/compliancerept.pdf.

efforts, it becomes clear that the areas where the OCR is actively enforcing are that much more relevant. Put simply, the OCR intends to send a message through its enforcement efforts that covered entities need to pay attention to issues such as Security Rule compliance.

However, one of the most helpful resources by far to respond to OCR audits is the OCR Audit Program Protocol itself.[109] This web page is an essential tool for covered entities (and business associates) to understand what the OCR specifically reviews when conducting an audit. The site lists a total of 169 entries, with 78 devoted to the Security Rule, 81 devoted to the Privacy Rule, and 10 devoted to the Breach Notification Rule. Each entry examines an ñEstablished Performance Criterionò (essentially, a given requirement under a regulatory section or subsection), the key activity that is expected to be taken to fulfill the requirement, the audit procedures the OCR takes to examine a covered entity with respect to the requirement, the level of ñimplementation specificationò (e.g., required or addressable), and the rule that applies.

The complexity of the site varies. While some regulations receive a single straightforward entry, others are addressed in multiple different entries to specifically examine different aspects of the regulatory requirement. For example, 45 CFR 164.404 ï which governs notification of individuals in the event of a breach ï has four separate entries to address (1) notification to individuals in general, (1) the timeliness of notification, (3) the methods of individual notification, and (4) the content of the notification. While the OCR generally will inquire of management as to whether a process exists to notify individuals, the precise information that the OCR will look for varies from entry to entry.[110]

The full scope of each entry and the type of actions the OCR will take and information it will examine is beyond the scope of this chapter, but much of the auditorsô focus is on documentation. For required specifications, there must be documentation that the action was taken.[111] For addressable specifications, there must be documentation showing how a covered entity determined to implement the addressable action (or not), and why the decision was made.[112] When the regulatory section does not address the required vs. addressable distinction,

[109] http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html. Note that the Audit Program Protocol indicates that it has not yet been updated to take into account the provisions of the Omnibus Rule published on January 25, 2013.

[110] For example, timeliness of notification requires the OCR auditor to verify that, if any breaches have occurred, the individuals have been notified within 60 days. Content of notification requires the OCR auditor to examine whether there is a standard template or form letter for notification, and to verify that, if any breaches have occurred, individuals have received letters containing all the elements required under the regulation.

[111] For example, to satisfy the requirement that a covered entityôs contingency plan for responding to disastrous events includes a recovery strategy, the OCR will ñInquire of management as to whether procedures exist for recovering documents from emergency or disastrous events. Obtain and review procedures and evaluate the content in relation to specified criteria for the recovery of documents from emergency or disastrous events. Determine if procedures are approved and updated on a periodic basis.ò

[112] For example, with respect to the addressable requirement to implement a mechanism to encrypt and decrypt ePHI, the auditor is instructed to ñInquire of management as to whether an encryption mechanism is in place to protect ePHI. Obtain and review formal or informal policies and procedures and evaluate the content relative to the specified criteria to determine that encryption standards exist to protect ePHIé If the covered entity has chosen not

as with many provisions of the Privacy and Breach Notification Rules, there must still be documentation ï usually in the form of policies and procedures ï regarding how the covered entity is meeting its regulatory requirements.[113]

Based on this information, it is clear that practices should develop policies and procedures that can respond to what OCR auditors will look for in the course of an audit. Where a regulatory requirement does not apply to the practice, the practiceôs policies and procedures should indicate as much and explicitly state that the requirement is not addressed because it does not apply, rather than being absent. Because so many of the auditing inquiries will be directed towards the practiceôs management, the management should familiarize itself with the practiceôs policies and procedures, as well as the process by which decisions were made in their development, so as to better respond to auditors.

By reviewing the Audit Program Protocol, as well as the other educational resources made available, physician practices and attorneys alike can gain a better understanding of how to reach compliance, and how to prepare for an audit. Audits will never be a pleasant process, but a practiceôs efforts to bring itself into compliance, and thoroughly document how it got to that point, all *before* an audit occurs will at least minimize the discomfort.

5 <u>Conclusion</u>

Audits for HIPAA and Meaningful Use, much like other increased government scrutiny of the health care industry[114], are unlikely to cease or be pared back in the future. The trajectory of government oversight with respect to HIPAA and Medicare incentive programs is instead one of ever-increasing scrutiny. Moreover, the federal government faces increasing budgetary and political pressure to ensure that its programs are operating efficiently, and that health care providers remain in compliance with the law. It is therefore reasonable to expect that the future holds yet more oversight in store for physicians and physician practices ï who have traditionally ñflown under the radarò of much government enforcement in these areas.

HIPAA and Meaningful Use both present complex and daunting regulatory schemes to physicians and physician practices. While many physicians have a general sense of what is required for compliance with the Privacy Rule, they often remain ignorant of their requirements with respect to the Security Rule. While a physician may know, generally, to use an encrypted patient portal to communicate with patients, the physician may not understand that merely having ñHIPAA compliantò software (as is often advertised) is not enough to meet the

to fully implement this specification, the entity must have documentation on where they have chosen not to fully implement this specification and their rationale for doing so. Evaluate this documentation if applicable.ò

[113] For example, with respect to the requirements of 45 CFR 164.526, regarding the right of an individual to request that their PHI be amended, the OCR auditors are instructed to ñInquire of management as to whether a policy exists regarding an individualôs right to amend their PHI in a designated record set. Obtain and review authoritative documentation to determine the individualôs right to amend PHI in a designated record set is included. Verify the process allows the individual the right to amend protected health information in a designated record set.ò

[114] Such as with respect to provider enrollment in the Medicare program.

requirements for the Security Rule. Similarly, while a physician may understand the day-to-day operation of their EHR software, the physician may not know how to manipulate that software so as to fully comply with Meaningful Use attestation requirements. It is one thing to know that one must counsel a patient on smoking cessation and check a box in the patientôs record in the EHR software; it is quite another to know how to make the software produce a report of such information over time, or even whether the software is fully capable of doing so.

For physicians and practices just beginning to confront these issues, the technical and highly detailed requirements for compliance can be bewildering and frightening ï all the more so if the physician or practice understands that it has *not* previously been compliant. Compliance requires a great deal of technical knowledge as well as legal knowledge, and the process of bringing a practice into compliance may be overwhelming. The temptation may be to ignore the problem because it is too complex and difficult for the practice to tackle, assuming that because no enforcement has previously occurred, the practice is probably safe. Alternatively, while recognizing the potential danger, the practice may procrastinate, assuming that theyôre safe ñfor nowò and will ñget to it later.ò However, as the OCRôs and CMSô enforcement efforts show, ñlaterò (or more accurately ñneverò in some cases) may often translate into ñtoo late.ò When a breach occurs or auditors come calling, the practice will discover that proverbial horses have already left the barn. Towards this end, it is the job of attorneys working in concert with compliance consultants to educate physicians and practices, and help them to tackle the issue of compliance with the Security Rule, and Meaningful Use. Nevertheless, physicians and physician practices need to be aware that with respect to OCR HIPAA and CMS Meaningful Use audits, the question is one of ñwhen,ò and not ñifò they will be subjected to an audit.

Of course, attorneys cannot be expected to preemptively solve all of a physician practice clientôs problems, and can only make suggestions about what constitutes a sound course of action. Moreover, the role of the attorney is not to address all of the technical considerations or resolve IT infrastructure problems. While it is certainly helpful for an attorney to understand the technical aspect of these issues ï so as to better advise the client ï an attorney cannot know all of the ins and outs of a practiceôs IT infrastructure, nor every nuance of how the practiceôs EHR software collects and reproduces Meaningful Use data.

Instead, the attorneyôs role is that of a guide through the compliance process. The attorney must educate the client on its need to address compliance directly, early, and often; the attorney must interface with practice compliance officers (in those practices large enough to have one), but can also direct physicians to information on the compliance process to make it easier to digest. Many of the citations in this chapter have been to documents written for a physician audience, rather than regulations and regulatory interpretations. This is by design. The cited documents are often written in plain language, and will help a client to understand the requirements with respect to Security Rule and Meaningful Use compliance, as well as providing guidance on the steps a practice can take to bring itself into compliance. Hopefully, this will help make the process less imposing, and make it appear that the practice can truly eat the compliance elephant one bite at a time.