**** Pre-Publication Draft****

HIPAA ENFORCEMENT ON THE BOOKS AND IN PRACTICE:

WHEN IT ALL GOES WRONG

By Daniel F. Shay, Esq.
Alice G. Gosfield and Associates, P.C.
2309 Delancey Place
Philadelphia, PA 19103
(P) 215-735-2384
(F) 215-735-4778
dshay@gosfield.com
www.gosfield.com

Accepted for publication in the Health Law Handbook, 2023 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

HIPAA Enforcement On the Books and In Practice:

When It All Goes Wrong

1. Introduction

For nearly thirty years, health care providers have been living with the provisions of the Health Insurance Portability and Accountability Act (HIPAA) of 1996[1]. Having existed since 2000[2], for most providers the specific requirements of the Privacy Rule[3] are likely the most familiar aspect of HIPAA. The Privacy Rule addresses rights for patients, as well as obligations for "covered entities" and "business associates," with respect to "protected health information" (PHI)[4] and impacts many day-to-day aspects of operation as a health care provider. In recent years, along with increased usage of electronic health records software, computer-based prescription order entry, and government incentives for the adoption of electronic health records infrastructure, health care providers have also become more familiar with the provisions of the Security Rule[5]. The Security Rule was first published in 2003[6], and imposes certain physical, technological, and administrative requirements relating to electronic PHI (ePHI). Some health care providers have had to address the requirements of the Breach Notification Rule[7], often through the unpleasant process of managing a possible breach. The Breach Notification Rule was first published in 2009[8] as an interim final rule, and in 2013[9] as a final rule. It governs how covered entities and business associates must respond to breaches of unsecured PHI (uPHI), including procedures for notifying individuals, the media, and the government upon the occurrence of a breach.

In spite of varying degrees of familiarity with the rules described above, many covered entities and business associates may be less familiar with the Enforcement Rule[10],

---

[1] P.L. 104-191.

[2] 65 Fed. Reg. 82462 (December 28, 2000).

[3] 45 CFR § 164.500, et seq.

[4] Definitions for each of these terms can be found at 45 CFR § 160.103.

[5] 45 CFR § 164.302, et seq.

[6] 68 Fed. Reg. 8334 (February 20, 2003).

[7] 45 CFR § 164.400, et seq.

[8] 74 Fed. Reg. 42740 (August 24, 2009).

[9] 78 Fed. Reg. 5566 (January 25, 2013).

[10] 45 CFR § 160.300, et seq.

although they are very likely aware of actual incidents of enforcement. This article will explore a range of issues relating to the Enforcement Rule. It will examine what the rule requires and how it is applied, as well as trends in enforcement. Finally it will examine specific instances of enforcement with an eye towards drawing from them practical guidance and insight on the enforcement process and how best to navigate it.

2. Enforcement Rule Overview

The Enforcement Rule covers several different aspects of HIPAA enforcement. Although the chief concern of this article is how the Enforcement Rule addresses (1) compliance and investigations, and (2) the imposition of civil money penalties (CMPs), the Enforcement Rule also covers matters pertaining to preemption of state law, and hearing procedures, which will not be addressed in detail. The preemption rules cover how the HIPAA regulations preempt state laws, as well as exceptions for state laws with requirements that are more rigorous than HIPAA's. The hearing rules cover the processes when a final determination of a HIPAA violation has been made, and the procedures whereby covered entities and business associates may challenge such determinations.[11]

Like other provisions of the HIPAA regulations, the Enforcement Rule has evolved over the years. It was originally published as part of the Privacy Rule in 2000.[12] Three years later, interim final rules were published.[13] Final rules were published in 2006.[14] These rules, as with the Privacy, Security, and Breach Notification Rules, were updated as part of the "Omnibus Rule," published in 2013.[15]

The government entity responsible for enforcing HIPAA is the Department of Health & Human Services' Office for Civil Rights (OCR). The greatest "stick" wielded by the OCR is the threat of CMPs, but they are only imposed following investigation of possible violations of HIPAA. Such investigations are usually accomplished by three different methods: (1) investigation of complaints submitted to OCR; (2) the performance of compliance reviews; and (3) the performance of "periodic audits."

The use of "periodic audits" was mandated with the passage of the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH)[16], which was itself part of the American Recovery and Reinvestment Act of 2009[17]. This prompted

---

[11] Preemption is addressed in 45 CFR §§ 160.200-160.205. Hearings are addressed at 45 CFR §§ 160.500-160.552.

[12] 65 Fed. Reg. 82462 (December 28, 2000).

[13] 68 Fed. Reg. 18895 (April 17, 2003).

[14] 71 Fed. Reg. 8390 (February 16, 2006). The commentary in the 2006 rule offers the most insight in to the meanings of the rules.

[15] 78 Fed. Reg. 5566 (January 25, 2013).

[16] P.L. 111-5, HITECH ACT, Section 13411.

[17] P.L. 111-5.

the development of an audit pilot program, which launched in 2011 and ran for roughly one year.[18] The pilot program was meant to determine the effectiveness of OCR's auditing protocol, as well as to understand those vulnerabilities faced by covered entities of which OCR was unaware. This resulted in a report that analyzed the pilot program's results, drew conclusions about the types of providers who had the greatest number of problems with HIPAA compliance, and the HIPAA requirements with which covered entities and business associates had the most trouble. Following the report, the OCR launched "Phase 2" of its audit program, which began in 2014. "Phase 2" completed in 2018, and a final report of the "Phase 2" audit results was published in 2020, at which point no further audits were initiated.[19] For the time being, the audit program has been paused, but it remains a mechanism by which the OCR may collect information surrounding possible HIPAA violations in the future.

2.1 Complaints & Investigations

The primary mechanism by which the OCR becomes aware of possible HIPAA violations is through its complaint system. Anyone who believes a covered entity or business associate is not complying with HIPAA may submit a complaint to the OCR; not merely affected patients.[20] The complaint must be filed in writing, either on paper or electronically. The complaint must include the subject of the complaint's name, and a description of the acts or omissions that are thought to be a violation of HIPAA. It must be filed within one hundred eighty days of the date on which the complainant knew or should have known that the act or omission occurred, although the OCR is permitted to waive the time limit for good cause.[21]

In addition to the 180-day window within which the complaint must be filed, the alleged violation must have occurred within the previous six years. That time limit is derived from the statute of limitations for the application of CMPs.[22] Because HIPAA only applies to covered entities and business associates[23], the complaint also must be filed against a covered entity or business associate or else it will be dismissed due to the OCR's lack of jurisdiction. The OCR provides all of this information on a website for prospective

---

[18] For more information on the HIPAA auditing programs, see Shay, Daniel F., "HIPAA and Meaningful Use Audits and the Security Risk Analysis Nexus," Health Law Handbook, 2015 ed., pp. 429-464.

[19] See, Annual Report to Congress on HIPAA Privacy, Security, and Breach Notification Rule Compliance for Calendar Year 2020, p. 8. Available at, https://www.hhs.gov/sites/default/files/breach-report-to-congress-2020.pdf. For the OCR's report, see, "2016-2017 HIPAA Audits Industry Report," published December, 2020, at https://www.hhs.gov/sites/default/files/hipaa-audits-industry-report.pdf.

[20] 45 CFR § 160.306(a).

[21] 45 CFR § 160.103(b).

[22] 45 CFR § 160.414.

[23] Defined at 45 CFR § 160.103.

complainants, which also describes what constitutes a covered entity or business associate in lay terms.[24]

Once the OCR receives the complaint, and accepts it for investigation, the OCR will notify both the complainant, and the covered entity or business associate that is the subject of the complaint. The OCR's discretion to pursue complaints depends on the facts discovered in the course of a preliminary review. Where the preliminary review discovers a possible violation arising from willful neglect, an investigation is mandated by law, although the OCR retains the discretion to investigate any complaint even if there is no willful misconduct.[25] Prior to the passage of the HITECH Act, every complaint investigation was at the OCR's discretion, but the HITECH Act added a provision that requires the investigation of cases involving willful neglect.[26]

During an investigation, the OCR may review a broad array of documents, such as policies, procedures, and practices. The OCR may request additional information from both the complainant, and the covered entity or business associate, to better assess and understand the facts. While complainants are not required to reply to these requests, covered entities are.[27]

2.2 Compliance Reviews

While most investigations derive from the OCR's formal complaint process, the OCR also conducts compliance reviews based on information from outside of the complaint process, including from breach notification reports, media reports, or other sources[28], although the OCR's discretion in conducting compliance reviews operates on the same basis as the complaint process. If a preliminary review of the facts indicates a possible violation that is due to willful neglect, the OCR is required by law to conduct a compliance review. However, as with the complaint process, the OCR retains discretion to conduct compliance reviews in any other circumstances.[29] As with the complaint process, prior to passage of the HITECH Act, the OCR was not required to conduct any compliance reviews.

---

[24] See, "What OCR Considers During Intake and Review," at https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/what-ocr-considers-during-intake-and-review/index.html.

[25] 45 CFR § 160.306(c).

[26] P.L. 111-5, HITECH Act, Section 13410(a). For a more information on these changes, see the discussion in the Omnibus Rule, at 78 Fed. Reg. 5478-5579 (January 25, 2013).

[27] 45 CFR § 160.310(b). See also, "How OCR Enforces the HIPAA Privacy & Security Rules," at https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/how-ocr-enforces-the-hipaa-privacy-and-security-rules/index.html.

[28] See, "Annual Report to Congress on HIPAA Privacy, Security, and Breach Notification Rule Compliance for Calendar Year 2020," p.11, available at, https://www.hhs.gov/sites/default/files/breach-report-to-congress-2020.pdf.

[29] 45 CFR § 160.308(a).

The HITECH Act again revised the compliance review process to make investigations mandatory in the case of suspected willful misconduct.[30]

There is little information available on what actually triggers an OCR compliance review. The regulations themselves do not provide any bases on which to conduct them, and the OCR has offered little by way of elaboration in its own public statements. This lack of specificity in what can prompt such a review apparently is by design. In the preface to the 2006 Enforcement Rule, the OCR responded to a comment requesting clarification on what prompts compliance reviews. The OCR demurred, explaining,

> "*Outlining specific instances in which a compliance review will be conducted could have the counterproductive effect of skewing compliance efforts towards those aspects of compliance that had been identified as likely to result in a compliance review. It also does not seem advisable to limit, by rule, the circumstances under which such reviews may be conducted at this early stage of the enforcement program, when our knowledge of the types of violations that may arise is necessarily limited."*[31]

The implication of this language is relatively straightforward: the OCR wants covered entities and business associates to focus on compliance itself, rather than on compliance review avoidance. The OCR recognized that enumerating specific triggers for compliance reviews would have the effect of encouraging covered entities and business associates to undertake only those compliance efforts necessary to avoid such reviews. One need not be a fortune teller to guess that this could also create potential vulnerabilities and HIPAA compliance failures, if the covered entities and business associates ignored other aspects of compliance, due to a myopic focus only on those issues which the OCR had stated could trigger a compliance review. To respond to the new problem areas that could develop, the OCR would be forced to revise its regulations – and going through the rulemaking process of publishing proposed regulations, soliciting and reviewing comments, and replying to those comments in a final rulemaking, all of which can take multiple months at least, only to see the process repeat itself after new areas became the focus and other areas were ignored. Thus, by not specifying what can trigger compliance reviews, the OCR forces covered entities and business associates to attend to all aspects of compliance, while simultaneously allowing the OCR to remain nimble in its enforcement efforts and avoid the need to undertake a lengthy rulemaking process merely to shift internal policy.

Compliance reviews impose certain responsibilities upon covered entities and business associates. First, a covered entity or business associate must retain records and submit compliance reports as required by the OCR, to permit the OCR to determine if the covered entity or business associate is in compliance with HIPAA.[32] In the course of a compliance review, covered entities and business associates must also cooperate with OCR requests to provide policies, procedures, or documentation of practices. In addition, the

---

[30] P.L. 111-5, HITECH Act, Section 13410(a); 45 CFR § 160.308.

[31] 71 Fed. Reg. 8396 (February 16, 2006).

[32] 45 CFR § 160.310(a).

covered entity or business associate must provide the OCR with access (during normal business hours) to its physical facilities, books, records, accountants, and other sources of information, including PHI. In the case of "exigent circumstances" (e.g., if the OCR has good reason to believe that documents have been or are being hidden or destroyed), then the access to such records must be provided at any time, and without notice.[33] In other words, if the OCR has good reason to believe that a covered entity is hiding or destroying records, the OCR may demand access outside of regular business hours or conduct "spot inspections" without prior notice to the covered entity.

The Enforcement Rule also includes regulations governing how the OCR should approach requests for information that is in the exclusive possession of a party other than the covered entity or business associate when that other party refuses to provide the information[34], and a provision permitting the OCR to disclose PHI to law enforcement agencies such as the Department of Justice[35]. The OCR will refer to the DOJ or other law enforcement authorities when it determines that there has been a criminal violation of HIPAA[36]; the OCR only has jurisdiction to enforce civil violations of HIPAA, and lacks jurisdiction to enforce criminal violations. This regulatory language allowing referrals to other agencies was added with the publication of the Omnibus Rule in 2013. In the preface to the Omnibus Rule, the OCR responded to a commenter's request for clarification on how federal agencies would work together to enforce suspected violations.[37] In response, the OCR directed the commenter to the OCR's website, which contains much of the information described above.[38]

In addition to records requests, the OCR may also issue subpoenas (referred to as "investigational inquiries) to obtain witness testimony and to produce additional evidence. These proceedings are not public, but they are formal hearings where witnesses are sworn under oath or affirmation, and the hearings are recorded and transcribed. The regulations also specify requirements for the content of the subpoena and the method by which it may be served, as well as rules governing the investigational inquiry proceeding itself. For example, the regulations state that witnesses must be given an opportunity to clarify their answers on the record following questioning by OCR; that claims of privilege by witnesses must be asserted on the record, as well as objections; and, whether non-witnesses are

[33] 45 CFR § 160.310(b), (c).

[34] 45 CFR § 160.310(c)(2).

[35] 45 CFR § 160.310(c)(3).

[36] Criminal provisions for HIPAA can be found at 42 USC § 1320d-6.

[37] For the Omnibus Rule discussion of this change, see 71 Fed. Reg. 5579 (January 25, 2013).

[38] See, "How OCR Enforces the HIPAA Privacy & Security Rules," at https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/how-ocr-enforces-the-hipaa-privacy-and-security-rules/index.html.

permitted to attend (although witnesses may be accompanied, advised, and represented by an attorney).[39]

2.3 After the Investigation or Compliance Review – Informal Resolution

Following the conclusion of a complaint investigation or compliance review, the OCR will make a determination as to whether HIPAA was violated. If there is no violation, the OCR closes the case and informs the covered entity or business associate, as well as any complainant, in writing that the matter has been closed. When noncompliance has been determined, however, the OCR is permitted to attempt to "reach a resolution of the matter satisfactory to the Secretary [of Health and Human Services] by informal means," which may include that compliance has been demonstrated by the covered entity or business associate, or that the covered entity or business associate has completed a corrective action plan or other agreement.[40]

In practice, this means that one of three outcomes has occurred: (1) voluntary compliance, (2) corrective action, and/or (3) a resolution agreement. Voluntary compliance occurs when the covered entity or business associate, which was initially not in compliance with the rules, manages to rectify the matter to the OCR's satisfaction without the OCR's assistance; in other words, the covered entity or business associate fixed the problem itself, and the OCR is mollified. The OCR may also offer "technical assistance," ranging from reminding a covered entity or business associate of its regulatory options, to providing specific guidance tailored to the covered entity or business associate's area of noncompliance. Resolution agreements are settlements wherein the covered entity or business associate enters into an agreement with the OCR to meet certain obligations, and in some cases to pay a percentage of the penalties the covered entity or business associate might owe if the OCR were to impose a CMP.[41]

The OCR has stated that most Privacy and Security Rule investigations end up concluding to the OCR's satisfaction using these approaches.[42] As the Enforcement Rule itself states, and as this article will illustrate, the primary goal of the OCR is not to impose penalties, but rather, "to the extent practicable and consistent with the provisions of [Subpart C, on Compliance and Investigations], seek the cooperation of covered entities and business associates in obtaining compliance with the applicable [HIPAA regulations]."[43]

---

[39] For additional information, see, 45 CFR § 160.314.

[40] 45 CFR § 160.312.

[41] For more information, see, "How OCR Enforces the HIPAA Privacy & Security Rules," at https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/how-ocr-enforces-the-hipaa-privacy-and-security-rules/index.html, and "Enforcement Data," at https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/index.html.

[42] See, "How OCR Enforces the HIPAA Privacy & Security Rules," at https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/how-ocr-enforces-the-hipaa-privacy-and-security-rules/index.html.

[43] 45 CFR § 160.304(a). The OCR has further stated that it "will seek to resolve matters by informal means enforce issuing findings of non-compliance, under its authority to investigate and resolve complaints, and to engage in compliance reviews." 68 Fed. Reg. 18897 (April 17, 2003).

Each of the three outcomes discussed above – voluntary compliance, corrective action, and resolution agreements – are informal resolutions. Even the fact that the resolution agreement itself is a formal document, its use is still considered part of the "informal means" by which the OCR may resolve HIPAA noncompliance. The alternative is formal enforcement: the imposition of CMPs.

2.4 After the Investigation or Compliance Review – CMPs

Once the OCR makes a "final determination" that a covered entity or business associate has violated one or more of the HIPAA rules, it must impose a CMP. This process is mandatory, if a final determination has been made; the OCR has no discretion to waive a CMP at that point.[44] As will become clear, it is far preferable for a covered entity or business associate to avail itself of one of the informal resolution processes above. However burdensome or painful remedial action and a potential settlement amount may be, the imposition of a CMP will be worse.

The amount of the CMP will vary depending on the covered entity or business associate's actual knowledge of the noncompliance, and what it could have known or learned through the exercise of reasonable diligence.[45] The annual cap on identical violations in a calendar year for all types of violations, without regard to the level of knowledge or care, is $1,919,173.[46] If a covered entity or business associate did not know and could not by the exercise of reasonable diligence have known of the violation, the penalty is between $127 and $63,973 for each provision violated. For a violation due to reasonable cause where there is no willful neglect, the penalty is between $1,280 to $63,973 per violation. For violations caused by willful neglect, but which are corrected during a 30-day period that begins on the first date the covered entity or business associate knew or could have known (by exercising reasonable diligence), the penalty for each violation is between $12,794 and $63,973. For violations due to willful neglect which are not corrected during the 30-day window, the per-violation amount is $63,973. Of course, determining the total amount of a CMP requires a determination on the total number of violations.

The number of violations depends on the covered entity or business associate's obligation to act (or not act) under the violated provision, such as an obligation to act (or not act) in a certain manner, within a specific timeframe, or with respect to specific persons.[47] For example, under the Privacy Rule, a covered entity must respond to requests

---

[44] 45 CFR § 160.402(a). The OCR may, however, waive a CMP when a covered entity or business associate submits information in support of such a waiver, as permitted under 45 CFR §

[45] 45 CFR § 160.404.

[46] 45 CFR § 160.404(b). Note that the penalty amounts in this regulatory section are inaccurate and serve merely as a baseline. They are adjusted annually, in accordance with adjustments to all CMPs published at 45 CFR § 102.3. As of this writing, updates for 2023 have not yet been published, so this article refers to the 2022 values.

[47] 45 CFR § 160.406.

to amend PHI within 60 days of an individual's request.[48] A covered entity also must appoint a privacy officer as part of its administrative obligations under the Privacy Rule.[49] A covered entity must not disclose PHI for reasons other than those specified in its notice of privacy practices, unless a patient signs an authorization. Each of these requirements can form the basis for an instance of noncompliance, and ongoing violations are treated as a separate instance for each day that they persist.

The preface to the 2006 Enforcement Rule offers a further illustration of this concept. It highlights how covered entities are required to enter into business associate agreements (BAAs) that contain two provisions: (1) a prohibition on the further disclosure of PHI in a manner that would violate the Privacy Rule, and (2) a requirement that the business associate use appropriate safeguards to prevent the use or disclosure of PHI other than as provided for in the underlying agreement.[50] If a covered entity enters into five different BAAs with five different business associates, and each BAA lacks both of the above provisions, the covered entity will be treated as having committed five violations of <u>each</u> of the two requirements (i.e., ten violations total).[51] As a result, in practice, total penalties can end up being quite significant, even with the annual limits on identical violations.

Federal common law rules of agency also apply to the imposition of CMPs, which can raise the question of "When is a business associate acting as an 'agent' of a covered entity?" The key to answering this question is the degree of control exercised by the covered entity over the performance of the business associate. The mere existence of a BAA between the parties does not itself create an agency relationship under these rules, nor does the title of a relationship. The critical question is whether the covered entity has the authority to give "interim instructions or directions" to the business associate; in other words, whether the covered entity has more direct control over the business associate's actions. In the Omnibus Rule, the OCR offered some examples, noting that where the only avenue of control by a covered entity is to either amend the terms of the agreement with its business associate or sue for breach of contract, no agency relationship exists. By contrast, if a covered entity has authority to direct the performance of the service in question once the relationship is established, then the business associate may be an agent of the covered entity.[52]

The OCR also takes mitigating and aggravating factors into account when determining the amount of a CMP. These include the nature and extent of the violation itself (such as the number of individuals affected, and the time period during which the violation occurred); the nature and extent of the harm caused by the violation (such as

---

[48] 45 CFR § 164.526.

[49] 45 CFR § 164.530.

[50] The general requirements for the content of a BAA can be found at 45 CFR § 164.504(e).

[51] 71 Fed. Reg. 8406 (February 16, 2006).

[52] For additional discussion of agency between covered entities and business associates, see 71 Fed. Reg. 8402-8404 (February 16, 2006); and, 78 Fed. Reg. 5581-5582 (January 25, 2013).

whether the violation caused physical harm; financial harm; harm to an individual's reputation; or whether it hindered the individual's ability to obtain health care); the covered entity or business associate's history of prior compliance and violations (such as whether the current violation is the same or similar to previous violations; whether and to what extent the covered entity or business associate has tried to correct prior noncompliance; how the covered entity or business associate has responded to technical assistance from the OCR; and how the covered entity or business associate has responded to prior complaints); and the financial condition of the covered entity or business associate (such as its size and ability to continue providing health care services).[53] Relatedly, the regulations allow for certain affirmative defenses to be raised by a covered entity or business associate.[54] Specifically, the OCR may forego imposing a CMP if the covered entity or business associate demonstrates to the OCR's satisfaction that the violations in question were not due to willful neglect, and were corrected during the 30-day period after it knew or should have known of the violation (or such additional period as the OCR may determine is appropriate).[55] It is also an affirmative defense (although hardly an ideal position) if the violation in question is a criminal violation of HIPAA.[56] The OCR also is permitted to waive the imposition of CMPs, in whole or in part, if the payment of a penalty would be excessive relative to the violation.[57] A CMP cannot be imposed more than 6 years after the date of the violation.[58]

Of course, the goal for most covered entities and business associates should be to avoid the imposition of CMPs in the first place. As the OCR's own reports of its enforcement activities show, this is a reasonable possibility as long as the covered entity or business associate takes its compliance efforts seriously and responds promptly to investigations, compliance reviews, and its own discoveries of possible HIPAA violations.

3. Trends in Enforcement

An understanding of the Enforcement Rule regulations is useful in recognizing what steps the OCR may take, and how enforcement actions and investigations may proceed. However, covered entities and business associates can better develop HIPAA compliance strategies by looking at the rules as they are applied in practice. While the ideal for covered entities and business associates is to achieve full compliance with HIPAA, it is reasonable to expect that these efforts will not always be wholly successful. Therefore it is

---

[53] 45 CFR § 160.408.

[54] 45 CFR § 160.410.

[55] 45 CFR § 160.410(c). This specifically applies to violations occurring on or after February 18, 2009. Due to the six-year statute of limitations on HIPAA civil penalties, this means that the provisions of 45 CFR § 160.410(a)(1) and (b) – which apply to violations occurring prior to February 18, 2011, and February 18, 2009, respectively – no longer apply.

[56] 45 CFR § 160.410(a)(2). Criminal violations are described in 42 USCA § 1320d-6.

[57] 45 CFR § 160.412.

[58] 45 CFR § 160.414.

helpful to understand which issues are the most common subjects of enforcement, the better to tailor compliance plans to focus on areas of greater potential exposure. The OCR's own website provides a wealth of information about enforcement trends, chiefly from three main sources: (1) publicly reported statistics and data, (2) resolution agreements and specific reported enforcement actions, and (3) reports to Congress.

3.1 Statistics and Data

The OCR's website contains a range of data including general information and "top-five" lists of common problem areas in HIPAA. For example, the OCR posts information on "Enforcement Results By Year," which analyzes a broad array of data points, including the total number of cases investigated (and the total number of cases overall), and the outcomes of complaints, compliance reviews based on breaches, and other compliance review investigations.[59] The data posted on this website covers a timeframe from 2018 through 2021; more current data has yet to be posted. It indicates that complaints are the primary basis for investigations. For the timeframe described above, the total number of cases per year ranged between roughly 31,000 and almost 40,000. Between 25,000 and 30,000 were the result of complaints, and this also tracks to the total number resolved each year. "Resolution" includes resolution after intake and review, investigations where no violation was determined, cases where post-investigational technical assistance was offered, and cases where corrective action was obtained. Technical assistance was offered in roughly 4,200 to 9,000 cases per year.

By contrast, compliance reviews were relatively uncommon: only between 438 and 573 cases per year resulted in a compliance review. The imposition of CMPs was even more rare, with only 10 to 19 CMPs imposed each year, amounting to less than 1% of all investigated cases per year, and less than 0.1% of total cases in any given year. For cases that went beyond preliminary review and preliminary resolutions, and which resulted in investigations, corrective action was obtained in most instances: between 995 and 1,357 cases each year. The raw numbers here likely paint the clearest picture of the OCR's goal of securing compliance. Given the miniscule number of CMPs in comparison to the various forms of informal resolution, it is clear that the OCR is not looking to mount heads on pikes, so to speak.

In addition, the OCR has published a "Top Five Issues in Investigated Cases Closed With Corrective Action, by Calendar Year" page. This page again covers the time period between 2018 and 2021, with newer data not yet posted. For this time period, the list has remained generally consistent. The single biggest issue found in investigated cases that were closed by corrective action has always been "impermissible uses & disclosures" (of PHI); in other words, those cases where someone improperly accessed, transmitted, or otherwise used PHI. This is unsurprising, given the breadth of the category itself. There are myriad ways to "impermissibly use or disclose" PHI, ranging from accidentally faxing or emailing PHI to the wrong person, to intentionally using another person's login credentials or physical key to access records that the person is not entitled to see.

---

[59] See, "Enforcement Results by Year," at https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-results-by-year/index.html.

The remaining issues have fluctuated in their order on the list, but have mostly included: Safeguards (generally speaking), Administrative Safeguards (as distinct from general Safeguards, and likely referring to the administrative safeguards under both the Privacy and Security Rule), and Access (meaning patient access to their own PHI). The final spot has varied between: Breach Notifications to Individuals, Minimum Necessary, and Technical Safeguards (which is specific to the Security Rule). Some of these issues are unsurprising to see on the list. As is discussed in more detail below, patient Access to their own PHI has been a focus of the OCR for several years now, and has formed the basis for dozens of resolution agreements. The presence of Safeguards, Administrative Safeguards, and Technical Safeguards likewise is unsurprising. In most cases where there is some kind of HIPAA violation, having appropriate safeguards in place likely would have prevented the violation from happening. While the list does not offer much detail, it does highlight the common areas where covered entities and business associates run afoul of HIPAA, and thus can inform the focus of future compliance efforts.

3.2 Case Examples

The specific experiences of other covered entities and business associates can be revealing. At a surface level, much like the "Top 5" list referenced above, these experiences can provide a general sense of common types of HIPAA violations. But they can also provide more specific insight into how these covered entities and business associates have failed to comply, how the OCR responded to such failures, and in many instances how the covered entity or business associate itself responded to the OCR's actions. The OCR website offers two resources towards these ends: case examples and resolution agreements.

The case examples consist of short summaries of certain incidents, but which lack certain specific information such as the names of the parties and details of their interactions with the OCR. Nevertheless, they provide a useful insight into how the OCR actually operates in practice. They also include tags that indicate the types of HIPAA compliance problems involved. As with the "Top 5" list, the overwhelming majority of case summaries deal with "impermissible uses & disclosures," with the next most common issues being safeguards and access. The examples can be organized by covered entity type, or by issue.[60]

For example, consider "Radiologist Revises Process for Workers Compensation Disclosures," a case involving "impermissible uses & disclosures." A radiology practice interpreted imaging tests and then submitted claims to workers compensation. One patient, however, was not a workers compensation patient, and the practice improperly shared the patient's PHI with the workers compensation payor. An investigation determined that the practice had relied upon incorrect billing information received from the hospital that took the radiology images, leading to the erroneous submission. The practice took corrective actions, including apologizing to the patient, sanctioning the employee who was responsible (although the case example does not describe the nature of

[60] See, "Case Examples," at https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/index.html.

the sanction), re-training billing and coding staff, and revising the practice's policies and procedures to require a specific request from a workers compensation carrier before submitting test results to them. The example does not include the name of the practice, however, and describes no steps taken by the OCR aside from investigating. It is unclear from the summary whether the OCR provided technical support of any kind, although it does not appear that the OCR imposed any kind of penalties or entered into any agreement with the practice such as a resolution agreement.

Another example is "Private Practice Implements Safeguards for Waiting Rooms." Again, the case involved impermissible uses and disclosures, but also included "safeguards." A staff member discussed HIV testing procedures with a patient in a waiting room, thereby inadvertently disclosing PHI to patients and other individuals also in the waiting room. Computer screens in the practice also were easily visible to other patients, and displayed patient information. The OCR required the provider to develop and implement policies and procedures regarding both administrative and physical safeguards relating to communicating PHI. In addition, the OCR required that the practice reposition computer monitors to prevent patients from seeing screens. The practice also installed computer monitor privacy screens, and re-trained its staff. Based on the description of the case, it seems that the OCR secured "corrective action" (or at least "voluntary compliance"), but there is no indication of any penalties, settlements or other resolution agreements.

Finally, consider the example of "Private Practice Revises Process to Provide Access to Records Regardless of Payment Source," in which patient "access" to records is the central issue. In this case, a practice denied a patient a copy of their medical records following an insurance company's request for an independent medical examination of the patient. The OCR determined that the patient was entitled to a copy of the records, and required the practice to revise its policies and procedures to reflect that a patient has a right to access their records, regardless of the source of payment for the medical services provided. Again, this matter appears to have been closed without the imposition of penalties, without a settlement, and even without much by way of remedial action taken by the covered entity.

These case examples demonstrate the OCR's focus on securing compliance either through voluntary self-correction, or through remedial steps requested by the OCR. When covered entities or business associates take these steps, the OCR is often satisfied, and does not seem to pursue enforcement further. The cases also highlight problem areas and show the ways in which covered entities and business associates run afoul of HIPAA.

3.3 Resolution Agreements and CMPs

Unlike the case examples discussed above, resolution agreements provide much more in-depth information. This includes the name of the covered entity or business associate involved, as well as details of the specific ways in which the covered entity or business associate violated HIPAA, and the corrective steps that the covered entity or business associate was required to take, as well as any settlements involved. Most end up resolved through the informal process described above, although there are some cases that result in CMPs.

For example, consider two cases both involving issues pertaining to patients being denied access to their medical records when the patient had an outstanding balance. Although these two cases are discussed in greater depth below[61], they are presented here in brief to illustrate the greater amount of information available in resolution agreements. In one instance, the practice had a six-figure CMP imposed, while in the other, the practice was required to pay less than $5,000. The first case involved ACPM Podiatry, a podiatric practice with multiple locations. A patient requested access to their records and was denied on two separate occasions, and submitted two separate complaints to the OCR. The OCR tried multiple times to contact the practice, but was generally ignored, resulting in the OCR imposing a $100,000 CMP.[62] This case stands in sharp contrast to that of Danbury Psychiatric Consultants, which also involved a patient requesting access to records and being denied by the practice. In this case, the OCR intervened, and the practice provided access and entered into a resolution agreement and corrective action plan, and paid a settlement of only $3,500.[63] There are significant differences in how each of the two practices behaved in these cases, but unlike the case examples discussed above, considerably more information is available to review and analyze.

The resolution agreements also offer insight into the OCR's enforcement priorities. For example, between 2019 and 2022, the OCR resolved 42 separate right of access cases as part of its Right of Access Initiative. Other common issues involve HIPAA breaches and Security Rule compliance (such as lost thumbdrives, stolen laptops, hacking breaches, or breaches due to the failure to implement effective administrative, technical, and/or physical safeguards). Specific resolution agreements are discussed more in-depth below.

3.4 Congressional Reports

The OCR also is required to submit reports to Congress, in accordance with the HITECH Act.[64]These reports can also provide insight into the OCR's enforcement trends, although the value of the reports depends heavily on the subject matter they cover.[65] Because the reports were first mandated as part of the HITECH Act, they only cover a period dating back to 2009. Second, in spite of the title of the OCR web page containing links to the reports, most of the reports focus only on breaches and the Breach Notification

---

[61] At 4.2. Technically, only one of the two cases was a "resolution agreement": that of Danbury Psychiatric Consultants. The other document was a Notice of Proposed Determination, used when the OCR intends to impose a CMP on the covered entity or business associate.

[62] See, ACPM Podiatry Notice of Proposed Determination, at https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/acpm-npd/index.html.

[63] See, Danbury Psychiatric Consultants Resolution Agreement & Corrective Action Plan, at https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/danbury-ra-cap/index.html.

[64] P.L. 111-5 Section 13402(i).

[65] The reports can be found on the OCR website page titled, "Report to Congress on Privacy Rule and Security Rule Compliance," at https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/reports-congress/index.html.

Rule; they do not address other violations of the Privacy or Security Rules. The HITECH section requiring the reports only requires the OCR to report on breaches (although the OCR may report on more than just breaches). Still, while they are narrowly focused, for breach-related trends, they provide some useful insight.[66]

The 2020 report, published in April, 2022, is the most informative of these. No newer reports have been published as of this writing. This report is the first to actually address broader Privacy and Security Rule compliance in addition to Breach Notification Rule compliance. It is therefore far more useful for purposes of analyzing trends in enforcement due to the breadth of issues covered and the enforcement actions taken in response.

The 2020 report takes numbers available elsewhere on the OCR's website[67], and provides additional context and more fine-tuned data. For example, the report explains that the number of complaints resolved in a year is actually the total of administrative closures, technical assistance closures, and investigated closures.[68] While these different types of closures are not defined within the report, one can surmise that administrative closures would include closures that are for reasons such as an improperly filed complaint, or where it is determined that no violation has occurred, or are otherwise resolved before a full investigation commences. Technical assistance closures are likely those where the covered entity or business associate received technical assistance, and the matter was closed as a result. Investigated closures likely involve cases where the OCR begins a formal investigation, and closes it once it determines that the covered entity or business associate has resolved the matter.

The report also clarifies that the new complaints received and complaints resolved in a calendar year are not the same as when the OCR carries a complaint investigation forward from the previous year, and that complaints resolved in a calendar year are not counted as "new" complaints in the year when they are resolved.[69] The report also makes clear that complaints can carry over from one year to another. For example, in 2020, the OCR received 27,182 new complaints, and carried 3,203 complaints over from 2019. There were 26,530 complaints resolved during 2020 (including some from prior years), and roughly 75% of those complaints were resolved before initiating an investigation. These pre-investigation resolutions could be for reasons such as the allegations involving an entity not covered by the HIPAA regulations, conduct that did not actually violate the regulations, or untimely allegations (e.g., beyond the statute of limitations). Roughly 5,000

[66] The focus of this article, however, is not solely on breach-related trends, and therefore the bulk of these reports are not analyzed here.

[67] Specifically, the "Enforcement Results by Year" information.

[68] "Annual Report to Congress on HIPAA Privacy, Security, and Breach Notification Rule Compliance for Calendar Year 2020," p. 9, footnote 6.

[69] "Annual Report to Congress on HIPAA Privacy, Security, and Breach Notification Rule Compliance for Calendar Year 2020," p. 9, footnote 5.

complaints were resolved by providing technical assistance rather than conducting an investigation.[70]

The report takes the top five complaint issues for resolved complaints, and provides actual numbers for them by subject area. For example, of the 26,530 complaints resolved in 2020, 714 involved impermissible uses and disclosures; 662 involved safeguards; 658 involved right of access; 265 involved Security Rule administrative safeguards; and 140 involved technical safeguards. The total number of complaints received also declined by 4% from 2019 to 2020.[71]

The report also breaks down data for compliance reviews, as distinct from complaint investigations. The report clarifies that compliance reviews are opened for all reports of breaches affecting 500 or more individuals, and for some reports of breaches impacting fewer than 500 individuals.[72] In the 2020 calendar year, 746 compliance reviews were opened which did not arise from complaints, with 659 compliance reviews initiated resulting from breaches of 500 or more individuals, and 15 resulting from breaches of fewer than 500 individuals. The 72 other reviews were based on incidents where the OCR received multiple complaints about a specific entity or practice, from media reports, or through other methods.[73] During 2020, 566 compliance reviews were closed, with 547 of these being based on breach reports, and 19 from other sources. In 86% of cases (485 cases), covered entities or business associates took corrected measures or paid a CMP. In 4% of cases (22 cases) , the OCR provided technical assistance after investigating, and in 9% of cases (51 cases), the OCR did not find sufficient evidence of a HIPAA violation. In only 1% of cases (8 cases) did the OCR determine it did not have jurisdiction to investigate the allegations.[74] Again, the OCR clarified that compliance reviews could span multiple years, and that reviews begun and reviews completed in a calendar year were not necessarily all from the same year. In other words, a completed review could have been initiated in a prior year, and reviews initiated in 2020 may not have been completed the same year and would carry forward.[75]

---

[70] "Annual Report to Congress on HIPAA Privacy, Security, and Breach Notification Rule Compliance for Calendar Year 2020," p. 9.

[71] "Annual Report to Congress on HIPAA Privacy, Security, and Breach Notification Rule Compliance for Calendar Year 2020," p. 9.

[72] "Annual Report to Congress on HIPAA Privacy, Security, and Breach Notification Rule Compliance for Calendar Year 2020," p. 11, footnote 8.

[73] "Annual Report to Congress on HIPAA Privacy, Security, and Breach Notification Rule Compliance for Calendar Year 2020," p. 11.

[74] "Annual Report to Congress on HIPAA Privacy, Security, and Breach Notification Rule Compliance for Calendar Year 2020," p. 11.

[75] "Annual Report to Congress on HIPAA Privacy, Security, and Breach Notification Rule Compliance for Calendar Year 2020," p. 11, footnote 9.

One notable metric was that the OCR secured roughly $13 million from monetary settlements based on only 8 compliance reviews.[76] This compares to a reported $2.5 million resulting from 11 complaint investigations where the OCR resolved matters through resolution agreements/corrective action plans and monetary settlements.[77] There were no complaints resolved by assessing CMPs.[78] While the dollar figures here are not inconsequential, the fact that they are based on a total of only 19 cases out of thousands of cases further emphasizes the OCR's position as being primarily concerned with securing compliance. Given the small number of cases in which money is recouped from covered entities or business associates, it seems that CMPs and settlement amounts used in conjunction with resolution agreements remain a risk that covered entities and business associates must take seriously, but one that is deployed only rarely.

4. Case Studies & Practical Guidance

An understanding of the Enforcement Rule can help guide health care providers, whether as covered entities or as business associates, in their efforts to maintain HIPAA compliance. Knowing how the Enforcement Rule actually functions can help health care providers to understand what the OCR is capable of doing, and what a covered entity or business associates' options are in the case of a possible violation. Reviewing the wealth of data published by the OCR can give health care providers a better sense of how the OCR actually employs the Enforcement Rule. However, much of this data is presented only in the aggregate and does not offer much insight into how covered entities or business associates should respond to an OCR investigation or compliance review. To glean this information, it can be helpful to review the resolution agreements and corrective action plans, and the notices of proposed determinations for the imposition of CMPs available on the OCR's website. By carefully reviewing how covered entities or business associates actually responded, one can gain a clearer understanding of best practices in responding to OCR investigations.

4.1 Impermissible Disclosures – Studies in Contrasts

In several cases, patients of covered entities (all dentists, in fact) posted negative reviews online, to which the practices responded in a manner that disclosed patient PHI. One of these cases resulted in the practice facing a CMP. The other two cases, however, resulted in resolution agreements and corrective action plans. Unsurprisingly, the way the practices responded differs sharply between the two different outcomes.

---

[76] The precise amount was $13,017,400. "Annual Report to Congress on HIPAA Privacy, Security, and Breach Notification Rule Compliance for Calendar Year 2020," p. 11. The specific compliance reviews that resulted in the settlements are listed in footnote 10.

[77] The precise amount was $2,537,500. "Annual Report to Congress on HIPAA Privacy, Security, and Breach Notification Rule Compliance for Calendar Year 2020," p. 10. The specific complaint investigations that resulted in the settlements are listed in footnote 7.

[78] "Annual Report to Congress on HIPAA Privacy, Security, and Breach Notification Rule Compliance for Calendar Year 2020," p. 10.

Consider the case of U. Phillip Igbinadolor, DMD, who treated a patient on two different occasions in 2013 and 2014. The patient posted a negative review on Dr. Igbinadolor's Google page in September, 2015, using a pseudonym to conceal their identity. The same day, Dr. Igbinadolor replied to the negative review, revealing the patient's actual name and detailing the treatment the patient had received and the patient's specific complaints, without a valid HIPAA authorization to do so.[79] The patient filed a complaint with the OCR in November, 2015, and the OCR notified Dr. Igbinadolor of its investigation in July, 2016.

In its initial data request, the OCR asked for copies of Dr. Igbinadolor's policies and procedures for responding to online patient reviews; policies and procedures covering general uses and disclosures of PHI; policies and procedures regarding safeguarding PHI; and, documentation of any HIPAA training performed by the practice both before and in response to the incident. The practice responded to OCR by acknowledging that it had replied to the patient's negative review, and providing the OCR with a copy of its Notice of Privacy Practices. However, the practice provided no documentation detailing policies and procedures or any training that was provided. In August, 2016, the OCR contacted the practice by telephone, informing that the online reply to the patient was an impermissible disclosure of PHI, and that the practice should remove the response. The OCR further informed the practice that it should develop policies and procedures (if none already existed) regarding use and disclosure of PHI, especially on social media.

Nine months later, in April, 2017, the OCR followed up with the practice to again request copies of policies and procedures pertaining to disclosures of PHI on social media, and asked for the removal of the review on the practice's Google page. In reply, the practice provided an "Acknowledgement of Training," but did not include any documents about the contents of the training, and still did not remove the review response from its Google page. No policies or procedures regarding disclosure of PHI of any sort were provided.

In September, 2017, the OCR requested financial statements and federal tax returns from the practice, which replied the following day by refusing to disclose such information because such documents "[did] not relate to HIPAA."[80] The OCR explained the relevance of

---

[79] The full text of the response is striking. Dr. Igbinadolor stated: "*It's so fascinating to see [Complainant's full name] make unsubstantiated accusations when he only came to my practice on two occasions since October 2013. He never came for his scheduled appointments as his treatment plans submitted to his insurance company were approved. He last came to my office on March 2014 as an emergency patient due to excruciating pain he was experiencing from the lower left quadrant. He was given a second referral for a root canal treatment to be performed by my endodontist colleague. Is that a bad experience? Only from someone hallucinating. When people want to express their ignorance, you don't have to do anything, just let them talk. He never came back for his scheduled appointment Does he deserve any rating as a patient? Not even one star. I never performed any procedure on this disgruntled patient other than oral examinations. From the foregoing, it's obvious that [Complainant's full name] level of intelligence is in question and he should continue with his manual work and not expose himself to ridicule. Making derogatory statements will not enhance your reputation in this era [Complainant's full name]. Get a life.*" Notice of Proposed Determination, paragraph II.6, p. 3, available at, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/upi/index.html.

[80] Notice of Proposed Determination, paragraph II.16, p. 4, available at, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/upi/index.html.

the documents (namely their use in determining the total fine to be imposed), but Dr. Igbinadolor refused to provide them, stating "I will see you in court."[81] The OCR served the practice with an administrative subpoena, directing it to produce its policies and procedures regarding the HIPAA Privacy Rule as well as other documentation, but the practice did not respond as of October 22, 2020, the date of the Notice of Proposed Determination. The practice also failed to reply to a Letter of Opportunity, by which the OCR gave the practice a chance to provide written evidence of mitigating factors or to support a waiver of the CMP that would be imposed.

The OCR determined that the violation was a case of willful neglect, which had not been corrected, and imposed a CMP. In describing the factors it considered, the OCR indicated that the violation involved only one patient, revealing the patient's name, medical history, and the nature of treatment received. The OCR stated "Despite repeated notice of this impermissible disclosure, [the practice] has not demonstrated any effort to mitigate any potential harmful effects of the impermissible disclosure or to come into compliance with the applicable provisions of the Privacy Rule by removing the PHI from its Google page." The OCR did note that there was no prior history of noncompliance by the practice. Finally, taking into account that Dr. Igbinadolor was a solo practitioner, the OCR determined that a $50,000 CMP was appropriate.

Compare the above case to two other similar cases involving disclosures of patient PHI online: one involving New Vision Dental, and the other relating to Elite Dental.[82] In both cases, the dental practices disclosed patient PHI in responses to reviews on Yelp. In both cases, following a single complaint, the OCR discovered that the practices had each disclosed multiple patients' PHI online, including names, treatment details, and in some cases insurance and cost information. In neither case did the practices have a valid authorization from the patients to do so. Both practices were found to have impermissibly disclosed PHI, and to have failed to include minimum required content in their respective Notices of Privacy Practices, and to have failed to implement policies and procedures regarding PHI (especially disclosures on social media). Both were required to enter into resolution agreements and corrective action plans which would, among other things, require the respective practices to: (1) develop policies and procedures to comply with the privacy and security of patient PHI (which must be submitted to the OCR 30 days before their effective date to allow the OCR to review and approve the policies); (2) to distribute the policies and procedures to workforce members, requiring them to sign a certification stating that they had read the policies and procedures, and to update such policies and procedures as necessary; (3) to investigate possible instances of failure to comply with the

[81] Notice of Proposed Determination, paragraph II.18, p. 5, available at, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/upi/index.html. Dr. Igbinadolor did not, in fact, take the OCR to court, likely because he forfeited his right to appeal the OCR's decision by failing to request a hearing in response to the Notice of Proposed Determination. See, Notice of Final Determination, available at, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/upi/index.html.

[82] The facts and resolution agreement for New Vision Dental can be found at, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/new-vision/index.html. The facts and resolution agreement for Elite Dental can be found at, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/elite/index.html.

policies and procedures, and to report violations where discovered; and, (4) to train workforce members on the practices' respective policies and procedures, and to require certification by workforce members of having received such training. With respect to settlement payments, the OCR required New Vision Dental to pay $23,000, while Elite Dental was required to pay $10,000.

From these instances, we can draw several conclusions based on the different outcomes for nearly identical baseline violations of HIPAA. In the case of Dr. Igbinadolor, it is clear that the refusal to cooperate with the OCR contributed to the imposition of a CMP, including a finding of willful neglect. This becomes evident when one considers that the OCR repeatedly notified Dr. Igbinadolor that his conduct had violated HIPAA and gave him ample opportunity to correct the matter, but he took no remedial steps. In addition, while the tone of the doctor's responses may be striking, it is likely more important that, although the doctor did not completely ignore the OCR's requests, his responses lacked any indication of substantive efforts to comply with HIPAA. It likely was this failure, rather than the tone of the responses, that ultimately led to the CMP.

One can compare this to the two other dental cases involving posting PHI as part of online review replies. While the record does not indicate what steps these practices took in response, it is clear that they at least did not ignore the OCR, and likely gave the OCR access to the information it requested; if this was not the case, the practices would likely have faced CMPs as well. Additionally, in the New Vision Dental corrective action plan, Section V.F.1 (Mitigation) requires the practice to remove all social media postings that include PHI. No similar language appears in the Elite Dental corrective action plan. Although the record does not state as much, the lack of a mitigation requirement may suggest that Elite Dental had <u>already</u> removed such postings by the time it entered into the resolution agreement with the OCR. This may also account for the lower dollar amount that Elite Dental was required to pay in settlement: only $10,000, as opposed to New Vision Dental's $23,000 payment. In other words, having taken corrective action prior to entering into the resolution agreement may have resulted in a less onerous payment and less burdensome remediation requirements.

The difference in outcomes for these practices strongly suggests what may seem like a common sense strategy to responding to the OCR's investigations. The first, and one would think most obvious, aspect of the strategy is to not ignore the OCR wholesale as Dr. Igbinadolor (mostly) did. An "ostrich defense" is both ineffective and counterproductive when facing an OCR inquiry. Instead, the covered entity or business associate should take the investigation (and any underlying complaint) seriously, recognizing the potential for stiff penalties if it fails to respond. When the OCR makes specific requests, the covered entity or business associate should take clear steps to follow the OCR's advice and comply with HIPAA as best it can. In the case of online reviews, this would include at a minimum removing the replies to the patients. Taking steps to bolster internal policies, procedures and practices to ensure future compliance with HIPAA is also an important step both in rectifying the problem and in demonstrating to the OCR that the practice is committed to HIPAA compliance. Certainly, offering non-responsive documentation (e.g., providing a Notice of Privacy Practices when asked to provide policies and procedures governing the

disclosure of PHI on social media) will not do. Other cases can also offer insights into effective (and ineffective) response strategies.

4.2 Two Access Cases – Yet More Contrasts

Since 2019, the OCR has vigorously investigated cases involving patients right to access records containing their PHI, as part of the OCR's Right of Access Initiative. From its launch until 2022, the OCR has reported 42 instances of either entering into resolution agreements or imposing CMPs on covered entities or business associates that failed to provide patients access in accordance with HIPAA requirements.[83] For a three-year period, this is a significant number of cases focused on a single issue. However, not every case proceeds the same. Although they were referenced earlier in this article, the cases of ACPM Podiatry and Danbury Psychiatric Consultants offer insight into best (and worst!) practices in responding to OCR investigations. Although both cases share a similar root cause (an individual requesting a copy of their records who was denied such records due to an outstanding payment), the response from each of these two entities are strikingly different.

In the case of ACPM Podiatry[84], a patient made several oral requests in 2018 for copies of their records to which the practice failed to respond, as well as a written request that same year. When the patient followed up on the written request one month later, the patient was informed that the practice was not trying to refuse the request, but "had a lot of surgeries to complete before year end." One month after the initial follow-up inquiry, the patient again inquired as to the status of their records request, and was told that because the patient's insurance had not paid, the practice would not release the records. Several months later, in mid April, 2019, the patient filed a complaint with the OCR, after which the OCR contacted the practice in letter containing technical assistance, informing ACPM Podiatry of an individual's right to access, and that a covered entity was not permitted to withhold records or deny a patient access merely because a bill had not been paid. The OCR then closed the investigation.

Six days after the OCR informed the patient and the practice that the investigation had been closed, the patient followed up on their request again, this time being told "We still have your request, and we have your number." In May, 2019, still having not received their records, the patient submitted a second complaint to the OCR. The complaint indicated that the patient needed copies of the records to appeal an unfavorable decision by their insurance company relating to payment of the bill for ACPM Podiatry's services, and that the patient had a July 2 deadline to submit the records in support of their request.

The OCR sent a further letter to ACPM Podiatry, requesting data and giving the practice until June 29 to respond. ACPM Podiatry, however, did not provide any response to the letter within the requested timeframe. The OCR also called ACPM Podiatry on the phone twice, on July 2, 2019 and July 9, 2019 – after the patient's deadline with their insurer – and was told on the second occasion that the physician who owned the practice

---

[83] Specifically, 45 CFR § 164.524.

[84] The facts of the case can be found in the Notice of Proposed Determination, available at https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/acpm-npd/index.html.

was aware of the inquiry, but no further substantive response was provided. The patient finally received their records on July 28, 2020, 618 days after their initial request. On November 9, 2020, the OCR sent a further letter to the practice, offering it a chance to submit written evidence of mitigating factors or affirmative defenses in support of a waiver of the OCR imposing a CMP. Incredibly, the practice provided no reply whatsoever. As a result, the OCR imposed a CMP of $100,000.

Standing in stark contrast to ACPM Podiatry's disregard of both its duty to provide records to the patient and the OCR's enforcement authority, consider the facts in the case of Danbury Psychiatric Consultants. Again, the case involves a patient with a prior balance requesting copies of their records and being denied by the practice, leading to the patient submitting a complaint to the OCR. As with the ACPM Podiatry case, the OCR contacted Danbury Psychiatric several months later to begin its investigation, after which Danbury Psychiatric provided the patient with full access to their records.[85] Following this, the OCR and Danbury Psychiatric entered into a Resolution Agreement and Corrective Action Plan[86]. The Corrective Action Plan required Danbury Psychiatric to develop and update policies and procedures regarding patient records access requests, to implement these policies, and to revise and update them when necessary. Copies of the policies and procedures would also have to be sent to the OCR for review prior to their implementation. The practice also was required to develop and implement training procedures for employees regarding patient records access requests, and such procedures also were required to be sent to the OCR for review before implementation. Finally, Danbury Psychiatric had to pay the OCR $3,500.

Both cases involve a single patient making requests for records, but with very different responses to the OCR's investigation. ACPM Podiatry is a case study in worst practices.[87] In the Notice of Proposed Determination, the OCR noted that the case was one

[85] It is unclear from the record whether the OCR provide Danbury with technical assistance in its initial letter.

[86] Available at, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/danbury-ra-cap/index.html.

[87] Surprisingly, ACPM is not the only incident involving a covered entity that denied patients access to their records, and then completely ignored the OCR's attempts to investigate the matter and return to compliance. In a 2020 Notice of Proposed Determination, Dr. Robert Glaser also had a patient submit multiple written and oral requests for records, which the doctor ignored. The OCR again sent multiple letters, all of which were ignored. In Glaser's case, the violation spanned multiple years, and the doctor failed to respond to the OCR's requests for data or follow-up requests for information necessary to complete its investigation. However, there was no prior history of noncompliance, and the OCR did take into account Glaser's status as a solo practitioner in analyzing his financial condition. Nevertheless, Glaser failed to provide the OCR with information about his financial condition, and failed to provide written evidence of mitigating factors or otherwise respond to the OCR's Letter of Opportunity (whereby he could have offered such information and petitioned for a waiver of the CMP), so the OCR ultimately determined that a $100,000 CMP was appropriate. See, "Dr. Robert Glaser Notice of Proposed Determination and Notice of Final Determination," available at https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/glaser/index.html. Another incident from 2011 also involved a covered entity refusing to provide multiple patients access to their records, and ignoring the OCR's attempts to contact it and investigate the matter, ultimately leading the OCR to submit a subpoena *duces tecum*, and petition a United States District Court to enforce the subpoena. In that case, the covered entity did not attend the hearing, and complied with the court's order by providing not only the affected individuals' records, but 59 boxes containing medical records of approximately 4,500 other

of uncorrected, willful neglect, and listed the factors it considered in determining the amount of the CMP.[88] Although the violation only affected one individual, it persisted for 618 days after the complainant requested access. The complainant also suffered financial harm, because ACPM's delay denied the complainant the opportunity to timely file their appeal with their insurance company. ACPM's history of prior compliance issues also was a significant factor. In addition to the complainant's own efforts in submitting multiple requests for access and multiple complaints to the OCR, the OCR noted that it had received a separate complaint two years prior, and had previously provided technical assistance on the same issue of access to records. This prior technical assistance was in addition to the technical assistance offered in 2019 to ACPM, neither of which apparently made any impact on ACPM. These factors, along with the OCR's analysis of what financial information it could gather on its own (since ACPM provided no information regarding its financial condition to the OCR), led the OCR to determine that a $100,000 CMP was appropriate under the circumstances.

By contrast, Danbury Psychiatric appears to have worked to correct its errors upon receiving notice that the OCR was investigating. Subsequent investigation may have determined that these efforts were insufficient and the practice could make the same mistake in the future unless remedial efforts were taken. However, based on the information available, it appears that the practice lived up to its requirements under the Resolution Agreement and Corrective Action Plan into which it entered with the OCR.

As with the cases above involving improper disclosures, these two cases relating to denials of records access further suggest how to (and how not to) respond to an OCR investigation. One would think most obvious, aspect of the strategy is to not ignore the OCR wholesale as ACPM Podiatry did. As ineffective and unresponsive as Dr. Igbinadolor's responses to the OCR were, they were at least responses. In ACPM's case, the record does not indicate that any response was ever provided at all. This approach allows the OCR to draw the worst inferences and impose a CMP. Further, failing to respond at all to the Letter of Opportunity and to request a hearing effectively gives up any appeal rights the covered entity or business associate might have (although, given the facts, there likely would have been little to appeal in the first place).

In Danbury Psychiatric's case, though, we can find evidence of effective responses. Danbury Psychiatric took steps to rectify its situation, first by providing the patient with access to their records once the OCR intervened. Second, Danbury Psychiatric worked to improve its policies and procedures. These steps likely helped it to avoid a CMP, although based on the information available, these steps were not enough to satisfy the OCR without requiring Danbury Psychiatric to pay a settlement amount and enter into a resolution

---

individuals for whom the OCR had made no requests or demands, and where the covered entity had no authority to disclose the PHI. This case resulted in a CMP of $4,351,600. See, "Cignet Health Fined a $4.3M Civil Money Penalty for HIPAA Privacy Rule Violations," available at https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/cignet-health/index.html.

[88] These factors are listed in Section V of the Notice of Proposed Determination.

agreement and corrective action plan. However, as the next case study will demonstrate, avoidance of all penalties is possible if the entity acts diligently.

4.3 Insight From Personal Experience – Navigating a Hacking Breach

There is often no greater teacher than firsthand experience. In 2016, one of our clients contacted us about a HIPAA breach incident involving hacking of the client's servers from overseas. The hack occurred between June 19 and 27, 2016, and was discovered on June 28, 2016. During the hack, the client's records became inaccessible because they were encrypted by the hackers. The client took corrective steps with its EMR provider, and investigated the incident internally, then contacted the OCR on August 9, 2016.

The client's situation at the start of this process was not ideal. Prior to the incident, while the client had in place some physical, administrative, and technical safeguards, many of these matters had been entrusted to a single IT support individual who was not well versed in the requirements of HIPAA. The client's server itself was not as physically secure as it could have been. It was kept in a secure room, but the door was often not locked. Cables running between the server and router had been moved to bypass the client's firewall, apparently in an effort to fix a specific network connectivity issue. In addition, anti-virus and anti-malware programs were not functioning properly and were out of date. Although the client's IT provider had stated that he would perform daily scans of the system, these scans had not been conducted for some time. More problematic was the fact that the client's Security Risk Assessment was years out of date, and what little did exist was sparse and inadequate. Rather than create policies and procedures specifically tailored to the practice, the client had relied upon a published book pertaining to HIPAA compliance issues to train its staff and to serve as its policies.

Once the hacking incident was discovered, the client took several remedial steps. First, the client conducted an internal investigation to determine what had happened. This included hiring an outside company to conduct an audit of the client, as well as instructing the EMR vendor to investigate the incident and restore access to the records. The client also fired the IT support individual, later demanding a return of all payments made to the individual during 2016, and hired a new company with HIPAA compliance experience to provide ongoing IT services. The client also hired a company to conduct a new, much more thorough Security Risk Assessment, from which it developed new policies and procedures, which were updated periodically thereafter. With respect to physical security, the client added door locks to its server room (and locked them appropriately), and also had security cameras installed on the exterior of its building. The client further improved its backup procedures, enabled screen lockouts on its computers, updated its computer software, and established a guest wifi system to allow for the use of personal devices within the office without compromising the security of the client's main network. All of these efforts were documented in exquisite detail, with contemporaneous emails and other records of communications, receipts for services and goods purchased, and other documentary evidence.

In response to the OCR's inquiry, the client and I spent over a month gathering evidence to demonstrate good faith attempts to comply with HIPAA, and to take proactive steps to remedy HIPAA deficiencies after discovery of the hack. The client and I created an

extensive narrative, coupled with documentary evidence, describing what errors had been made and how they had been corrected, what matters the client had control over as well as what had been beyond its knowledge or control at the time, and what steps the client had taken to rectify the problems that had arisen. As mentioned above, the client assembled contemporaneous communications between itself and its IT provider, its EMR provider, and the new companies the client had hired to perform audits, and perform its Security Risk Assessment and help it develop new policies and procedures more tailored to the practice's specific needs. These documents, along with the policies and procedures that had been in place at the time (including a physical copy of the policy book the client had used), and its newly developed policies and procedures were offered as exhibits to the narrative.

We provided physical copies of all of this documentation which was enough to fill a file box to capacity, and also provided electronic copies of all evidence that we could scan in on a thumb drive for ease of reference by the OCR's investigators. I personally hand delivered these materials to the OCR's office (during a snowstorm) before the OCR's deadline in March, 2017. The process involved dozens of phone calls and email communications between myself and the client, to coordinate the gathering and organizing of the evidence, and to gradually develop and edit the narrative. Following delivery, I contacted the OCR on several occasions to inquire as to the status of the case, but received no substantive responses other than that the investigation was ongoing. During this time, the client remained nervous, concerned about the possibility of CMPs being imposed, or being forced to enter into a resolution agreement and corrective action plan, what that could entail, and whether it would include monetary penalties (to say nothing of the potential expense of any further remedial efforts).

In December, 2018, the OCR finally closed the case. There were neither penalties applied nor any resolution agreement entered into. The OCR determined that the client had demonstrated "voluntary compliance." The OCR further provided technical assistance in the form of a Security Guide for small medical practices, but otherwise considered the matter resolved.

This was as good an outcome as we could have hoped for: no penalties, and no further remedial action were required. Nevertheless, the process was costly, including attorneys fees and the amounts paid to outside contractors to provide new IT services, conduct audits, perform Security Risk Assessments, and develop policies and procedures for the client. Beyond the monetary costs, the client surely felt the burden of the investigative process and the emotional toll of simply worrying what the ultimate outcome would be.

However, from this experience, one can draw certain conclusions. First, the client was able to demonstrate voluntary compliance not least because it actually took significant proactive steps to remedy its HIPAA problems. The client undertook internal audits, hired additional contractors, and developed useful and substantive HIPAA policies and procedures specifically designed around its needs, instead of using an "off the shelf" solution like a pre-made compliance plan. As noted, the client also maintained meticulous documentation of all of its efforts in becoming compliant. The client also wrote a detailed, precise, compelling narrative that both acknowledged its own failures, and clearly

described the efforts it had taken to remediate them. Finally, all of this information was provided to the OCR within the deadlines set, with no need for further requests or a request for a deadline extension.[89]

Put simply, the client, with our assistance, very clearly demonstrated that it took its obligations under HIPAA seriously, and was committed to taking the actions necessary to comply with HIPAA going forward. The substantive steps to return to compliance were also sufficient to satisfy the OCR. Had the client taken insufficient steps, it is likely that the OCR would have at least required the client to enter into a resolution agreement and corrective action plan to remedy any remaining deficiencies, and it is possible that the client would have been required to pay some monetary settlement. Moreover, because the client responded as it did, it was able to avoid the imposition of a CMP.

5. Conclusion

The best defense against HIPAA violations is to not make them in the first place. Yet, perfect compliance with HIPAA is likely more of a Platonic ideal than a practical reality. Whether through human error or technological foul-up, things go wrong and sometimes those things run afoul of HIPAA. When this happens, and especially when covered entities and business associates find themselves the subject of an OCR investigation, the best approach is to work diligently to rectify the problem, and to respond substantively to the OCR in a way that demonstrates a commitment to HIPAA compliance. Towards this end, being able to provide effective documentation that shows the risk assessments, policies and procedures, training methods, and other steps to ensure compliance taken by the covered entity or business associate will be critical. Moreover, when a covered entity has these documents in place, and especially when it undertakes regular efforts to review and update its compliance documentation, conduct internal audits, and engage in re-training its workforce, it is likely already in a position to respond effectively to OCR inquiries and to avoid facing a resolution agreement and settlement, or worse, a CMP. With a better understanding of the OCR's goals, the methods it may deploy in investigations, the possible penalties, as well as effective response strategies, experienced health care counsel can help shepherd a covered entity in its responses to the OCR in a manner that avoids penalties and remediation.

[89] While it is possible that the OCR might have given such a deadline extension if a substantive response from our office had requested one, given the length of time required to resolve the matter. However, if such a request had been granted, it likely would have extended the time it would have taken to resolve the matter and finish the investigation.