Annual Report to Congress on HIPAA Privacy, Security, and Breach Notification Rule Compliance

For Calendar Year 2022

As Required by the Health Information Technology for Economic and Clinical Health (HITECH) Act, Public Law 111-5, Section 13424

Submitted to the
Senate Committee on Health, Education, Labor, and Pensions,
House Committee on Ways and Means, and
House Committee on Energy and Commerce

U.S. Department of Health and Human Services
Office for Civil Rights

Executive Summary Overview

This report summarizes key Health Insurance Portability and Accountability Act of 1996 (HIPAA) enforcement activities undertaken by the United States Department of Health and Human Services (HHS), Office for Civil Rights (OCR) during the 2022 calendar year. The Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as title XIII of division A and title IV of division B of the American Recovery and Reinvestment Act of 2009 (Pub. L. 111-5), requires OCR to produce an Annual Report to Congress on HIPAA Privacy, Security, and Breach Notification Rule Compliance that identifies the number of complaints received, the method by which those complaints were resolved, the number of compliance reviews initiated by OCR, the outcome of each review, the number of audits performed, a summary of audit findings, the number of subpoenas or inquiries issued, and OCR's anticipated compliance and enforcement initiatives for the following year. OCR did not perform any audits in 2022 due to a lack of financial resources.

There have been significant increases in HIPAA complaints received (17% increase from 2018 to 2022) and large breaches reported (107% increase from 2018 to 2022), without any increases in appropriations during that same time period. Further, in April 2019, as a part of HHS's review of existing regulations, HHS issued a Notification of Enforcement Discretion Regarding HIPAA Civil Money Penalties that significantly reduced the maximum annual cap for three of the four penalty tiers. OCR requested that the HITECH civil monetary penalty caps be increased in the HHS FY 2023 Discretionary A-19 Legislative Supplement that was sent to Congress in September 2021. Additionally, the implementation of the 2021 HITECH Amendment[1] requires OCR to consider whether a HIPAA regulated entity has "adequately demonstrated that it had, for not less than the previous twelve months, recognized security practices in place" that may mitigate a civil money penalty or "remedies that would otherwise be agreed to in any agreement with respect to resolving potential violations of the HIPAA Security rule." These efforts have significantly increased OCR's workload and the length of time to complete HIPAA Security Rule investigations. These factors have combined to cause a severe strain on OCR's limited staff and resources. This lack of necessary funding limits OCR's HIPAA enforcement activities during a time of substantial growth in cybersecurity attacks to the health care sector.

Summary

OCR received 30,435 new complaints alleging violations of the HIPAA Rules and the HITECH Act, and resolved 32,250 complaints, as explained in detail in this Report. Of those, OCR resolved 28,107 (87%) before initiating an investigation. OCR resolved 2,882 (9%) complaints by providing technical assistance in lieu of an investigation (pre-investigational technical assistance). In 560 (2%) of the investigations, a covered entity or business associate took corrective action, and in 15 (1%) of these complaints, OCR provided technical assistance after initiating an investigation (post-investigated technical assistance). OCR resolved 17 complaint investigations with Resolution Agreements and Corrective Action Plans (RA/CAPs) and monetary settlements totaling $802,500, and one complaint investigation with a civil money penalty in the amount of $100,000.

[1] See Section 1 of Pub. L. 116-321, 134 Stat. 5072 (January 5, 2021).

OCR completed 846 compliance reviews and required subject entities to take corrective action or pay a civil money penalty in 80% (674) of these investigations. Three compliance reviews were resolved with RA/CAPs and monetary payments totaling $2,425,640. In the remaining 172 (20%) completed compliance reviews, OCR provided the covered entity or business associate with post-investigation technical assistance (4%), found insufficient evidence of a violation of the HIPAA Rules (11%), or lacked jurisdiction to investigate the allegations (5%). OCR issued no subpoenas, and no audits were initiated.

OCR engaged in 124 outreach activities to increase education to the public about their HIPAA rights, and to regulated entities about trends in large HIPAA breaches reported to OCR, the requirements of the HIPAA Rules, and significant OCR HIPAA investigations resolved with corrective action plans and a resolution agreement or civil money penalty.

OCR's HIPAA web content is updated regularly, providing information and guidance in both English and Spanish. Visits to OCR's HIPAA webpages averaged 340,000 unique visits per month, and approximately 4 million visits overall. In October of 2022, OCR produced a video for organizations covered under the HIPAA Rules on the 2021 HITECH Amendment regarding recognized security practices[2] that is intended to educate the health care industry on the categories of recognized security practices and how entities regulated under the HIPAA Rules may demonstrate implementation. The video covers the HITECH Amendment generally, how regulated entities can demonstrate that recognized security practices are in place, the evidence of recognized security practices that may be requested by OCR in an investigation or audit, where to find more information about recognized security practices, and provides answers to a selection of questions submitted to OCR on recognized security practices. This video has been viewed over 10,000 times since its publication.

Background

HIPAA was enacted on August 21, 1996. Subtitle F of HIPAA, known as the Administrative Simplification provisions, permitted the Secretary to establish standards for the privacy and security of individually identifiable health information held by an entity subject to HIPAA, defined in the HIPAA Rules as a "covered entity." A covered entity is a health plan, a health care provider that electronically transmits any health information in connection with certain financial and administrative transactions (such as electronically billing health insurance carriers for services), or a health care clearinghouse. The HITECH Act, which strengthened HIPAA's privacy and security protections, also expanded the applicability of certain provisions of the HIPAA Rules to business associates of covered entities.[3] A "business associate" is a person or entity, other than a member of the workforce of a covered entity, that performs certain functions for or activities on behalf of, or provides certain services to, a covered entity that involve creating, receiving,

[2] "The term 'recognized security practices' means the standards, guidelines, best practices, methodologies, procedures, and processes developed under section 2(c)(15) of the National Institute of Standards and Technology Act, the approaches promulgated under section 405(d) of the Cybersecurity Act of 2015, and other programs and processes that address cybersecurity and that are developed, recognized, or promulgated through regulations under other statutory authorities." (Act of Jan. 5, 2021, Pub. L. 116-321, www.congress.gov/116/plaws/publ321/PLAW-116publ321.pdf.)

[3] On January 25, 2013, HHS published a final rule that implemented changes required by the HITECH Act and by the Genetic Information Nondiscrimination Act of 2008. Among other things, the final rule extends liability for violations of the HIPAA Security Rule and certain provisions of the HIPAA Privacy Rule to businessassociates of HIPAA covered entities, effective September 23, 2013.

maintaining, or transmitting protected health information (PHI).[4] Any subcontractor ofa business associate that creates, receives, maintains, or transmits PHI on behalf of that business associate is also a business associate.

The HIPAA Privacy Rule, found at 45 CFR Part 160 and Subparts A and E of Part 164, provides important federal protections to protect the privacy of PHI and gives individuals rights with respect to that information. Covered entities and their business associates may not use or disclose PHI, except either as the Privacy Rule permits or requires.

The HIPAA Security Rule, found at 45 CFR Part 160 and Subparts A and C of Part 164, establishes national standards to protect electronic PHI (ePHI) created, received, maintained, or transmitted by covered entities and their business associates. The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and availability of ePHI.

The HIPAA Breach Notification Rule, found at 45 CFR Part 160 and Subparts A and D of Part 164, requires HIPAA covered entities to notify affected individuals, HHS, and, in some cases, the media, following the discovery of a breach of unsecured PHI. Business associates are also required to notify covered entities following the discovery of a breach.

Section 13424(a) of the HITECH Act requires the Secretary of Health and Human Services (the Secretary) to prepare and submit an annual report to the Senate Committeeon Health, Education, Labor, and Pensions, the House Committee on Ways and Means, and the House Committee on Energy and Commerce (the Committees), regarding "complaints of alleged violations of law, including the provisions [of the HITECH Act] as well as the provisions of [thePrivacy and Security Rules promulgated under HIPAA] relating to privacy and security of health information that are received by the Secretary during the year for which the report is being prepared."

Section 13424(a)(1) of the HITECH Act requires that the report include:

- the number of complaints received by the U.S. Department of Health and Human Services (HHS);
- the number of such complaints resolved informally, a summary of the types of such complaints so resolved, and the number of covered entities that received technical assistance from the Secretary during such year in order to achieve compliance with such provisions and the types of such technical assistance provided;
- the number of such complaints that have resulted in the imposition of civil money penalties (CMPs) or that have been resolved through monetary settlements, including the nature of the complaints involved and the amount paid in each penalty or settlement;

[4] Protected Health Information means individually identifiable health information: (1) Except as provided in paragraph (2) of this definition, that is: (i) Transmitted by electronic media; (ii) Maintained in electronic media; or (iii) Transmitted or maintained in any other form or medium. (2) Protected health information excludes individually identifiable health information: (i) In education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g; (ii) In records described at 20 U.S.C. 1232g(a)(4)(B)(iv); (iii) In employment records held by a covered entity in its role as employer; and (iv) Regarding a person who has been deceased for more than 50 years. See 45 C.F.R. §160.103.

- the number of compliance reviews HHS conducted and the outcome of each review;
- the number of subpoenas or inquiries issued;
- the Secretary's plan for improving compliance with and enforcement of the HIPAA Rules for the following year; and
- the number of audits performed and a summary of audit findings pursuant to section 13411 of the HITECH Act.

For most HIPAA covered entities, compliance with the Privacy Rule was required by April 14, 2003, compliance with the Security Rule was required by April 20, 2005, and compliance with the Breach Notification Rule was required for breaches that occurred on or afterSeptember 23, 2009.[5] This report includes information about HHS's enforcement process with regard to the Privacy, Security, and Breach Notification Rules (the HIPAA Rules), and information about HHS's actions to enforce the HIPAA Rules during the calendar year of 2022.

This report is prepared for the calendar year 2022. The Reports to Congress on Compliance with the HIPAA Privacy and Security Rules for previous years are available at www.hhs.gov/hipaa/for-professionals/compliance-enforcement/reports-congress/index.html.

Enforcement Process

OCR enforces the HIPAA Rules by investigating written complaints filed with OCR, either submitted on paper, by e-mail, or through its complaint portal. OCR also conducts compliance reviews to determine if covered entities or business associates are in compliance with the HIPAA Rules. In addition, OCR's compliance activities include conducting audits[6] and providing education and outreach to support compliance with the HIPAA Rules, which are discussed later in this report. When necessary, OCR has authority to issue subpoenas to compel cooperation with an investigation.

Complaints

Under the law, OCR may act only on complaints that meet the following conditions[7]:

- The alleged violation must have occurred after compliance with the HIPAA Rules was required.
- The complaint must be filed against an entity that is required by law to comply with the HIPAA Rules (i.e., either a covered entity or a business associate).

[5] A separate Report to Congress, available at www.hhs.gov/hipaa/for-professionals/breach-notification/reports-congress/index.html, describes the types and numbers of breaches reported to the Secretary and the actions that have been taken by covered entities and business associates in response to the reported breaches.
[6] Section 13411 of the HITECH Act, which became effective on February 17, 2010, requires HHS to undertake periodic audits to ensure that covered entities and business associates comply with the HIPAA Rules.
[7] *See also* 45 C.F.R. §160.306(c) (1) and (2) which provide that a complaint will be investigated when a preliminary review of the facts indicates a possible violation due to willful neglect, and any other complaint may be investigated.

- The complaint must describe an activity that, if determined to have occurred, would violate the HIPAA Rules.

- The complaint must be filed within 180 days of when the individual submitting the complaint knew or should have known about the act or omission that is the subject of the complaint. OCR may waive this time limit if it determines that the individual submitting the complaint shows good cause for not submitting the complaint within the 180-day time frame (e.g., circumstances that made submitting the complaint within 180 days impossible).

OCR must determine whether a complaint presents an eligible case for enforcement of the HIPAA Rules, as described above. If OCR determines that it lacks jurisdiction because the complaint alleges a violation by an entity not covered by the HIPAA Rules, describes an activitythat would not violate the HIPAA Rules, or is untimely, OCR closes the case. Where the case iseligible for enforcement, OCR may provide technical assistance to the covered entity or business associate to resolve the case quickly without further investigation.

Compliance Reviews

The HIPAA regulations provide that the Secretary may initiate a compliance review into the practices of an entity subject to HIPAA in circumstances other than in response to a complaint.[8] OCR may open compliance review investigations of covered entities and business associates based on an event or incident brought to OCR's attention, such as through the media, referrals from other agencies, or based upon patterns identified through multiple complaints alleging the same or similar violations against the same entity.

If individual complaints are received during the course of an open investigation that assert the same allegations/potential violations being investigated in the open transaction, OCR will consolidate the complaint(s) into the open investigation (*e.g.* a compliance review or an investigation of a reported breach).[9] Multiple complaints alleging the same or similar violations demonstrate systemic compliance deficiencies that are better investigated under one transaction rather than on an individual complaint basis for purposes of achieving compliance.

OCR may also initiate a compliance review investigation if information gathered from an ongoing investigation requires such action. For example, while investigating a breach reported by a covered entity, OCR may learn that the breach was caused by the covered entity's business associate and may therefore open a compliance review of the business associate.

[8] "The Department generally conducts compliance reviews to investigate allegations of violations of the HIPAA Rules brought to the Department's attention through a mechanism other than a complaint." (2013 Omnibus Rule, Page 5579) *See also* 45 C.F.R. §160.308(a) and (b) which provide that compliance reviews will be conducted when a preliminary review of the facts indicates a possible violation due to willful neglect, and compliance reviews may be conducted to determine compliance in any other circumstances.

[9] When a complaint is consolidated into an open investigation, it is not counted as closed since it would mean double counting (*i.e.* counting it closed and consolidated). The consolidated complaint is deleted and not counted as closed so as not to double count complaint cases.

Investigations

Once OCR initiates an investigation, OCR collects evidence through interviews, witness statements, requests for data from the entity involved, site visits, or other available, relevant documents. Covered entities and business associates are required by law to cooperate with complaint investigations and compliance reviews. If a complaint or other event implicates the criminal provision of HIPAA (42 U.S.C. § 1320d-6), OCR may refer the complaint to the Department of Justice (DOJ) for investigation. If DOJ opens a case referred by OCR for criminal investigation, OCR may still investigate for potential civil violations of the HIPAA Rules and will coordinate with DOJ during its investigation of the case.

In some cases, OCR may determine, based on the evidence, that there is insufficient evidence to support a finding that a covered entity or business associate violated the HIPAA Rules. In such cases, OCR sends a closure letter to the parties involved explaining the results of the investigation.

In other cases, OCR may determine, based on the evidence, that the covered entity or business associate was not in compliance with the HIPAA Rules. In such cases, OCR will generally first attempt to resolve the case by obtaining voluntary compliance through corrective action, which may include a resolution agreement.

Where corrective action is sought, OCR obtains satisfactory documentation and other evidence from the covered entity or business associate that it undertook the required corrective action to resolve the potential HIPAA violation(s). In the vast majority of cases, a covered entity or business associate will, through voluntary cooperation and corrective action, be able to demonstrate satisfactory compliance with the HIPAA Rules.

Resolution Agreements

Where OCR finds indications of noncompliance due to willful neglect, or where the nature and scope of the noncompliance warrants additional enforcement action, OCR pursues a resolution agreement with a payment of a settlement amount and an obligation to complete a corrective action plan (CAP). In these cases, OCR notifies the covered entity or business associate that, while OCR is prepared to assess a CMP with regard to the potential violations of the HIPAA Rules, OCR is willing to negotiate the terms of a resolution agreement and CAP to informally resolve the indications of noncompliance. These settlement agreements involve the payment of amonetary amount that is a reduced percentage of the potential CMP for which the covered entity or business associate could be liable. Additionally, in most cases, the resolution agreement includes a CAP that requires the covered entity or business associate to fix remaining complianceissues and to undergo OCR monitoring of its compliance with the HIPAA Rules for a specified time. While this type of resolution still constitutes informal enforcement action on the part of OCR, resolution agreements and CAPs are powerful enforcement tools for OCR as they address noncompliance and deter future noncompliance with the HIPAA Rules for entities under investigation, and when OCR announces those resolutions, the announcements serve as reminders to the wider regulated community of their own HIPAA obligations.

Civil Money Penalties

If OCR and a covered entity or business associate are unable to reach a satisfactory agreement to resolve the matter informally, or if a covered entity or business associate breaches the terms of a resolution agreement, OCR may pursue formal enforcement. In such cases, OCR notifies the covered entity or business associate of a proposed determination of a violation of the HIPAA Rules and OCR's intent to impose a CMP. If a CMP is proposed, the covered entity or business associate may request a hearing in which the Departmental Appeals Board decides if the CMP is supported by the evidence in the case. If the covered entity or business associate does not request a hearing within 90 days of receipt of OCR's proposed determination, OCR will issuea final determination and impose a CMP.

Audits

Section 13411 of the HITECH Act requires HHS to perform periodic audits of covered entity and business associate to assess compliance with the HIPAA Rules.

These audits are reviews of covered entities and business associates that are initiated not becauseof any particular event or incident indicating possible noncompliance on the part of the covered entity or business associate, but rather based on the application of a set of objective selection criteria.The objective of the audits is to 1) assess an entity's effort to comply with the HIPAA Rules, 2) ensure that covered entities and business associates are adequately safeguarding PHI, and 3) ensure that individuals are provided the rights afforded to them by the HIPAA Rules.

OCR did not initiate any audits in 2022 and is currently developing the criteria for implementing future audits should financial resources become available.

Summary of Complaints and Compliance Reviews

As discussed in greater detail below, in addition to requiring covered entities and business associates to take corrective action in hundreds of cases in 2022, OCR resolved 21 investigations with resolution agreements/CAPs or the imposition of CMPs totaling $3.3 million.

As shown in the table below, the number of complaints and breaches reported to OCR continues to increase. Between 2018 and 2022, the number of complaints received by OCR increased 17%, compliance reviews initiated by OCR increased by 51%, breaches affecting fewer than 500 individuals increased 1%, and breaches affecting 500 or more individuals rose 107%.

Year	Complaints Received	Compliance Reviews Initiated	Under 500 Breaches Reported	500+ Breaches Reported	% Change in complaints received	% Change in Compliance Reviews Initiated	% Change in Under 500 Breaches Reported	% Change in 500+ Breaches Reported
2022	30,435	676	63,966	626	-11% decrease	<1% increase	1% increase	3% increase
2021	34,077	674	63,571	609	25% increase	-10% decrease	-4% decrease	-7% decrease
2020	27,182	746	66,509	656	-4% decrease	22% increase	6% increase	61% increase
2019	28,261	611	62,771	408	9% increase	37% increase	-.5% decrease	35% increase
2018	25,912	447	63,098	302	-	-	-	-
2018 to 2022	-	-	-	-	17% increase	51% increase	1% increase	107% increase

Source: Current and previous Reports to Congress

Enforcement Data

Complaint Resolutions

2022 Complaints

During calendar year 2022, OCR received 30,435 new HIPAA complaints and carried over 11,465 open complaints from 2021. OCR resolved 32,250 complaints during calendar year 2022.[10] Of those, OCR resolved 28,107 (87%) before initiating an investigation. Examples of pre-investigation closures include complaints that alleged violations by an entity not covered by the HIPAA Rules and allegations involving conduct that did not violate the HIPAA Rules or that were untimely. OCR resolved 2,882 complaints (9%) by providing technical assistance in lieu of an investigation. *See Figure 1.*

[10] The number of new complaints received, and complaints resolved in a calendar year are not the same as OCR has complaint investigations that carry over from the previous year and are not counted as new complaints received when they are closed in a subsequent calendar year.

OCR completed 1,261 complaint investigations.[11] In 560 of these investigations, OCR required the covered entity or business associate to take corrective action (44% of the complaints investigated). In 686 of the investigated complaints (54% of the complaints investigated), OCR found insufficient evidence that a violation of the HIPAA Rules had occurred. In 15 of these investigations, OCR provided technical assistance after initiating an investigation (1% of the complaints investigated). *See Figure 2.*

[11] The number of complaints resolved in a given calendar year is the sum of administrative closures, technical assistance closures, and investigated closures.

Compliance Reviews

2022 Compliance Reviews

During calendar year 2022, OCR initiated 676 compliance reviews to investigate allegations of violations of the HIPAA Rules that did not arise from complaints.[14] Of these, 626 compliance reviews were initiated as a result of a breach report affecting 500 or more individuals and 2 were a result of a breach report affecting fewer than 500 individuals. The remaining 48 compliance reviews were opened based on incidents brought to OCR's attention through multiple complaints regarding an entity or practice, media reports, or other means.

OCR closed 846 compliance reviews in 2022, the vast majority of these cases were resolved following an investigation with the regulated entity taking corrective actions due to OCR involvement during the course of the investigation to come into compliance, agreeing to a settlement with a corrective action plan, or the imposition of a CMP.[15] Of the closed cases, 799 originated from breach reports and 47 originated from other means. The covered entity or business associate took corrective action or paid a CMP in 674 cases (80%). OCR provided the covered entity or business associate with technical assistance after investigation in 38 cases (4%). OCR found that there was insufficient evidence of a violation of the HIPAA Rules in 93 cases (11%), and OCR determined that it did not have jurisdiction to investigate the allegations in 41 cases (5%). Of the completed compliance reviews, three cases were resolved with resolution agreements, CAPs and monetary settlements totaling $2,425,640.[16] *See Figure 3*.

[14] Compliance reviews are opened for all reports of breaches affecting 500 or more individuals, and for some reports of breaches affecting fewer than 500 individuals.

[15] The new compliance reviews initiated, and compliance reviews resolved in a calendar year are not the same as OCR has compliance review investigations that carry over from the previous year and are not counted as new compliance reviews initiated when they are closed in a subsequent calendar year.

[16] The three cases that were resolved with RA/CAPs and monetary settlements are Oklahoma State University –Center for Health Sciences, New England Dermatology dba New England Dermatology and Laser Center, and Banner Health.

HHS OFFICE FOR CIVIL RIGHTS

COMPLIANCE REVIEWS

NUMBER OF CASES CLOSED AND TYPES OF CLOSURES

JANUARY 1, 2022 – DECEMBER 31, 2022

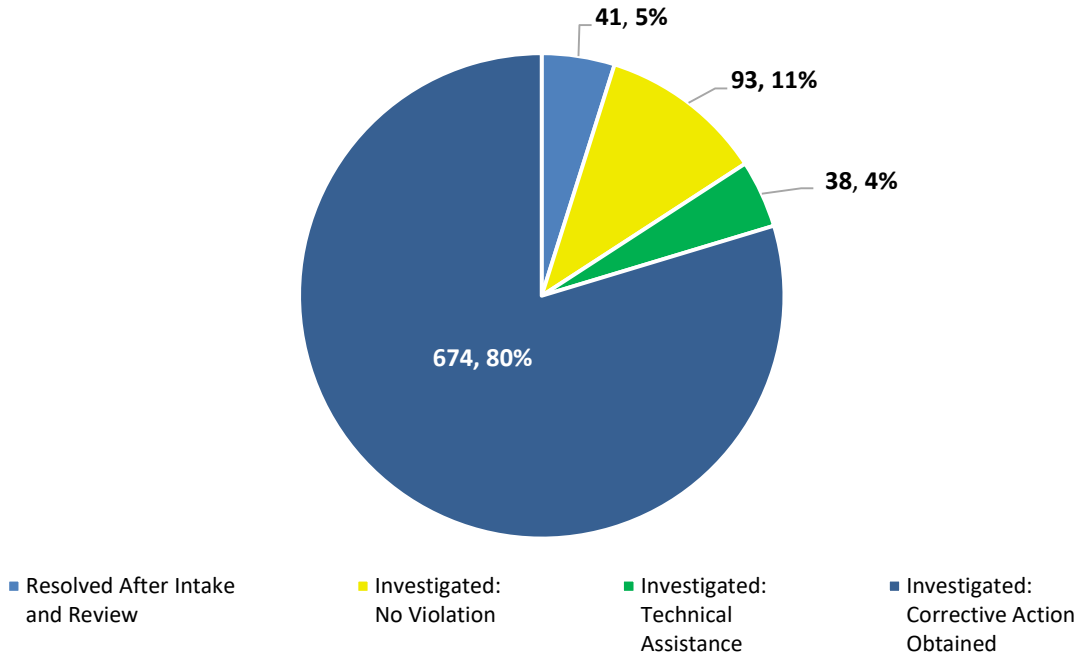

Figure 3

Subpoenas

OCR did not issue any subpoenas in 2022.

Secretary's Plan for Improving Compliance – Ongoing Outreach Efforts to Increase Awareness and Compliance

OCR continued to build its public outreach and education efforts to increase education to both HIPAA regulated entities and individual consumers, and to address compliance deficiencies in the regulated community that have been identified by OCR investigations. OCR's 2022 outreach highlights include:

- OCR conducted 124 outreach events for HIPAA covered entities, business associates, and other health care industry stakeholders. These presentations addressed new rulemaking and guidance, trends in large breaches reported to OCR, recent HIPAA enforcement actions, cybersecurity and ransomware resources, and the requirements of the HIPAA Rules.

- An amendment to the HITECH Act was signed into law and effective January 5, 2021, requiring OCR to consider whether a regulated entity has "adequately demonstrated that it had, for not less than the previous twelve months, recognized security practices (RSPs) in place" that may mitigate a civil money penalty or "remedies that would otherwise be agreed to in any agreement with respect to resolving potential violations of the HIPAA Security Rule." In support of this amendment, OCR published a request for information to obtain public input to assist in developing potential future guidance or rulemaking regarding RSPs, and OCR published a video in October 2022, explaining how OCR is requesting evidence of RSPs, how regulated entities can demonstrate their implementation of RSPs, resources on RSPs, and answers to questions received on RSPs. The video may be found on OCR's YouTube channel at: https://youtu.be/e2wG7jUiRjE. It has over 11,000 views.

- OCR and ONC hosted a series of webinars with over 2,000 registrants, to review updates to the popular HHS Security Risk Assessment Tool, highlighting a number of enhancements which make the tool easier to use and apply more broadly to the risks to health information. The tool is designed for use by small to medium sized health care practicesand business associates to help them identify risks and vulnerabilities to electronic protected health information (ePHI). The updated tool provides enhanced functionality to document how such organizations can implement or plan to implement appropriate security measures to protect ePHI.

- OCR hosted eleven convenings in support of President Biden's two Executive Orders issued in the weeks after the *Dobbs* decision that mapped the Administration's plan for ensuring access to reproductive care, EO 14076 *Protecting Access to Reproductive and Other Healthcare Service*s and EO 14079 *Securing Access to Reproductive and Other Healthcare Services*. These convenings consisted of conversations with health care providers and other stakeholders across the country, to provide information on Federal non-discrimination laws as well as how to better protect sensitive information related to reproductive health care and bolster patient-provider confidentiality under HIPAA.

- OCR issued "Guidance on the HIPAA Privacy Rule and Disclosures of Information Relating to Reproductive Health Care" following the *Dobbs v. Jackson Women's Health Organization* decision to address how the HIPAA Privacy Rule protects individuals' private medical information relating to abortion and other sexual and reproductive health care. This guidance addresses the circumstances under which the Privacy Rule permits disclosure of protected health information without an individual's authorization and explains that disclosures for purposes not related to health care, such as disclosures to law enforcement officials, are permitted only in narrow circumstances tailored to protect the individual's privacy and support their access to health care, including abortion care.

- OCR issued guidance on "Protecting the Privacy and Security of Your Health Information When Using Your Personal Cell Phone or Tablet". This guidance explains that, generally, the HIPAA Rules do not apply to individuals' health information when it is stored or access using a personal mobile device. This guidance also explains how to turn off the location services on Apple and Android devices and identifies best practices for selecting apps, browsers, and search engines that are recognized as supporting increased privacy and security.

- OCR issued "Guidance on HIPAA and Audio-Only Telehealth" helping to ensure that individuals can continue to benefit from audio-only telehealth by clarifying how covered entities can provide telehealth services and improve public confidence that covered entities are protecting the privacy and security of their health information. While telehealth can significantly expand access to health care, certain populations may have difficulty accessing or be unable to access technologies used for audio-video telehealth because of various factors, including financial resources, internet access, availability of sufficient broadband, and cell coverage in the geographic area. Audio-only telehealth, especially using technologies that do not require broadband availability, can help address the needs of some of these individuals.

- OCR published a cybersecurity newsletter issued via OCR's listserv and available on OCR's website on Defending Against Common Cyber-Attacks to support improved cybersecurity in defense of hacking, the most common type of large breach reported to OCR annually. This newsletter addresses phishing, exploitation of known vulnerabilities (*e.g.*, unpatched software), and weak cybersecurity practices (*e.g.*, weak passwords), and it identifies best practices, HIPAA Security Rule requirements, and resources for regulated entities to consult.

- OCR published a cybersecurity newsletter issued via OCR's listserv and available on OCR's website on the HIPAA Security Rule Security Incident Procedures requirement. The newsletter provides best practices and requirements for drafting security incident policies and procedures, forming a security incident response team, identifying security incidents, responding to security incidents, mitigating the harmful effects of security incidents, documenting security incidents, and fulfilling HIPAA Breach Notification requirements.

- OCR, The Federal Trade Commission (FTC), the HHS Office of the National Coordinator for Health Information Technology (ONC), and the Food and Drug Administration (FDA) updated the Mobile Health App Interactive Tool, a tool that is designed to help developers of health-related mobile apps understand what federal laws and regulations might apply to them, including the FTC Act, the FTC's Health Breach Notification Rule, the Children's Online Privacy Protection Act (COPPA), the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Federal Food, Drug and Cosmetics Act (FD&C Act), and the 21st Century Cures Act and ONC Information Blocking Regulations.

- OCR issued a bulletin on Use of Online Tracking Technologies to address a growing concern OCR was observing in media reports and news stories about health care entities using tracking technologies like Google Analytics or Meta Pixel to collect and analyze information about how internet users are interacting with their websites or mobile applications. The Bulletin addresses potential impermissible disclosures of ePHI by HIPAA regulated entities to online technology tracking vendors. The Bulletin explains what tracking technologies are, how they are used, and what steps regulated entities must take to protect ePHI when using tracking technologies to comply with the HIPAA Rules.

Audits

OCR did not initiate any audits in 2022 due to a lack of financial resources.

Appendix

Resolution Agreements and Civil Money Penalties[17] in 2022

Resolution Agreement with Northcutt Dental

Northcutt Dental-Fairhope, LLC (Northcutt) paid $62,500 and agreed to take corrective actions to settle potential violations of the HIPAA Privacy Rule. Northcutt is a dental practice serving patients in southern Alabama and the Florida panhandle.

In May 2018, OCR received a complaint filed against Northcutt alleging that it impermissibly provided patients' protected health information (PHI) to unauthorized third parties for political campaign purposes. OCR's investigation determined that Northcutt impermissibly shared the PHI of 9,043 patients with a campaign manager and a third-party marketing firm to assist with a state senate election campaign, Northcutt did not designate a privacy official until November 2017, and Northcutt did not implement privacy and breach notification policies and procedures until January 2018.

In addition to the monetary settlement, Northcutt agreed to:

- Review and revise its written policies and procedures to comply with the HIPAA Rules;
- Distribute policies and procedures to workforce members; and
- Train workforce members on the revised policies and procedures.

This settlement occurred in March 2022. The resolution agreement is available at the following link:
www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/northcutt/index.html.

Civil Money Penalty imposed on ACPM Podiatry

OCR imposed a civil money penalty of $100,000 against ACPM Podiatry (ACPM) for failing to provide timely access to medical records in violation of the HIPAA Privacy Rule's right of access provision. ACPM is a group practice providing podiatry services to patients in Peoria and Canton, Illinois.

In April 2019, OCR received a complaint alleging that ACPM failed to respond to a request for medical records. OCR provided ACPM with written technical assistance regarding the Privacy Rule's right of access standard and the need to provide the requested records and closed the matter. The following month, OCR received a second complaint from the complainant alleging that ACPM still had not provided him with a copy of his medical records after numerous requests. OCR initiated an investigation; however, ACPM did not respond to OCR's data requests or other inquiries regarding the investigation. Upon the conclusion of the investigation, OCR sent ACPM

[17] Information provided here on Resolution Agreements and CMPs are based on the year in which the Agreement was signed, or the CMP assessed. Investigations of these cases were initiated in years prior to 2022.

a Notice of Proposed Determination notifying them of the results of the investigation and providing the opportunity to resolve the matter via a resolution agreement and corrective action plan. ACPM did not engage in settlement negotiations and did not request a hearing to contest the findings in OCR's Notice of Proposed Determination. OCR imposed a civil money penalty in the amount of $100,000.

The notice of final determination was issued in April 2022. The notice of proposed determination and notice of final determination are available at the following link: www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/ACPM/index.html.

Resolution Agreement with Lawrence Bell, Jr., DDS, PA

Lawrence Bell, Jr., DDS, PA (Bell) paid $5,000 and agreed to take corrective actions to settle a potential violation of the HIPAA Privacy Rule's right of access standard. Bell is a dental practice located in Baltimore, Maryland.

In October 2019, OCR received a complaint alleging that Bell failed to respond in a timely manner to a patient's request for access to his PHI. OCR's investigation determined that Bell's failure to provide timely access to the requested records was a potential violation of the HIPAA right of access standard. As a result of OCR's investigation, Bell provided access to all of the requested records.

In addition to the monetary settlement, Bell agreed to:

- Provide the patient with access to the requested records;
- Review, and if necessary, revise right of access policies and procedures to comply with the HIPAA Privacy Rule;
- Submit a listing of all requests for access to PHI every ninety (90) days and any denials of requests for access for the duration of the CAP; and
- Train workforce members on the policies and procedures and HIPAA's right of access provisions.

This settlement occurred in April 2022. The resolution agreement is available at the following link: www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/bell-dental/index.html.

Resolution Agreement with Oklahoma State University – Center for Health Sciences

Oklahoma State University – Center for Health Sciences (OSU-CHS) paid $875,000 and agreed to take corrective actions to settle potential violations of the HIPAA Privacy, Security, and Breach Notification Rules. OSU-CHS is a public land-grant research facility that provides preventative, rehabilitation, and diagnostic care in Oklahoma.

OCR began investigating OSU-CHS after it filed a breach report stating that an unauthorized third party had gained access to a web server that contained electronic PHI. The hackers installed malware that ultimately resulted in the impermissible disclosure of the PHI of 279,865 individuals. OCR's investigation found potential violations of the HIPAA Rules including

impermissible uses and disclosures of PHI, failure to conduct an accurate and thorough risk analysis, failure to implement audit controls, failure to provide security incident response and reporting, and failure to provide timely breach notification to affected individuals and HHS.

In addition to the monetary settlement, OSU-CHS agreed to:

- Conduct a comprehensive and thorough risk analysis;
- Develop an enterprise-wide Risk Management Plan to address and mitigate security risks and vulnerabilities found in the risk analysis;
- Develop, maintain, and revise, as necessary its written policies and procedures to comply with the HIPAA Rules;
- Distribute policies and procedures to workforce members; and
- Train workforce members on the policies and procedures for the privacy and security of PHI.

This settlement occurred in May 2022. The resolution agreement is available at the following link: www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/osu/index.html.

Resolution Agreement with Southwest Surgical Associates

Southwest Surgical Associates (SWSA) paid $65,000 and agreed to take corrective actions to settle a potential violation of the HIPAA Privacy Rule's right of access standard. SWSA is a group practice serving the greater Houston, Texas area.

In December 2020, OCR received a complaint alleging that SWSA failed to respond in a timely manner to a patient's request for a copy of her PHI. OCR's investigation determined that SWSA's failure to provide timely access to the requested records was a potential violation of the HIPAA right of access standard. As a result of OCR's investigation, SWSA provided access to all of the requested records.

In addition to the monetary settlement, SWSA agreed to:

- Review, and if necessary, revise right of access policies and procedures to comply with the HIPAA Privacy Rule;
- Submit a listing of all requests for access to PHI every ninety (90) days and any denials of requests for access for the duration of the CAP; and
- Train workforce members on the policies and procedures and HIPAA's right of access provisions.

This settlement occurred in May 2022. The resolution agreement is available at the following link: www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/southwest-surgical/index.html.

Resolution Agreement with Memorial Hermann Health System

Memorial Hermann Health System (MHHS) paid $240,000 and agreed to take corrective actions to settle a potential violation of the HIPAA Privacy Rule's right of access standard. MHHS is a

not-for-profit health system with 17 hospitals located in Southeast Texas.

In August 2020, a complaint was filed with OCR alleging that MHHS failed to take timely action in response to a patient's multiple requests (five) for her medical and billing records. OCR initiated an investigation and determined that MHHS's failure to provide timely access to the requested medical records was a potential violation of the HIPAA right of access standard. As a result of OCR's investigation, MHHS provided access to all of the requested records.

In addition to the monetary settlement, MHHS agreed to:

- Revise right of access policies and procedures to comply with the HIPAA Privacy Rule;
- Train workforce members on the policies and procedures and HIPAA's right of access provisions; and
- Submit a listing of all requests for access to PHI every ninety (90) days sent to MHHS's billing department and any denials of requests for access for the duration of the CAP.

This settlement occurred in May 2022. The resolution agreement is available at the following link: www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/memorial-hermann-roa/index.html.

Resolution Agreement with Melrose Wakefield Healthcare

Melrose Wakefield Healthcare (MWH) paid $54,500 and agreed to take corrective actions to settle a potential violation of the HIPAA Privacy Rule's right of access provision. MWH is located in Melrose, Massachusetts.

In July 2020, a complaint was filed with OCR alleging that MWH failed to take timely action in response to a personal representative's request for a copy of her mother's medical records. OCR initiated an investigation and determined that MHHS's failure to provide timely access to the requested medical records was a potential violation of the HIPAA right of access standard. As a result of OCR's investigation, MWH provided the complainant with a copy of the requested records.

In addition to the monetary settlement, MWH agreed to:

- Develop, maintain, and revise, as necessary, its written policies and procedures to comply with the HIPAA Privacy Rule; and
- Train workforce members on the HIPAA policies and procedures.

This settlement occurred in May 2022. The resolution agreement is available at the following link: www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/melrose/index.html.

Resolution Agreement with Hillcrest Commons Nursing & Rehabilitation Center

Hillcrest Commons Nursing & Rehabilitation Center (Hillcrest) paid $55,000 and agreed to take corrective actions to settle a potential violation of the HIPAA Privacy Rule's right of access provision. Hillcrest is a nursing and rehabilitation center located in Pittsfield, Massachusetts.

In July 2020, OCR initiated an investigation after receiving a complaint that, as her son's healthcare proxy, the complainant was denied a copy of her son's medical records. OCR's investigation revealed that Hillcrest failed to provide timely access to the requested records. As a result of the investigation, Hillcrest provided access to all of the requested records.

In addition to the monetary settlement, Hillcrest agreed to:

- Develop, maintain, and revise, as necessary, its written policies and procedures to comply with the HIPAA Privacy Rule; and
- Train workforce members on the HIPAA policies and procedures.

This settlement occurred in May 2022. The resolution agreement is available at the following link: www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/hillcrest/index.html.

Resolution Agreement with Danbury Psychiatric Consultants

Danbury Psychiatric Consultants (DPC) paid $3,500 and agreed to take corrective actions to settle a potential violation of the HIPAA Privacy Rule's right of access provision. DPC is a group practice offering psychiatric services in Massachusetts.

In March 2020, OCR received a complaint alleging that DPC failed to provide the complainant with a copy of her medical records. OCR's investigation found that DPC was withholding the requested records until the complainant (1) submitted a signed request or authorization for the release of the records and (2) paid an outstanding monetary balance for services rendered. OCR initiated an investigation and determined that DPC's failure to provide timely access to the requested medical records was a potential violation of the HIPAA right of access standard. As a result of OCR's investigation, DPC provided the requested records.

In addition to the monetary settlement, DPC agreed to:

- Develop, maintain, and revise, as necessary, its written policies and procedures to comply with the HIPAA Privacy Rule; and
- Train all workforce members on the policies and procedures.

This settlement occurred in May 2022. The resolution agreement is available at the following link: www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/danbury/index.html.

Resolution Agreement with Coastal Ear, Nose, & Throat

Coastal Ear, Nose, & Throat (Coastal ENT) paid $20,000 and agreed to take corrective actions to settle a potential violation of the HIPAA Privacy Rule's right of access provision. Coastal ENT is a group practice providing services in Florida.

In January and April 2021, OCR received several complaints alleging that Coastal ENT failed to provide a complainant with a copy of his medical records after multiple requests. OCR's investigation determined that Coastal ENT's failure to provide timely access to the requested medical records was a potential violation of the HIPAA right of access standard. As a result of OCR's investigation, Coastal ENT provided the requested records.

In addition to the monetary settlement, ENT agreed to:

- Develop, maintain, and revise, as necessary, its written policies and procedures to comply with the HIPAA Privacy Rule; and
- Train all workforce members on the policies and procedures.

This settlement occurred in May 2022. The resolution agreement is available at the following link: www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/coastal-ent/index.html.

Resolution Agreement with Fallbrook Family Health Center

Fallbrook Family Health Center (FFHC) paid $30,000 and agreed to take corrective actions to settle a potential violation of the HIPAA Privacy Rule's right of access standard. FFHC is located in Nebraska, and provides family health care services.

In March 2020, OCR received a complaint alleging that FFHC failed to provide the complainant with a copy of her medical records despite requesting them, in writing, three times. OCR initiated an investigation and determined that FFHC's' failure to provide the requested medical records was a potential violation of the HIPAA right of access standard. As a result of OCR's investigation, FFHC provided a complete copy of the requested medical records.

In addition to the monetary settlement, FFHC agreed to:

- Review and to the extent necessary, revise its right of access policies and procedures to comply with the HIPAA Privacy Rule;
- Train workforce members on the policies and procedures; and
- Review and to the extent necessary, revise its Notice of Privacy Practices to comply with the HIPAA Privacy Rule.

This settlement occurred in June 2022. The resolution agreement is available at the following link: www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/fallbrook/index.html.

Resolution Agreement with Erie County Medical Center Corporation

Erie County Medical Center (ECMC) paid $50,000 and agreed to take corrective actions to settle a potential violation of the HIPAA Privacy Rule's right of access standard. ECMC is a public hospital located in Buffalo, New York.

In December 2019, OCR received a complaint alleging that ECMC failed to provide the complainant's husband with a complete copy of his medical records. OCR initiated an investigation and during the investigation ECMC provided the complainant's husband with a complete copy of his requested records. OCR's investigation determined that ECMC failed to provide timely access to PHI.

In addition to the monetary settlement, ECMC agreed to:

- Review and to the extent necessary, revise its right of access policies and procedures to comply with the HIPAA Privacy Rule;

- Train workforce members on the policies and procedures; and
- Submit a listing of all requests for access to PHI and any denials of requests for access every ninety (90) days for the duration of the CAP.

This settlement occurred in June 2022. The resolution agreement is available at the following link: www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/ecmc/index.html.

Resolution Agreement with Associated Retina Specialists

Associated Retina Specialists (ARS) paid $22,500 and agreed to take corrective actions to settle a potential violation of the HIPAA Privacy Rule's right of access standard. ARS is an ophthalmology practice located in New York, New York.

In February 2021, OCR received a complaint alleging that ARS failed to provide the complainant with a copy of her medical records. OCR initiated an investigation and determined that ARS's failure to provide timely access to medical records was a potential violation of the HIPAA right of access standard. As a result of OCR's investigation, the complainant received a copy of her medical records, nearly five months after the initial request.

In addition to the monetary settlement, ARS agreed to:

- Review and to the extent necessary, revise its right of access policies and procedures to comply with the HIPAA Privacy Rule; and
- Train workforce members on the policies and procedures.

This settlement occurred in June 2022. The resolution agreement is available at the following link: www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/associated-retina/index.html.

Resolution Agreement with New England Dermatology dba New England Dermatology and Laser Center

New England Dermatology, P.C. dba New England Dermatology and Laser Center (NEDLC) paid $300,640 and agreed to take corrective actions to settle a potential violation of the HIPAA Privacy Rule. NEDLC is located in Massachusetts and provides dermatology services.

OCR began investigating NEDLC after it filed a breach report stating that empty specimen containers with PHI on the labels were placed in garbage bins located in the parking lot. In its investigation, OCR found potential violations of the HIPAA Privacy Rule including the impermissible use and disclosure of PHI and failure to maintain appropriate safeguards to protect the privacy of PHI.

In addition to the monetary settlement, NEDLC agreed to:

- Develop, maintain, and revise, as necessary its written policies and procedures to comply with the HIPAA Privacy Rule;
- Distribute policies and procedures to workforce members; and

- Train workforce members on the policies and procedures for the privacy of PHI.

This settlement occurred in July 2022. The resolution agreement is available at the following link: www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/nedlc/index.html.

Resolution Agreement with Family Dental Care

Family Dental Care (FDC) paid $30,000 and agreed to take corrective actions to settle a potential violation of the HIPAA Privacy Rule's right of access standard. FDC is located in Chicago, Illinois and provides dental services.

In August 2020, OCR received a complaint alleging that FDC failed to provide the complainant with a complete copy of her medical records after requesting them in May 2020. OCR's investigation determined that FDC's failure to provide a complete copy of the requested medical records was a potential violation of the HIPAA right of access standard. As a result of OCR's investigation, FDC provided the complainant with a complete copy of her medical records.

In addition to the monetary settlement, FDC agreed to:

- Develop, maintain, and revise, as necessary its written policies and procedures to comply with the HIPAA Privacy Rule; and
- Train all workforce members on the policies and procedures.

This settlement occurred in August 2022. The resolution agreement is available at the following link: www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/fdc/index.html.

Resolution Agreement with Great Expressions Dental Care of Georgia

Great Expressions Dental Care of Georgia (GEDC-GA) paid $80,000 and agreed to take corrective actions to settle potential violations of the HIPAA Privacy Rule's right of access standard. GEDC-GA is a dental and assessing orthodontics provider with multiple locations in Georgia.

In November 2020, OCR received a complaint alleging that GEDC-GA failed to provide the complainant with a copy of her medical records until she paid the copying fee of $170. The complainant first requested her medical records in November 2019 but did not receive them until February 2021, as a result of OCR's investigation. OCR determined that the practice's failure to provide the requested medical records in a timely fashion and its practice of copying fees that were not reasonable or cost-based were potential violations of the HIPAA right of access standard.

In addition to the monetary settlement, GEDC-GA agreed to:

- Develop, maintain, and revise, as necessary its written policies and procedures to comply with the HIPAA Privacy Rule; and
- Train workforce members on HIPAA's right of access provisions.

This settlement occurred in August 2022. The resolution agreement is available at the following link: www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/gedc-ga/index.html.

Resolution Agreement with B. Steven L. Hardy, DDS dba Paradise Family Dental

B. Steven L. Hardy, DDS dba Paradise Family Dental (Paradise) paid $25,000 and agreed to take corrective actions to settle a potential violation of the HIPAA Privacy Rule's right of access standard. Paradise is a dental practice located in Las Vegas, Nevada.

In October 2020, OCR received a complaint alleging that Paradise failed to provide the complainant with a copy of her and her son's medical records. OCR initiated an investigation and determined that Paradise's failure to provide the requested medical records was a potential violation of the HIPAA right of access standard. As a result of OCR's investigation, the complainant received a copy of her and her son's medical records on December 31, 2020, more than eight months after the initial request.

In addition to the monetary settlement, Paradise agreed to:

- Develop its right of access policies and procedures to comply with the HIPAA Privacy Rule;
- Review and revise its Notice of Privacy Practices to comply with the HIPAA Privacy Rule; and
- Train workforce members on policies and procedures and Notice of Privacy Practices.

This settlement occurred in August 2022. The resolution agreement is available at the following link: www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/paradise/index.html.

Resolution Agreement with Brandon Au, DDS dba New Vision Dental

Brandon Au, DDS dba New Vision Dental (New Vision) paid $23,000 and agreed to take corrective actions to settle potential violations of the HIPAA Privacy Rule. New Vision is a dental practice located in South Pasadena and Glendora, California.

In November 2017, OCR received a complaint alleging that New Vision impermissibly disclosed the PHI of numerous patients in response to online reviews of its practice. OCR's investigation found indicia that New Vision impermissibly disclosed PHI, failed to have the minimum content required in its Notice of Privacy Practices, and failed to implement policies and procedures with respect to PHI, including releasing PHI on social media/public platforms. In addition to the monetary settlement, New Vision agreed to:

- Develop, maintain, and revise, as necessary its written policies and procedures to comply with the HIPAA Privacy Rule;
- Distribute policies and procedures to workforce members;
- Train workforce members on the policies and procedures;
- Remove all social media posts containing PHI;
- Notify individuals whose PHI was disclosed;

- Provide substitute notice on its individual Yelp page;
- Submit breach notice on OCR's breach portal pertaining to the individuals' whose PHI was disclosed;
- Develop a compliant Notice of Privacy Practices; and
- Update its website with the revised Notice of Privacy Practices.

This settlement occurred in November 2022. The resolution agreement is available at the following link: www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/new-vision/index.html.

Resolution Agreement with Health Specialists of Central Florida

Health Specialists of Central Florida (Health Specialists) paid $20,000 and agreed to take corrective actions to settle a potential violation of the HIPAA Privacy Rule's right of access provision. Health Specialists is a primary care practice in Florida.

In August 2019, OCR received a complaint alleging that Health Specialists failed to provide the complainant with a copy of her deceased father's medical records after submitting multiple requests. OCR's investigation determined that Health Specialists' failure to provide timely access to the requested medical records was a potential violation of the HIPAA right of access standard. As a result of OCR's investigation, Health Specialists provided the requested records nearly five months after the initial request.

In addition to the monetary settlement, Health Specialists agreed to:

- Develop, maintain, and revise, as necessary its written policies and procedures to comply with the HIPAA Privacy Rule; and
- Train all workforce members on the policies and procedures.

This settlement occurred in November 2022. The resolution agreement is available at the following link: www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/health-specialists/index.html.

Resolution Agreement with Life Hope Labs

Life Hope Labs (LHL) paid $16,500 and agreed to take corrective actions to settle a potential violation of the HIPAA Privacy Rule's right of access provision. LHL is a diagnostic laboratory located in Sandy Springs, Georgia.

In August 2021, OCR received a complaint alleging that LHL failed to provide the complainant with a copy of her deceased father's medical records in a timely fashion. The complainant initially filed the request for medical records in July 2021; however, she did not receive them until February 2022, seven months after the initial request and as a result of OCR's investigation. OCR's investigation determined that LHL's failure to provide timely access to the requested medical records was a potential violation of the HIPAA right of access standard.

In addition to the monetary settlement, LHL agreed to:

- Develop, maintain, and revise, as necessary its written policies and procedures to comply with the HIPAA Privacy Rule; and
- Train all workforce members on the policies and procedures.

This settlement occurred in December 2022. The resolution agreement is available at the following link: www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/life-hopes/index.html.

Resolution Agreement with Banner Health

Banner Health Affiliated Covered Entities (Banner Health) paid $1,250,000 and agreed to take corrective actions to settle potential violations of the HIPAA Security Rule. Banner is a nonprofit health system headquartered in Phoenix, Arizona.

OCR began investigating Banner after it filed a breach report stating that a threat actor had gained unauthorized access to ePHI. The hackers were able to gain access to the PHI of 2.81 million individuals. OCR's investigation found potential violations of the HIPAA Rules including failures to: conduct an accurate and thorough risk analysis, regularly review records of information system activity, implement procedures to verify that a person or entity seeking access to ePHI is the one claimed, and implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network.

In addition to the monetary settlement, Banner agreed to:

- Conduct a comprehensive and thorough risk analysis;
- Develop an enterprise-wide risk management plan to address and mitigate security risks and vulnerabilities found in the risk analysis;
- Develop, maintain, and revise, as necessary its written policies and procedures to comply with the HIPAA Rules; and
- Distribute policies and procedures to workforce members.

This settlement occurred in December 2022. The resolution agreement is available at the following link: www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/banner-health/index.html.