Annual Report to Congress on HIPAA Privacy, Security, and Breach Notification Rule Compliance For Calendar Year 2023

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 2023 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 received 30,968 new complaints and carried over 9,680 complaints from 2022, alleging violations of the HIPAA Rules and the HITECH Act. OCR resolved 38,601 complaints. OCR resolved five complaint investigations with Resolution Agreements and Corrective Action Plans (RA/CAPs) and monetary settlements totaling $320,000.

OCR initiated 773 compliance reviews and completed 737 compliance reviews. Nine compliance reviews were resolved with RA/CAPs and monetary settlements totaling $7,415,000. OCR issued no subpoenas, and no audits were initiated.

OCR engaged in 182 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 updated its HIPAA web content regularly, providing information and guidance in both English and Spanish. Visits to OCR's HIPAA webpages averaged 412,000 unique visits per month, and approximately 4.9 million visits overall.

Background

HIPAA was enacted on August 21, 1996. Subtitle F of HIPAA, known as the Administrative Simplification provisions, permitted the Secretary of HHS (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.[1] A "business associate" is a person or

[1] 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 business associates of HIPAA covered entities, effective September 23, 2013.

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, maintaining, or transmitting protected health information (PHI).[2] Any subcontractor of a 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 C.F.R. Part 160 and Subparts A and E of Part 164, provides important federal protections to protect the privacy of PHI and gives individuals certain 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 C.F.R. 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 C.F.R. 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 to prepare and submit an annual report to the Senate Committee on 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 [the Privacy 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 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;

[2] 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 after September 23, 2009.[3] This report includes information about HHS's enforcement process with regard to the Privacy, Security, and Breach Notification Rule (the HIPAA Rules), and information about HHS's actions to enforce the HIPAA Rules during the calendar year of 2023.

This report is prepared for the calendar year 2023. 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[4] and providing education and outreach to support compliance with the HIPAA Rules, which are discussed later in this report. When necessary, OCR has the 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[5]:

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

[3] 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 of unsecured PHI reported to the Secretary and the actions that have been taken by covered entities and business associates in response to the reported breaches.

[4] 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.

[5] *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 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.[6] 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).[7] 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.

Investigations

Once OCR initiates an investigation, OCR may collect evidence through interviews, witness

[6] "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.

[7] 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.

statements, requests for data from the entity involved, site visits, or other available, relevant documents and information. 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, an OCR investigation may determine that there is insufficient evidence to support a finding that a covered entity or business associate violated the HIPAA Rules. In such cases, OCR may send 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 the regulated entity's compliance through corrective action, which may include a resolution agreement.

Where corrective action is sought, OCR may obtain satisfactory documentation and other evidence from the covered entity or business associate that it undertook the required corrective action toresolve 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 HIPAA noncompliance warrants additional enforcement action, OCR typically pursues a resolution agreement ("RA") with a payment of a settlement amount and an obligation to complete a corrective action plan ("CAP", or "RA/CAP"). In these cases, OCR notifies the covered entity or business associate that, while OCR is prepared to assess a CMP with regard to identified 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 generally involve the payment of a monetary settlement 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 (*e.g.,* one to three years). 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 the investigated entities' noncompliance and deter future noncompliance with the HIPAA Rules, and when OCR announces those resolutions, the announcements serve as reminders to the wider regulated community of their own HIPAA compliance 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 OCR proposes a CMP, 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 issue a final determination and impose a CMP.

Audits

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

These reviews 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 2023 due to a lack of financial resources.

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 2023, OCR resolved 14 investigations with RA/CAPs or the imposition of CMPs totaling $7,735,000.[8]

As shown in the table on the following page, between 2019 and 2023, the number of complaints received by OCR increased 10%, and the number of compliance reviews initiated by OCR increased by 27%.

[8] David Mente, MA, LPC ($15,000), MedEvolve, Inc. ($350,000), Manasa Health Center ($30,000), iHealth Solutions, LLC ($75,000), Yakima Valley Memorial Hospital (formerly Virginia Mason) ($240,000), L.A. Care Health Plan ($1,300,000), UnitedHealthcare Insurance Company ($80,000), St. Joseph's Medical Center ($80,000), Doctor's Management Services ($100,000), Phoenix Healthcare LLC dba Green County Care Center ($35,000), Green Ridge Behavioral Health, LLC ($40,000), Lafourche Medical Group, LLC ($480,000), Riverside Medical Group/Optum Medical Care of New Jersey ($160,000), and Montefiore Medical Center ($4,750,000).

Year	Complaints Received	Compliance Reviews Initiated (Included Reported Breaches)	% Change in Complaints Received (Year-Over-Year)	% Change in Compliance Reviews Initiated (Year-Over-Year)
2023	30,968	773	2% increase	14% increase
2022	30,435	676	11% decrease	<1% increase
2021	34,077	674	25% increase	10% decrease
2020	27,182	746	4% decrease	22% increase
2019	28,261	611	-	-
2019 to 2023	-	-	10% increase	27% increase

Source: Current and previous reports to Congress https://www.hhs.gov/ocr/about-us/reports/index.html

Enforcement Data

Complaint Resolutions

2023 Complaints

During calendar year 2023, OCR received 30,968 new HIPAA complaints and carried over 9,680 open complaints from 2022. OCR resolved 38,601 complaints during calendar year 2023.[9] Of those, OCR resolved 30,464 (79%) 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 6,749 complaints (17%) by providing technical assistance in lieu of an investigation. See Figure 1.

OCR completed 1,388 complaint investigations.[10] In 691 of these investigations (50%), OCR required the covered entity or business associate to take corrective action. In 695 of the investigated complaints (50%), OCR found insufficient evidence that a violation of the HIPAA Rules had occurred. In 2 of these investigations, OCR provided technical assistance after initiating an investigation (<1%). See Figure 2.

[9] 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.

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

HHS OFFICE FOR CIVIL RIGHTS
COMPLAINT RESOLUTIONS AND INVESTIGATIONS

NUMBER OF CASES CLOSED AND TYPE OF CLOSURES

JANUARY 1, 2023, THROUGH DECEMBER 31, 2023

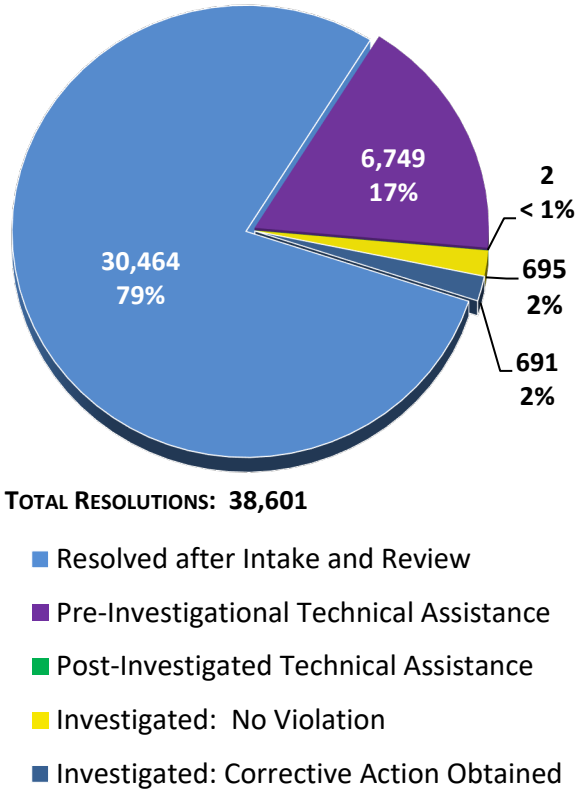

Figure 1

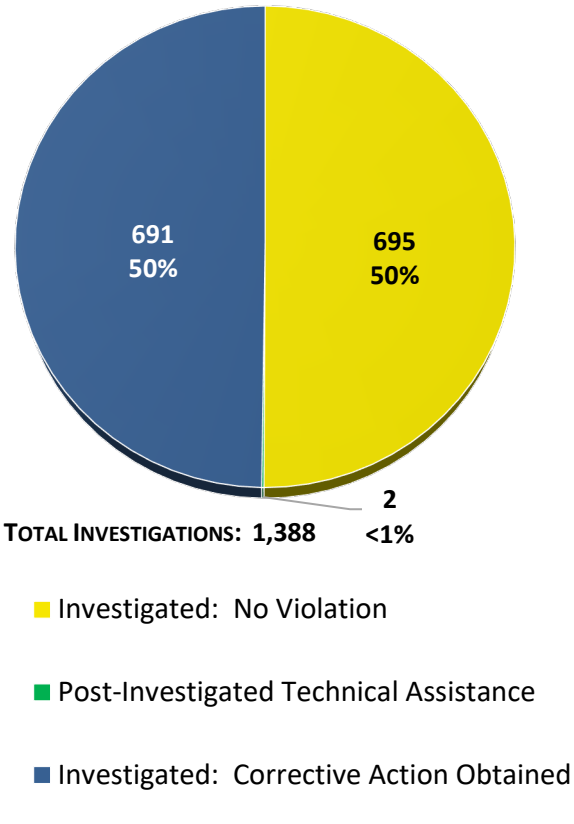

Figure 2

OCR resolved five complaint investigations in 2023 with resolution agreements and/or CAPs and monetary settlements totaling $320,000.[11]

For the 38,601 complaints that OCR resolved in 2023, the top five issues alleged were *Right of Access* (796 complaints), *Impermissible Uses and Disclosures* (502 complaints), *General Safeguards* (412 complaints), *Administrative Safeguards* (Security Rule) (145 complaints), and *Breach-Notice to Individuals* (107 complaints).

[11] The five complaint investigations resolved with RA/CAPs and monetary settlements are: David Mente, MA, LPC ($15,000); Manasa Health Center ($30,000); UnitedHealthcare Insurance Company ($80,000); Optum Medical Care of New Jersey ($160,000); and Phoenix Healthcare LLC dba Green County Care Center ($35,000).

Compliance Reviews

2023 Compliance Reviews

During calendar year 2023, OCR initiated 773 compliance reviews to investigate allegations of violations of the HIPAA Rules that did not arise from complaints.[12] Of these, 732 compliance reviews were initiated because of a breach report of unsecured PHI affecting 500 or more individuals and 9 were a result of a breach report affecting fewer than 500 individuals. The remaining 32 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 737 compliance reviews in 2023. Most 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.[13] Of the closed cases, 724 originated from breach reports and 13 originated from other means. The covered entity or business associate took corrective action in 580 cases (79%). OCR provided the covered entity or business associate with *technical assistance* after investigation in 60 cases (8%). OCR found that there was insufficient evidence of a violation of the HIPAA Rules in 67 cases (9%), and OCR determined that it did not have jurisdiction to investigate the allegations in 30 cases (4%). Of the completed compliance reviews, nine cases were resolved with resolution agreements, CAPs and monetary settlements totaling $7,415,000.[14] See Figure 3.

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

[13] The new compliance reviews initiated, and compliance reviews resolved in a calendar year are not the same asOCR 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.

[14] The nine cases that were resolved with RA/CAPs and monetary settlements are MedEvolve, Inc. ($350,000), iHealth Solutions, LLC ($75,000), Yakima Valley Memorial Hospital ($240,000), L.A. Care Health Plan ($1,300,000), St. Joseph's Medical Center ($80,000), Doctor's Management Services ($100,000), Green Ridge Behavioral Health, LLC ($40,000), Lafourche Medical Group, LLC ($480,000), and Montefiore Medical Center ($4,750,000).

HHS OFFICE FOR CIVIL RIGHTS
COMPLIANCE REVIEWS

NUMBER OF CASES CLOSED AND TYPES OF CLOSURES

JANUARY 1, 2023 – DECEMBER 31, 2023

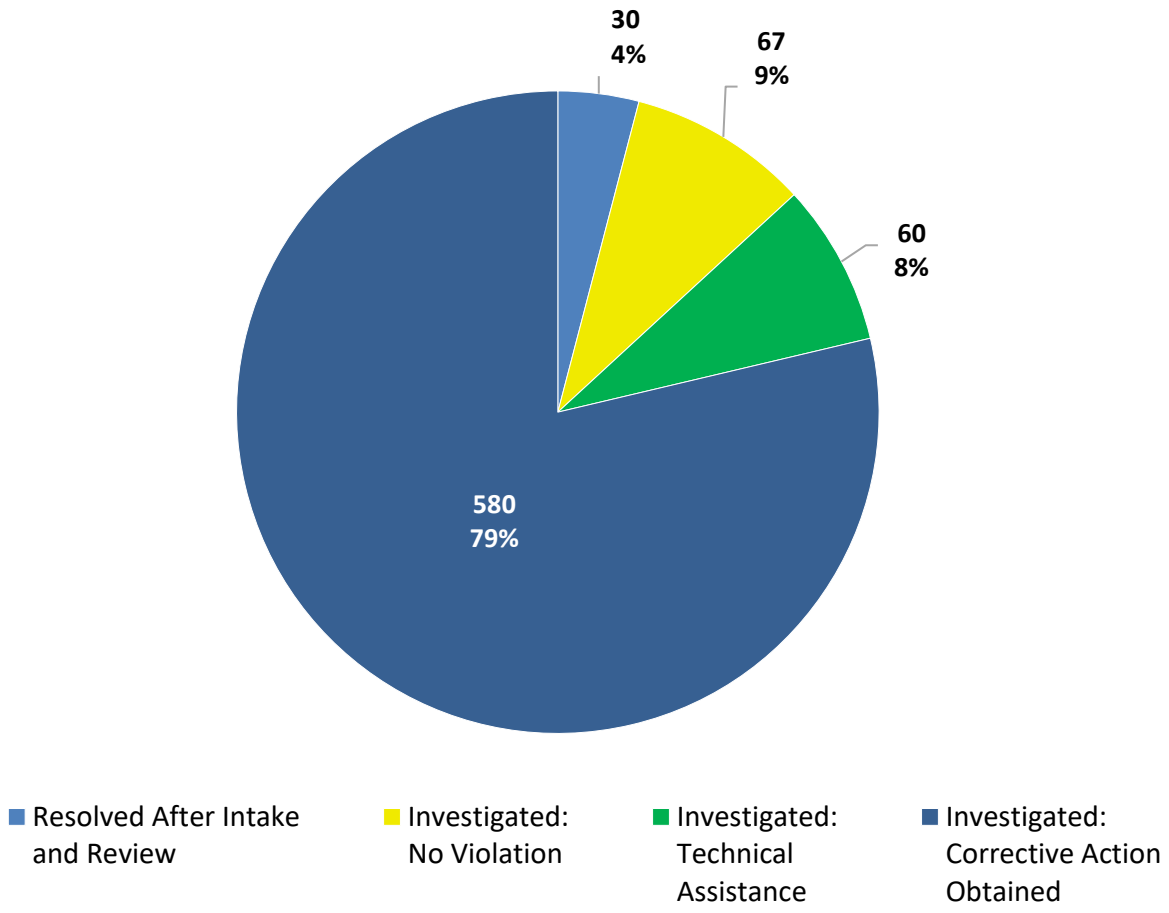

Figure 3

Subpoenas

OCR did not issue any subpoenas in 2023.

Secretary's Plan for Improving Compliance – Ongoing Outreach Efforts to IncreaseAwareness 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 2023 outreach highlights include:

- OCR conducted 182 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.
- In April 2023, OCR issued a Notice of Proposed Rulemaking (NPRM) on the HIPAA Privacy Rule to Support Reproductive Health Care Privacy. The proposal would modify existing standards by prohibiting uses and disclosures of PHI for criminal, civil, or administrative investigations or proceedings against individuals, regulated entities, or other persons for seeking, obtaining, providing, or facilitating lawful reproductive health care.
- In June 2023, OCR published a cybersecurity newsletter issued via OCR's listserv and available on OCR's website on HIPAA and Cybersecurity Authentication to support improved cybersecurity in defense of hacking, the most common type of large breach reported to OCR annually. This newsletter addresses multi-faceted authentication processes and procedures, as well as requirements outlined in the HIPAA Security Rule to implement strong authentication practices to ensure the confidentiality, integrity, and availability of electronic protected health information (ePHI).
- In July 2023, OCR and the Federal Trade Commission (FTC) sent a joint letter to approximately 130 hospital systems and telehealth providers to emphasize the risks and concerns about the use of technologies, such as the Meta/Facebook pixel and Google Analytics, that can track a user's online activities. The letter explained that these tracking technologies gather identifiable information about users, usually without their knowledge and in ways that are hard for users to avoid, as users interact with a website or mobile app. Tracking technologies are used to collect and analyze information about how users interact with websites or mobile apps. Generally, tracking technologies developed by third parties send information directly to the third parties who developed such technologies and may continue to track users and gather information about them even after they navigate away from the original website to other websites. The letter reminded recipients that HIPAA-regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to third parties or any other violations of the HIPAA Rules.
- In August 2023, OCR and the Office of the National Coordinator for Health Information Technology (ONC) updated the Security Risk Assessment (SRA)Tool, and in September, provided two webinars to teach regulated entities how to use the SRA Tool. The SRA Tool is designed to aid small and medium-sized health care organizations in their efforts to assess security risks. The 2023 version of the SRA Tool contained a variety of feature enhancements based on user feedback and public input. New features included a Remediation Report, glossary, and updated references to Health Industry Cybersecurity Practices (HICP) for 2023.

- In October 2023, OCR published a cybersecurity newsletter issued via OCR's listserv and available on OCR's website on How Sanction Policies Can Support HIPAA Compliance. The newsletter reminds regulated entities that sanction policies are specifically required by both the Privacy Rule and the Security Rule and discusses how sanction policies can strengthen compliance with HIPAA Rules. In particular, OCR explained that imposing consequences on workforce members who violate a regulated entity's policies or the HIPAA Rules can be effective in creating a culture of HIPAA compliance and improved cybersecurity because of the knowledge that there is a negative consequence to noncompliance, which enhances the likelihood of compliance.
- In October 2023, OCR issued two resource documents to promote cybersecurity in telehealth. The first, "Educating Patients about Privacy and Security Risks to Protected Health Information when Using Remote Communication Technologies for Telehealth," is tailored for health care providers. This resource can be used by health care providers to explain to patients, in plain language, the health information privacy and security risks that are present when using remote communication technologies such as video conferencing websites and applications ("apps") for telehealth. The information in this resource expands on the Department's existing resources for health care providers on preparing patients for telehealth with a focus on privacy and security. The second telehealth resource, "Telehealth Privacy and Security Tips for Patients" is tailored for patients. It provides real-life tips for the public about protecting and securing their health information when accessing telehealth.
- In October 2023, OCR released two videos, in English and Spanish, on the HIPAA Security Rule and how it can help regulated entities defend against cyber-attacks. The videos discuss real-world cyber-attack trends, based on OCR's experience with its breach reports and enforcement, along with ways to detect and mitigate common cyber-attacks.
- In October 2023, OCR hosted a webinar titled "The HIPAA Security Rule Risk Analysis Requirement" for an audience of over 4,000 registrants. A risk analysis is a key and necessary step for effective cybersecurity and HIPAA Security Rule compliance. This webinar discussed what is required to conduct an accurate and thorough risk assessment to protected health information.

Audits

OCR did not initiate any audits in 2023 due to a lack of financial resources.

Appendix

Resolution Agreements and Civil Money Penalties[15] in 2023

Resolution Agreement with David Mente, MA, LPC

David Mente, MA, LPC, paid $15,000 and agreed to take corrective actions to settle potential violations of the HIPAA Privacy Rule. David Mente is a healthcare provider providing psychological care in Pittsburgh, Pennsylvania.

In December 2017, OCR received a complaint filed against David Mente alleging that he failed to provide an individual with access to his minor child's PHI. OCR provided David Mente with technical assistance regarding the individual's right of access to PHI and closed the complaint. On May 2, 2018, OCR received a second complaint concerning David Mente's continued noncompliance with the requirements of the Privacy Rule concerning access. OCR's investigation determined that David Mente'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, David Mente provided access to all of the requested records.

In addition to the monetary settlement, David Mente agreed to:

- Review and revise, as necessary, its written policies and procedures related to access to PHI as required by the Privacy Rule; and
- Train workforce members on the Privacy Rule requirements concerning the individual's right of access to PHI.

This settlement occurred in January 2023. The resolution agreement is available at the following link:
www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/mente-ra-cap/index.html

Resolution Agreement with MedEvolve

MedEvolve paid $350,000 and agreed to take corrective actions to settle potential violations of the HIPAA Privacy and Security Rules. MedEvolve is a business associate that provides practice management, revenue cycle management, and practice analytics software services to health care entities.

OCR began investigating MedEvolve after it filed a breach report in July 2018, stating that due to a misconfiguration of its server, the PHI of 230,572 individuals was left unsecured and accessible on the Internet. The potential HIPAA violations in this case included the impermissible disclosure of PHI of 230,572 individuals; a failure to conduct an accurate and thorough risk analysis to determine risk and vulnerabilities to its information systems; and a failure to enter into a business associate agreement with a subcontractor.

[15] 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 2023.

In addition to the monetary settlement, MedEvolve agreed to:

- Conduct an accurate and thorough risk analysis;
- Develop a 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 Privacy and Security 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 March 2023. The resolution agreement is available at the following link:
www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/medevolve-ra-cap/index.html

Resolution Agreement with Manasa Health Center

Manasa Health Center (Manasa) paid $30,000 and agreed to take corrective actions to settle a potential violation of the HIPAA Privacy Rule. Manasa is a medical practice located in Kendall Park, New Jersey, and provides adult and child psychiatric care.

In November 2020, OCR received a complaint alleging that Manasa disclosed the PHI of four individuals in response to negative online reviews posted on Google Reviews. OCR's investigation determined that the potential HIPAA violations, in this case, included the impermissible disclosure of PHI of four individuals, and a failure to implement privacy policies and procedures.

In addition to the monetary settlement, Manasa 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 for the privacy and security of PHI; and
- Issue breach notices to all individuals, or the individuals' personal representatives, whose PHI was disclosed by the covered entity on Google Reviews or any other internet platform without a valid authorization.

This settlement occurred in March 2023. The resolution agreement is available at the following link:
www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/manasa-ra-cap/index.html

Resolution Agreement with iHealth Solutions

iHealth Solutions (iHealth) paid $75,000 and agreed to take corrective actions to settle potential violations of the HIPAA Privacy and Security Rules. iHealth is a business associate based in Kentucky that provides medical coding, billing, and information technology services to health care providers.

OCR began investigating iHealth after it filed a breach report in August 2017, stating that the PHI of 267 individuals was accessible over the Internet due to an unsecured server. OCR's investigation determined that the potential HIPAA violations in this case included a failure to conduct an accurate and thorough risk analysis to determine risk and vulnerabilities to its information systems and a failure to develop a risk management plan.

In addition to the monetary settlement, iHealth agreed to:

- Conduct an accurate and thorough risk analysis;
- Develop a risk management plan to address and mitigate security risks and vulnerabilities found in the risk analysis;
- Implement a process for evaluating environmental and operational changes;
- Develop, maintain, and revise, as necessary, its written policies and procedures to comply with the HIPAA Privacy and Security Rules; and
- Distribute policies and procedures to workforce members.

This settlement occurred in April 2023. The resolution agreement is available at the following link:
www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/ihealth-ra-cap/index.html

Resolution Agreement with Yakima Valley Memorial Hospital

Yakima Valley Memorial Hospital (Yakima) paid $240,000 and agreed to take corrective actions to settle a potential violation of the HIPAA Security Rule. Yakima is a community hospital located in central Washington.

OCR began investigating Yakima in May 2018 after it filed a breach report stating that an employee impermissibly accessed the PHI of 415 individuals. OCR's investigation found a potential violation of the HIPAA Security Rule's requirement to implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of the Security Rule.

In addition to the monetary settlement, Yakima agreed to:

- Conduct an accurate and thorough risk analysis;
- Develop a 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;
- Train workforce members on the policies and procedures for the privacy and security of PHI; and
- Provide OCR with an accounting of all business associates and copies of all business associate agreements.

This settlement occurred in May 2023. The resolution agreement is available at the following link:
www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/yakima-ra-cap/index.html

Resolution Agreement with UnitedHealthcare Insurance Company

UnitedHealthcare Insurance Company (UHIC) paid $80,000 and agreed to take corrective actions to settle a potential violation of the HIPAA Privacy Rule's right of access standard. UHIC is a health insurer that provides insurance coverage to millions of individuals across the United States.

In March 2021, OCR received a complaint alleging that UHIC did not respond to the complainant's request for a copy of their medical record. OCR's investigation found a potential violation of the HIPAA Privacy Rule's timely access to PHI requirement.

In addition to the monetary settlement, UHIC agreed to:

- Review and revise, as necessary, its written policies and procedures related to access to PHI as required by the Privacy Rule;
- Distribute policies and procedures to workforce members;
- Train workforce members on the Privacy Rule requirements concerning the individual's right of access to PHI; and
- Provide OCR with a list of written requests for access to PHI received by UHIC and any documentation related to requests for PHI that were denied by UHIC.

This settlement occurred in August 2023. The resolution agreement is available at the following link:
www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/uhc-ra-cap/index.html.

Resolution Agreement with LA Care Health Plan

LA Care Health Plan (LACHP) paid $1,300,000 and agreed to take corrective actions to settle potential violations of the HIPAA Privacy and Security Rules. LACHP is the nation's largest publicly operated health plan.

In January 2016, OCR opened a compliance review of LACHP based on online media reports that patients were able to view the PHI of other members via its online payment portal. In addition, in March 2019, OCR received a breach report from LACHP stating that, due to a mailing error, some members received the member identification cards of other members. OCR's investigation found that the potential violations of the HIPAA Privacy and Security Rules included the impermissible diNana Habib <nhabib@securefiledrive.net>sclosure of the PHI of 1,498 individuals; a failure to conduct an accurate and thorough risk analysis; a failure to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level; a failure to implement sufficient procedures to regularly review records of information system activity; a failure to perform a periodic technical and nontechnical evaluation; and a failure to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.

In addition to the monetary settlement, LACHP agreed to:

- Conduct an accurate and thorough risk analysis;
- Develop a risk management plan to address and mitigate security risks and vulnerabilities found in the risk analysis;

- Submit a report to OCR detailing any environmental or operational changes materially affecting the security of its ePHI during the course of the compliance term;
- Develop, maintain, and revise, as necessary, its written policies and procedures to comply with the HIPAA Privacy and Security 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 August 2023. The resolution agreement is available at the following link:
www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/la-care-health-plan/index.html

Resolution Agreement with Saint Joseph's Medical Center

Saint Joseph's Medical Center (SJMC) paid $80,000 and agreed to take corrective actions to settle a potential violation of the HIPAA Privacy Rule. SJMC is an academic medical center offering a full range of medical services in New York.

OCR opened an investigation in April 2020 after the Associated Press published an article about the medical center's response to the COVID-19 public health emergency, which included photographs and information about the facility's patients. SJMC allowed the reporter access to the patients and their clinical information. OCR's investigation found that SJMC potentially impermissibly disclosed the PHI of three individuals. In addition to the monetary settlement, SJMC 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 all workforce members on the policies and procedures for the privacy and security of PHI.

This settlement occurred in August 2023. The resolution agreement is available at the following link:
www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/sjmc-ra-cap/index.html

Resolution Agreement with Doctors' Management Services

Doctors' Management Services (DMS) paid $100,000 and agreed to take corrective actions to settle potential violations of the HIPAA Privacy and Security Rules. DMS is a medical management company based in Massachusetts that provides billing and payor credentialing to several covered entities.

In April 2019, OCR initiated an investigation after receiving a breach report from DMS stating that it experienced a ransomware attack that compromised the PHI of 206,695 individuals. OCR's investigation found that the potential violations of the HIPAA Privacy and Security Rules included the impermissible disclosure of the PHI of 206,695 individuals; a failure to conduct an accurate and thorough risk analysis that assessed technical, physical, and environmental risks and vulnerabilities associated with handling ePHI; a failure to implement procedures to regularly

review records of information system activity, such as audit logs, access reports, and security incident tracking reports; and a failure to implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of the Security Rule.

In addition to the monetary settlement, DMS agreed to:

- Review and update its risk analysis;
- Update its risk management plan to address and mitigate security risks and vulnerabilities found in the updated risk analysis;
- Develop, maintain, and revise, as necessary, its written policies and procedures to comply with the HIPAA Security Rule;
- 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 September 2023. The resolution agreement is available at the following link:
www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/dms-ra-cap/index.html

Resolution Agreement with Phoenix Healthcare LLC dba Green Country Care Center

Phoenix Healthcare LLC dba Green Country Care Center (GCCC) paid $35,000 and agreed to take corrective actions to settle a potential violation of the HIPAA Privacy Rule. GCCC is a skilled nursing facility located in Tulsa, Oklahoma.

In April 2019, OCR received a complaint alleging that GCCC would not provide the complainant with a copy of her mother's medical records unless it received a fee, which the complainant felt was unreasonable. OCR's investigation found that GCCC assessed fees for medical records which were not reasonable or cost-based and did not have a business associate agreement in place with its legal counsel. The monetary settlement was reached after GCCC requested a hearing from an administrative law judge (ALJ) after contesting OCR's proposed civil money penalty. In February 2023, the ALJ ruled in favor of OCR and upheld the violations cited by OCR in regard to the HIPAA Privacy Rule. GCCC then appealed the decision and the Departmental Appeals Board also ruled in favor of OCR. OCR and GCCC subsequently settled this investigation.

In addition to the monetary settlement, GCCC agreed to:

- Revise right of access policies and procedures to comply with the HIPAA Privacy Rule; and
- Train workforce members on the policies and procedures and HIPAA's right of access provisions.

This settlement occurred in September 2023. The resolution agreement is available at the following link:
www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/phoenix-healthcare/index.html

Resolution Agreement with Green Ridge Behavioral Health

Green Ridge Behavioral Health (GRBH) paid $40,000 and agreed to take corrective actions to settle potential violations of the HIPAA Privacy and Security Rules. GRBH is a multidisciplinary group practice that provides comprehensive outpatient mental health services in Washington, D.C.

In December 2019, OCR initiated an investigation after receiving a breach report from GRBH stating that it experienced a ransomware attack that compromised the PHI of approximately 14,000 individuals. OCR's investigation found that the potential violations of the HIPAA Privacy and Security Rules included the failure to conduct an accurate and thorough risk analysis of the potential risks and vulnerabilities to the confidentiality, integrity and availability of its ePHI; the failure to implement security measures sufficient to reduce risks and vulnerabilities to ePHI to a reasonable and appropriate level; the failure to implement policies and procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports; and a failure to not use or disclose protected health information except as permitted by the Privacy Rule.

In addition to the monetary settlement, GRBH agreed to:

- Conduct an accurate and thorough risk analysis;
- Develop a risk management plan to address and mitigate security risks and vulnerabilities found in the risk analysis;
- Review, and as necessary, develop or revise certain written policies and procedures to comply with the HIPAA Privacy and Security Rules;
- Distribute these policies and procedures to workforce members;
- Train workforce members on the policies and procedures for the privacy and security of PHI; and
- Review all relationships with vendors and third-party service providers to identify business associates and provide HHS with an accounting of GRBH's business associates and provide copies of the business associate agreements that GRBH maintains with each business associate.

This settlement occurred in October 2023. The resolution agreement is available at the following link:
www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/green-ridge-behavioral-health-ra-cap/index.html

Resolution Agreement with Lafourche Medical Group

Lafourche Medical Group (LMG) paid $480,000 and agreed to take corrective actions to settle potential violations of the HIPAA Security Rule. LMG is a group practice providing medical services in Louisiana.

In May 2021, OCR received a breach report filed by LMG stating that one of its owners was the subject of an email phishing attack. LMG could not determine the exact number of individuals affected, so, in its mitigation efforts, it provided a breach notice to all of its 34,862 patients. OCR's investigation found that the potential violations of the HIPAA Security Rule included a

failure to conduct an accurate and thorough risk analysis of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of its ePHI; and a failure to implement procedures to regularly review records of information system activity.

In addition to the monetary settlement, LMG agreed to:

- Conduct an accurate and thorough risk analysis;
- Develop a 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 Privacy and Security Rules;
- Distribute policies and procedures to workforce members; and
- Train workforce members on its policies and procedures for the privacy and security of PHI.

This settlement occurred in November 2023. The resolution agreement is available at the following link:
www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/lafourche-medical-group/index.html

Resolution Agreement with Optum Medical Care of New Jersey

Optum Medical Care of New Jersey (Optum) paid $160,000 and agreed to take corrective actions to settle potential violations of the HIPAA Privacy Rule's right of access standard. Optum is a private multi-specialty physician group with approximately 150 locations serving patients throughout New Jersey and Southern Connecticut.

Between October and November of 2021, OCR received six complaints from individual complainants alleging that Optum refused to provide copies of either the complainant's medical records or the complainant's minor children's medical records. OCR's investigation found a potential violation of the HIPAA Privacy Rule's requirement to provide timely access to PHI.

In addition to the monetary settlement, Optum agreed to:

- Review and to the extent necessary, revise its right of access 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; and
- Submit a report with a monthly count of all requests for access to PHI every 90 days in which the corrective action plan is in effect.

This settlement occurred in November 2023. The resolution agreement is available at the following link:
www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/optum-medical-care.html

Resolution Agreement with Montefiore Medical Center

Montefiore Medical Center (MMC) paid $4,750,000 and agreed to take corrective actions to settle potential violations of the HIPAA Security Rule. MMC is a not-for-profit academic medical center located in the Bronx borough of New York.

In July 2015, OCR received a breach report from MMC alleging that one of its employees inappropriately accessed the PHI of 12,517 individuals and sold this information to an identity theft ring. OCR's investigation found that the potential violations of the HIPAA Security Rule included a failure to conduct an accurate and thorough risk analysis of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of its ePHI; a failure to implement procedures to regularly review records of information system activity; and a failure to implement hardware, software, and/or procedural mechanisms that record and examine activity in all information systems that contain ePHI.

In addition to the monetary settlement, MMC agreed to:

- Conduct an accurate and thorough risk analysis;
- Develop a risk management plan to address and mitigate security risks and vulnerabilities found in the risk analysis;
- Implement audit controls using hardware, software, or procedural mechanisms that record and examine activity in all information systems that contain or use PHI;
- Review, and to the extent necessary, revise its written policies and procedures to comply with the HIPAA Privacy and Security 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 November 2023. The resolution agreement is available at the following link:
www.hhs.gov/hipaa/for-professionals/complianceenforcement/agreements/montiefore/index.html