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

For Calendar Year 2024

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 2024 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 30,256 new complaints and carried over 2,955 complaints from previous years alleging violations of the HIPAA Privacy, Security, and Breach Notification Rules (HIPAA Rules). OCR resolved 28,228 complaints. OCR resolved nine complaint investigations with Resolution Agreements and Corrective Action Plans (RA/CAPs) and monetary settlements, or civil money penalties totaling $1,180,781.

OCR initiated 730 compliance reviews and completed 797 compliance reviews. Thirteen compliance reviews were resolved with RA/CAPs and monetary settlements or civil money penalties totaling $8,763,831. OCR issued no subpoenas, and no audits were initiated.

OCR engaged in 89 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. There were approximately 10.6 million visits to OCR's HIPAA webpages.

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 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 CFR Part 160 and Subparts A and E of Part 164, provides important federal protections for 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 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 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

[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.

[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 USC 1232g; (ii) In records described at 20 USC 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 CFR 160.103.

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;
- 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 2024.

This report is prepared for the calendar year 2024. The Reports to Congress on Compliance with the HIPAA Privacy and Security Rules for previous years are available at https://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 authority to issue subpoenas to compel cooperation with an investigation.

[3] A separate Report to Congress, available at http://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.

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, 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 activity that would not violate the HIPAA Rules, or is untimely, OCR closes the case. Where the case is eligible 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

[5] *See also* 45 CFR 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.
[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 CFR 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.

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 suggest 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, it may collect evidence through interviews, witness 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 USC 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 to resolve the potential HIPAA violation(s). In most 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

[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.

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 compliance issues 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.

OCR's HIPAA Audit Program is an important part of OCR's overall health information privacy, security, and breach notification compliance activities. OCR uses the audit program to assess the HIPAA compliance efforts of a range of entities covered by the HIPAA regulations. The audits present an opportunity to examine mechanisms for compliance, identify best practices, discover risks and vulnerabilities that may not have come to light through OCR's ongoing complaint investigations and compliance reviews, and enable us to get out in front of problems before they result in breaches. OCR will broadly identify best practices gleaned through the audit process and will provide guidance targeted to identified compliance challenges.

OCR did not initiate any audits in 2024 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 2024, OCR resolved 22 investigations

with RA/CAPs or the imposition of CMPs totaling $9,944,612.

As shown in the table below, between 2020 and 2024, the number of complaints received by OCR increased 11%, and the number of compliance reviews initiated by OCR increased by 7%.

Year	Complaints Received	Compliance Reviews (including reported breaches) Initiated	% Change in Complaints Received Year over Year	% Change in Compliance Reviews Initiated year over year
2024	30,256	797	2% decrease	3% increase
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
2020 to 2024	-	-	11% increase	7% increase

Source: Current and previous Reports to Congress

Enforcement Data

Complaint Resolutions

2024 Complaints

During calendar year 2024, OCR received 30,256 new HIPAA complaints and carried over 2,955 open complaints from 2023. OCR resolved 28,228 complaints during calendar year 2024.[8] Of those, OCR resolved 17,466 (62%) before initiating an investigation. Examples of pre-investigation closures include complaints that alleged violations by an entity not covered by

[8] 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.

the HIPAA Rules and allegations involving conduct that did not violate the HIPAA Rules or that were untimely. OCR resolved 9,392 complaints (33%) by providing technical assistance in lieu of an investigation. See Figure 1.

OCR completed 1,370 complaint investigations.[9] In 663 of these investigations (48%), OCR required the covered entity or business associate to take corrective action. In 704 of the complaints investigated (51%), OCR found insufficient evidence that a violation of the HIPAA Rules had occurred. In three of these investigations, OCR provided technical assistance after initiating an investigation (<1%). See Figure 2.

HHS OFFICE FOR CIVIL RIGHTS

COMPLAINT RESOLUTIONS AND INVESTIGATIONS

NUMBER OF CASES CLOSED AND TYPE OF CLOSURES

JANUARY 1, 2024, THROUGH DECEMBER 31, 2024

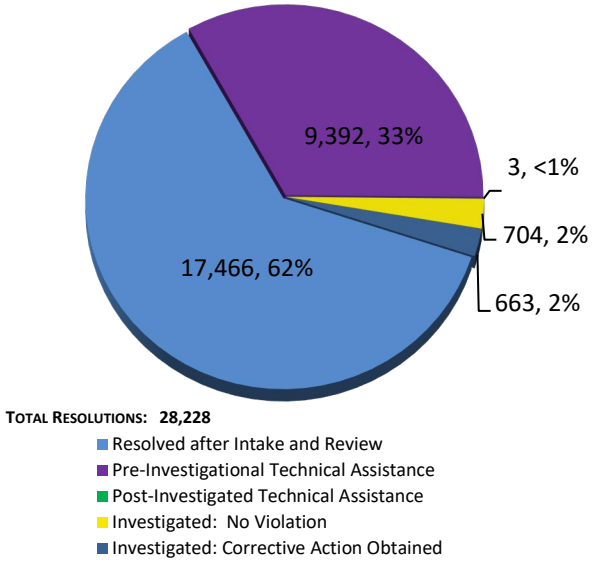

Figure 1

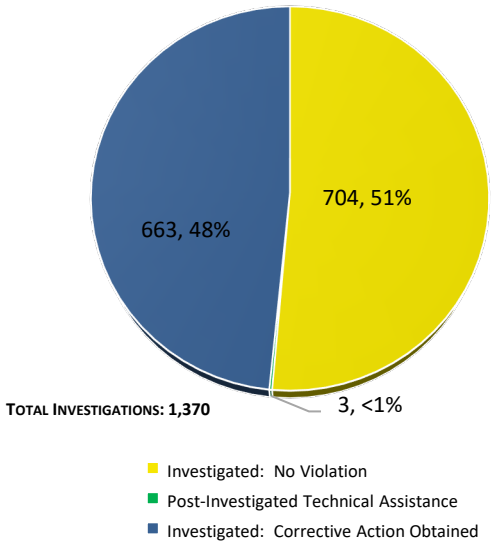

Figure 2

OCR resolved nine complaint investigations in 2024 with resolution agreements and/or CAPs and monetary settlements totaling $1,180,781.

For the 28,228 complaints that OCR resolved in 2024, the top five issues alleged were Impermissible Uses and Disclosures (660 complaints), Right of Access (541 complaints), General Safeguards (481 complaints), Administrative Safeguards (Security Rule) (147 complaints), and Breach-Notice to Individuals (122 complaints).

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

Compliance Reviews

2024 Compliance Reviews

During calendar year 2024, OCR initiated 730 compliance reviews to investigate allegations of violations of the HIPAA Rules that did not arise from complaints.[10] Of these, 663 compliance reviews were initiated because of a breach report of unsecured PHI affecting 500 or more individuals and two were a result of a breach report affecting fewer than 500 individuals. The remaining 65 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 797 compliance reviews in 2024. Most of these cases were resolved following an investigation with the regulated entity taking corrective actions to come into compliance during the investigation, agreeing to a settlement with a corrective action plan, or the imposition of a CMP.[11] Of the closed cases, 785 originated from breach reports and 12 originated from other means. The covered entity or business associate took corrective action in 670 cases (84%). OCR provided the covered entity or business associate with technical assistance after investigation in 63 cases (8%). OCR found that there was insufficient evidence of a violation of the HIPAA Rules in 44 cases (6%), and OCR determined that it did not have jurisdiction to investigate the allegations in 20 cases (3%). Of the completed compliance reviews, 13 cases were resolved with resolution agreements, CAPs and monetary settlements totaling $8,763,831. See Figure 3.

[10] In 2024, compliance reviews were opened for all reports of breaches affecting 500 or more individuals, and for some reports of breaches affecting fewer than 500 individuals.

[11] 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.

HHS OFFICE FOR CIVIL RIGHTS

COMPLIANCE REVIEWS

NUMBER OF CASES CLOSED AND TYPES OF CLOSURES

JANUARY 1, 2024 – DECEMBER 31, 2024

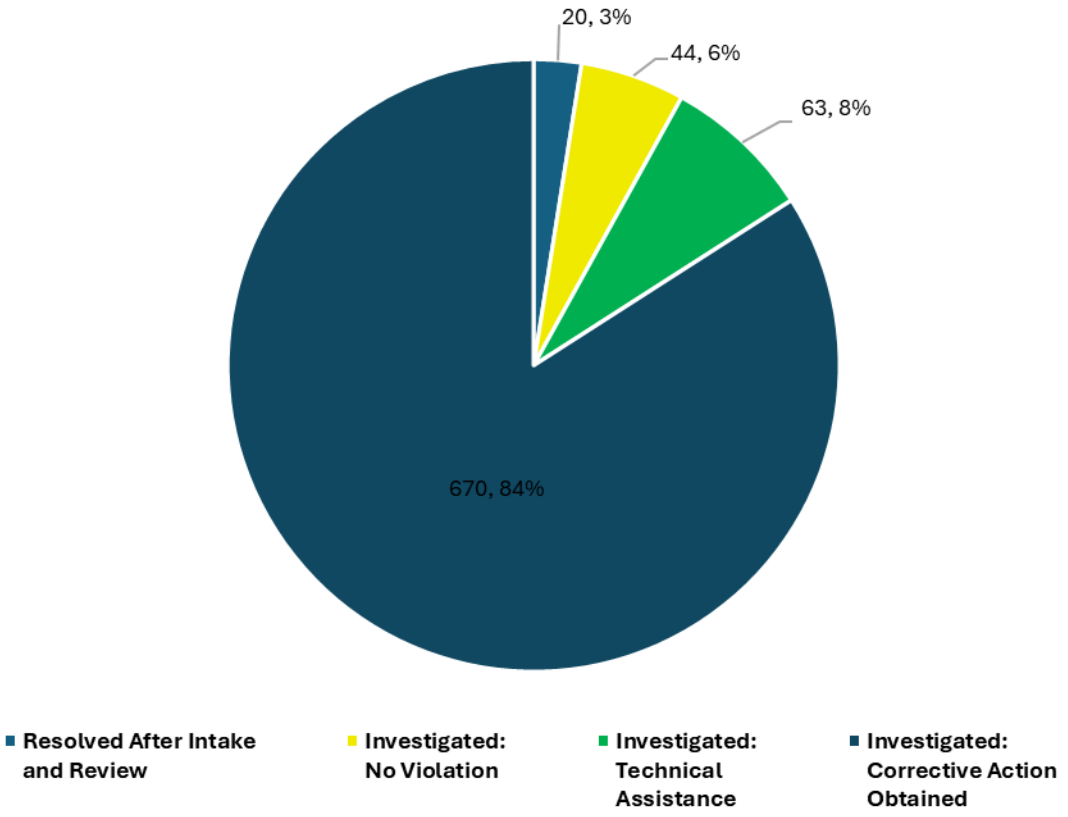

Figure 3

Subpoenas

OCR did not issue any subpoenas in 2024.

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 were identified by OCR investigations. OCR's outreach highlights include:

- OCR conducted 89 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 February 2024, OCR and the National Institute of Standards and Technology (NIST) announced the publication of the final version of Special Publication (SP) 800-66 Revision 2, Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide. This revised publication, a collaborative effort between NIST and OCR, includes resources for HIPAA covered entities (most health care providers, health plans and health care clearinghouses) and their business associates to help their understanding of the HIPAA Security Rule, drive compliance with the law, and bolster security.
- In March 2024, following the cyberattack on Change Healthcare, OCR published a "Dear Colleague Letter" announcing OCR's investigation into this incident, and identifying available cybersecurity resources published by HHS and OCR including HIPAA Security Rule guidance and newsletters, videos on how the HIPAA Security Rule protects against cyberattacks, the HIPAA Security Rule Risk Analysis requirement, the HHS Security Risk Assessment Tool, a Ransomware and HIPAA Factsheet, and the Healthcare and Public Health Cybersecurity Performance Goals.
- In April 2024, OCR posted a new webpage to share answers to frequently asked questions (FAQs) concerning the HIPAA Rules and the cybersecurity incident impacting Change Healthcare. The webpage answers questions and provides helpful information on many topics, including:
    - Why did OCR issue the March 13, 2024, "Dear Colleague Letter"?
    - Why is OCR initiating an investigation and what does it cover?
    - Has OCR received breach reports from Change Healthcare, UHG, or any affected health care providers?
    - Are large breaches (those affecting 500 or more individuals) posted on the HHS Breach Portal on the same day that OCR receives a regulated entity's breach report?
    - Is OCR's 2016 ransomware guidance applicable to the Change Healthcare cyberattack?
    - Are covered entities that are affected by the cyberattack involving Change Healthcare and UHG required to file breach notifications?

- What HIPAA breach notification duties do covered entities have with respect to the Change Healthcare cyberattack?
- What HIPAA breach notification duties do business associates have with respect to the Change Healthcare cyberattack?

- In April 2024, OCR published a final rule on the HIPAA Privacy Rule to Support Reproductive Health Care Privacy. The final rule modified 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 2024, OCR held a webinar explaining the changes to the HIPAA Privacy Rule following the publication of the final rule on the HIPAA Privacy Rule to Support Reproductive Health Care Privacy.

- In August 2024, OCR published a cybersecurity newsletter issued via OCR's listserv and available on OCR's website on HIPAA Security Rule Facility Access Controls that details what facility access controls are and how to implement them. The Facility Access Controls standard of the HIPAA Security Rule requires that regulated entities implement policies and procedures to limit physical access to [their] electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed. The four HIPAA Security Rule implementation plan guidelines, which are discussed in detail are contingency operations, facility security plans, access control and validation procedures, and maintenance records.

- In September 2024, OCR held two webinars on the HHS Security Risk Assessment Tool, 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. Updates include new content on mitigating organizational threats and vulnerabilities including supply chain risks, references to the Healthcare and Public Health (HPH) Cybersecurity Performance Goals (CPGs), and updated references to the latest version of the NIST Cybersecurity Framework (version 2.0).

- In October 2024, OCR published a cybersecurity newsletter issued via OCR's listserv and available on OCR's website on Social Engineering: Searching for Your Weakest Link which details types of social engineering designed to engage individuals into taking certain actions or revealing information that could put them or their organization at risk. This newsletter discusses common social engineering threats and how individuals and HIPAA regulated entities can defend against them.

- In October 2024, OCR and the NIST Information Technology Laboratory held a two-day cybersecurity conference where federal regulators including, HHS, OCR, Federal Trade Commission, Food and Drug Administration, Veterans Health Administration, Assistant Secretary for Technology Policy, and the Administration for Strategic Preparedness and

Response spoke on cybersecurity regulations, guidance, best practices, trends, resources and new threats and risks to electronic health information.

- In October 2024, OCR published a cybersecurity video on ransomware that provided updates to the health care industry on the ransomware trends OCR sees in its cybersecurity investigations, OCR guidance and resources, best practices and practical advice on how HIPAA compliance can help HIPAA regulated entities prevent, detect, respond to, and recover from ransomware attacks.

- In December 2024, OCR issued a Notice of Proposed Rulemaking (NPRM) to update the HIPAA Security Rule, aiming to strengthen cybersecurity for ePHI. The NPRM, published in the Federal Register on January 6, 2025, proposes significant changes, including new standards for risk analysis, multi-factor authentication, incident response plans, and requires entities to deploy anti-malware protections.

Audits

OCR did not initiate any audits in 2024 due to a lack of financial resources.

Appendix

Resolution Agreements and Civil Money Penalties[12] in 2024

Civil Money Penalty (CMP) imposed on Essex Residential Care dba Hackensack Meridian Health, West Caldwell Care Center

OCR imposed a civil money penalty of $100,000 against Essex Residential Care dba Hackensack Meridian Health, West Caldwell Care Center (WCCC). WCCC is a residential care facility serving patients in New Jersey.

In May 2020, OCR received a complaint filed against WCCC alleging that the facility failed to provide the complainant with a copy of his mother's medical records. Previously, on April 22, 2020, WCCC notified the complainant via email that his April 2020 request for his mother's medical records was denied until it received a copy of his power of attorney, medical proxy, or similar document executed by the mother establishing that he was her personal representative.

On April 23, 2020, the complainant provided a power of attorney; however, the requested medical records were not provided until December 1, 2020. OCR's investigation determined that WCCC's failure to provide timely access to the requested records was a potential violation of the HIPAA right of access standard.

Upon the conclusion of the investigation, OCR notified WCCC of OCR's findings. When the investigation was not resolved with a resolution agreement and corrective action plan, OCR issued a Notice of Proposed Determination. In January 2024, OCR issued a Notice of Final Determination and imposed a civil money penalty in the amount of $100,000.

Civil Money Penalty imposed on American Medical Response

OCR imposed a civil money penalty of $115,200 against American Medical Response (AMR). AMR is a private ambulance company doing business in multiple states.

In July 2019, OCR received a complaint filed against AMR alleging that the company failed to provide the complainant with a copy of her medical and billing records after multiple access requests. The complainant initially contacted AMR in October 2018; AMR did not respond to the request until 121 days later requiring payment prior to providing the requested records. The requested records were finally provided to the complainant in November 2019, well over a year

[12] Information provided here on Resolution Agreements and CMPs is based on the year in which the Agreement was signed, or the CMP assessed. Investigations of these cases were initiated in years prior to 2024.

after the initial request.

Upon the conclusion of the investigation, OCR notified AMR of OCR's findings. When the investigation was not resolved with a resolution agreement and corrective action plan, OCR issued a Notice of Proposed Determination in October 2023. In January 2024, OCR issued a Notice of Final Determination and imposed a civil money penalty in the amount of $115,200.

Resolution Agreement with Heritage Valley Health System

Heritage Valley Health System (HVHS) paid $950,000 and agreed to take corrective actions to settle potential violations of the HIPAA Security Rule. HVHS is an integrated delivery network providing comprehensive health care for residents of Allegheny, Beaver, Butler and Lawrence counties, in Pennsylvania, eastern Ohio, and the panhandle of West Virginia.

In October 2017, OCR opened a compliance review of HVHS based on media reports stating that HVHS experienced a data security incident. OCR's investigation found that the potential violations of the HIPAA Security Rule including the failure to conduct a compliant risk analysis, the failure to implement a contingency plan to respond to emergencies, like a ransomware attack, that damage systems that contain ePHI, and the failure to implement policies and procedures to allow only authorized users access to ePHI.

This settlement occurred in February 2024. In addition to the monetary settlement, HVHS agreed to:

- Conduct an accurate and thorough risk analysis to determine the potential risks and vulnerabilities to the confidentiality, integrity, and availability of its ePHI;
- 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.

Resolution Agreement with Plastic Surgery Associates of South Dakota

Plastic Surgery Associates of South Dakota (PSA) paid $500,000 and agreed to take corrective actions to settle potential violations of the HIPAA Security Rule. OCR initiated an investigation following the receipt of a breach report filed in July 2017, which reported that it discovered that nine workstations and two servers were infected with ransomware, affecting the PHI of 10,229 individuals.

OCR's investigation revealed multiple potential violations of the HIPAA Security Rule, including failures to conduct a compliant risk analysis to determine the potential risks and vulnerabilities to

PHI in its systems; implement security measures sufficient to reduce the risks and vulnerabilities to PHI to a reasonable and appropriate level; implement procedures to regularly review records of information system activity; and implement policies and procedures to address security incidents.

This settlement occurred in May 2024. In addition to the monetary settlement, PSA agreed to:

- Conduct an accurate and thorough risk analysis to determine the potential risks and vulnerabilities to the confidentiality, integrity, and availability of its ePHI;
- 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.

Resolution Agreement with Cascade Eye and Skin Centers

Cascade Eye and Skin Centers (Cascade) paid $2,500,000 and agreed to take corrective actions to settle a potential violation of the HIPAA Security Rule. Cascade is a privately-owned health care provider located in the state of Washington.

In May 2017, OCR received a complaint alleging that Cascade had experienced a ransomware attack of its computer systems that compromised the PHI of 291,000 individuals. OCR launched an investigation and found multiple potential violations of the HIPAA Security Rule, including failures by Cascade to conduct a compliant risk analysis to determine the potential risks and vulnerabilities to PHI in its systems, and to have sufficient monitoring of its health information systems' activity to protect against a cyber-attack.

This settlement occurred in June 2024. In addition to the monetary settlement, Cascade agreed to:

- Conduct an accurate and thorough risk analysis to determine the potential risks and vulnerabilities to the confidentiality, integrity, and availability of its ePHI;
- Develop a risk management plan to address and mitigate security risks and vulnerabilities identified in the risk analysis;
- Develop a written process to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports;
- Develop, maintain, and revise, as necessary, written policies and procedures to comply with the HIPAA Rules; and
- Distribute policies and procedures to workforce members.

Civil Money Penalty imposed on Providence Medical Institute

OCR imposed a civil money penalty of $240,000 against Providence Medical Institute (PMI). PMI is a non-profit physician services organization with 200 providers across 32 medical offices, including seven urgent care centers throughout California.

OCR initiated an investigation following the receipt of a breach report filed by PMI in April 2018, which reported that its systems were impacted by a series of ransomware attacks that affected the ePHI of 85,000 individuals between February and March 2018. OCR's investigation determined that servers containing ePHI were encrypted with ransomware three times. OCR found two potential violations of the HIPAA Security Rule, including failure to have a business associate agreement in place and failure to implement policies and procedures to allow only authorized persons or software programs access to ePHI.

In March 2024, OCR issued a Notice of Proposed Determination seeking to impose a civil money penalty. Providence Medical Institute waived its right to a hearing and did not contest OCR's findings. Accordingly, in July 2024, OCR issued a Notice of Final Determination and imposed a civil money penalty of $240,000.

Resolution Agreement with Bryan County Ambulance Authority

Bryan County Ambulance Authority (BCAA) paid $90,000 and agreed to take corrective actions to settle a potential violation of the HIPAA Security Rule. BCAA provides emergency medical services in Oklahoma.

OCR began investigating BCAA in May 2022 after it filed a breach report stating that it experienced a ransomware attack that encrypted its network and compromised the PHI of 14,273 individuals. OCR's investigation found that BCAA had failed to conduct a compliant risk analysis to determine the potential risks and vulnerabilities to ePHI in BCAA's systems.

This settlement occurred in July 2024. In addition to the monetary settlement, BCAA agreed to:

- Conduct an accurate and thorough risk analysis to determine the potential risks and vulnerabilities to the confidentiality, integrity, and availability of its ePHI;
- 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; and
- Train workforce members on the policies and procedures for the privacy and security of PHI.

Civil Money Penalty imposed on Rio Hondo Community Mental Health Center

OCR imposed a civil money penalty of $100,000 against Rio Hondo Community Mental Health Center (Rio Hondo). Rio Hondo is a mental health center located in Cerritos, California.

OCR launched an investigation after receiving a complaint from a patient that they were not given timely access to their medical records, despite multiple requests in writing and by telephone. OCR's investigation found that it took nearly seven months from the time the patient first requested the records until Rio Hondo provided them. The patient made multiple telephone calls in July and August 2020 regarding the status of her request but still did not receive the requested records.

OCR found that Rio Hondo failed to take timely action in response to the patient's right of access in accordance with the HIPAA Privacy Rule. In July 2024, OCR issued a Notice of Proposed Determination to impose a $100,000 civil monetary penalty. Rio Hondo waived its right to a hearing and did not contest the findings of OCR's Notice of Proposed Determination. Accordingly, in August 2024, OCR issued a Notice of Final Determination and imposed a civil money penalty of $100,000.

Resolution Agreement with Inmediata Health Group

Inmediata Health Group (Inmediata) paid $250,000 and agreed to take corrective actions to settle potential violations of the HIPAA Security Rule. Inmediata is a health care clearinghouse located in San Juan, Puerto Rico.

In November 2018, OCR received a complaint concerning PHI left unsecured on the internet. Following the initiation of OCR's investigation, Inmediata provided breach notification to HHS and affected individuals. OCR's investigation determined that from May 2016 through January 2019, the PHI of 1,565,338 individuals was made publicly available online. The PHI disclosed included patient names, dates of birth, home addresses, Social Security numbers, claims information, diagnosis/conditions, and other treatment information. These impermissible disclosures of PHI were potential violations of the HIPAA Privacy Rule.

OCR's investigation also identified multiple potential HIPAA Security Rule violations including failures by Inmediata to conduct a compliant risk analysis to determine the potential risks and vulnerabilities to PHI in its systems and to monitor and review its health information systems' activity.

This settlement occurred in August 2024. OCR determined that a corrective action plan was not necessary in this resolution as Inmediata had previously agreed to a settlement with 33 states that includes corrective actions that address OCR's findings in this matter.

Resolution Agreement with Holy Redeemer Hospital

Holy Redeemer Hospital (HRH) paid $35,581 and agreed to take corrective actions to settle potential violations of the HIPAA Privacy Rule. HRH is a hospital located in Meadowbrook, Pennsylvania.

In September of 2023, OCR received a complaint alleging that HRH impermissibly disclosed a female patient's full medical records to the patient's prospective employer, including her surgical history, gynecological history, obstetric history, and other sensitive health information concerning reproductive health care. The Complainant stated that she had requested that HRH send one specific test result, unrelated to her reproductive health, to a prospective employer. OCR's investigation found that HRH disclosed the patient's full medical record, including PHI concerning her reproductive health care, that it did not have the patient's authorization for the broad disclosure, and that there otherwise was no applicable requirement or permission under the Privacy Rule for such a broad release of her medical records.

This settlement occurred in September 2024. In addition to the monetary settlement, HRH agreed to:

- Submit a breach report to HHS regarding this incident;
- Develop, maintain, and revise, as necessary, its 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 and security of PHI.

Civil Money Penalty imposed on Children's Hospital Colorado

OCR imposed a civil money penalty of $548,265 against Children's Hospital Colorado (CHC). CHC is a children's hospital headquartered in Aurora, Colorado.

OCR launched an investigation after receiving breach reports in 2017 and 2020 regarding email phishing and cyberattacks. These breach incidents compromised one email account containing the PHI of 3,370 individuals and three additional email accounts containing the PHI of 10,840 individuals. OCR's investigation determined that the first reported breach occurred because multi-factor authentication was disabled, and the second breach occurred when workforce members gave permission to unknown third parties to access their email accounts. OCR also found violations of the HIPAA Privacy Rule for failure to train workforce members on the HIPAA Privacy Rule, and the HIPAA Security Rule requirement to conduct a compliant risk analysis to determine the potential risks and vulnerabilities to PHI in its computer systems.

In June 2024, OCR issued a Notice of Proposed Determination seeking to impose a civil money penalty. Children's Hospital Colorado waived its right to a hearing and did not contest OCR's findings. Accordingly, in September 2024, OCR issued a Notice of Final Determination and imposed a civil money penalty of $548,265.

Civil Money Penalty imposed on Gulf Coast Pain Management Consultants

OCR imposed a civil money penalty of $1,190,000 against Gulf Coast Pain Management Consultants (Gulf Coast). Gulf Coast is a pain management medical practice with 126 employees with locations in Alabama, Florida, Delaware, Maryland, New Jersey, and Pennsylvania.

OCR initiated an investigation following the receipt of a breach report in April 2019 by Gulf Coast which reported that a former contractor had impermissibly accessed Gulf Coast's electronic medical record system. OCR's investigation determined that the impermissible access occurred on three occasions, affecting approximately 34,310 individuals. The compromised PHI included patient names, addresses, phone numbers, email addresses, dates of birth, Social Security numbers, chart numbers, insurance information, and primary care information. OCR found four violations by Gulf Coast of the HIPAA Security Rule, including failures to:

- Conduct an accurate and thorough risk analysis to determine the potential risks and vulnerabilities to the confidentiality, integrity, and availability of its ePHI;
- Implement procedures to regularly review records of activity in information systems;
- Implement procedures to terminate former workforce members' access to ePHI; and
- Implement procedures for establishing and modifying workforce members' access to information systems.

In August 2024, OCR issued a Notice of Proposed Determination seeking to impose a civil money penalty. Gulf Coast waived its right to a hearing and did not contest OCR's findings. Accordingly, in September 2024, OCR issued a Notice of Final Determination and imposed a civil money penalty of $1,190,000.

Civil Money Penalty imposed on Gums Dental Care

OCR imposed a civil money penalty of $70,000 against Gums Dental Care (GDC). GDC is a solo dental practice in Maryland that provides family dental care.

In May 2019, OCR received a complaint alleging that GDC failed to provide the Complainant with complete copies of her and her minor children's dental records. OCR closed the complaint with technical assistance to GDC on the HIPAA right of access requirements. In August 2019, OCR received a second complaint when GDC still had not provided the Complainant with the requested records. OCR initiated an investigation and subsequently found that GDC failed to take timely action in response to the patient's right of access request. Specifically, the Complainant submitted written requests for the records in April 2019, and again in June 2019, but GDC did not attempt to provide the records until May 2022.

In March 2022, OCR issued a Notice of Proposed Determination seeking to impose a $70,000 civil monetary penalty. GDC challenged OCR's Notice of Proposed Determination and requested a hearing before an Administrative Law Judge (ALJ). On September 29, 2023, the ALJ imposed a $70,000 civil monetary penalty. GDC appealed the decision, and on March 22, 2024, the Departmental Appeals Board affirmed the Decision. In October 2024, OCR issued a Notice of Final Determination and imposed a civil money penalty in the amount of $70,000.

Resolution Agreement with Elgon Information Systems

Elgon Information Systems (Elgon) paid $80,000 and agreed to take corrective actions to settle potential violations of the HIPAA Security Rule. Elgon is a company that provides electronic

medical records and billing support services and is located in Massachusetts.

In June 2023, Elgon filed a breach report stating that approximately 31,248 individuals were affected when Elgon's computer system was infected with ransomware. OCR's investigation determined that Elgon failed to conduct an accurate and thorough risk analysis to determine the potential risks and vulnerabilities to ePHI in its computer system.

This settlement occurred in November 2024. In addition to a monetary settlement, Elgon agreed to:

- Review and update its risk analysis to determine the potential risks and vulnerabilities to the confidentiality, integrity, and availability of its ePHI;
- 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.

Resolution Agreement with Virtual Private Network Solutions

Virtual Private Network Solutions (VPNS) paid $90,000 and agreed to take corrective actions to settle potential violations of the HIPAA Security Rule. VPNS provides data hosting, cloud services, and user and application support to covered entities and business associates. It is based in Richmond, Virginia.

In December 2021, OCR received a breach report from VPNS stating that it experienced a ransomware incident that impacted portions of its server infrastructure. OCR's investigation determined that VPNS failed to conduct a compliant risk analysis to determine the potential risks and vulnerabilities to ePHI in their system.

This settlement occurred in November 2024. In addition to the monetary settlement, VPNS agreed to:

- Conduct an accurate and thorough risk analysis to determine the potential risks and vulnerabilities to the confidentiality, integrity, and availability of its ePHI;
- Implement a risk management plan to address and mitigate security risks and vulnerabilities identified in its risk analysis;
- Develop, maintain, and revise, as necessary, its written policies and procedures to comply with the HIPAA Rules; and
- Conduct a breach risk assessment of the October 31, 2021, breach and provide evidence to OCR that all covered entities affected by the breach have been notified of the breach and the identity of individuals affected by the breach.

Resolution Agreement with Northeast Surgical Group

Northeast Surgical Group (NESG) paid $10,000 and agreed to take corrective actions to settle potential violations of the HIPAA Security Rule. NESG provides surgical care in Michigan.

In March 2023, OCR received a breach report concerning a ransomware incident that had affected NESG's information system. NESG concluded that the ePHI of 15,298 patients had been encrypted and exfiltrated from its network. OCR's investigation determined that NESG had failed to conduct a compliant risk analysis to determine the potential risks and vulnerabilities to ePHI in NESG's systems.

This settlement occurred in November 2024. In addition to the monetary settlement, NESG agreed to:

- Conduct an accurate and thorough risk analysis to determine the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI;
- Implement a risk management plan to address and mitigate security risks and vulnerabilities identified in the risk analysis;
- Develop, maintain, and revise, as necessary, its written policies and procedures to comply with the HIPAA Rules; and
- Train workforce members on the policies and procedures for the privacy and security of PHI.

Resolution Agreement with USR Holdings

USR Holdings (USR) paid $337,750 and agreed to take corrective actions to settle potential violations of the HIPAA Security Rule. USR is located in Florida and provides administrative oversight and support services as a HIPAA business associate.

In February 2019, OCR initiated an investigation after receiving a breach report from USR Holdings stating that it experienced a cyberattack that compromised the PHI of 2,903 individuals. OCR's investigation found that USR failed to conduct an accurate and thorough risk analysis to identify vulnerabilities to the confidentiality, integrity, and availability of ePHI, failed to implement procedures for reviewing records of information system activities, failed to establish procedures to create and maintain retrievable exact copies of ePHI, and failed to prevent the unauthorized access and deletion of ePHI.

This settlement occurred in December 2024. In addition to the monetary settlement, USR agreed to:

- Conduct an accurate and thorough risk analysis to determine the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI;
- Implement a risk management plan to address and mitigate security risks and vulnerabilities identified in the risk analysis;
- Develop a process to evaluate any environmental or operational changes that affect the

security of PHI;

- Develop, maintain, and revise, as necessary, its written policies and procedures to comply with the HIPAA Rules; and
- Train workforce members on the policies and procedures for the privacy and security of PHI.

Resolution Agreement with Solara Medical Supplies

Solara Medical Supplies (Solara) paid $3,000,000 and agreed to take corrective actions to settle potential violations of the HIPAA Security and Breach Notification Rules. Solara provides medical supplies to individuals with diabetes in California.

In November 2019, OCR received a breach report concerning a phishing attack in which an unauthorized third party gained access to eight of Solara's employees' email accounts between April and June 2019, resulting in the breach of 114,007 individuals' ePHI. In January 2020, OCR received notification of a second breach, when Solara reported that it had sent 1,531 breach notification letters to the wrong mailing addresses. OCR's investigation determined that Solara failed to conduct a compliant risk analysis to identify the potential risks and vulnerabilities to ePHI in Solara's systems; failed to implement security measures sufficient to reduce the risks and vulnerabilities to ePHI to a reasonable and appropriate level; and failed to provide timely breach notification to individuals, HHS, and the media.

This settlement occurred in December 2024. In addition to the monetary settlement, Solara agreed to:

- Conduct an accurate and thorough risk analysis to determine the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI;
- Implement a risk management plan to address and mitigate security risks and vulnerabilities identified in the risk analysis;
- Develop, maintain, and revise, as necessary, its written policies and procedures to comply with the HIPAA Rules; and
- Train workforce members on the policies and procedures for the privacy and security of PHI.

Settlement Agreement with South Broward Memorial Hospital District dba Memorial Healthcare System

South Broward Memorial Hospital District dba Memorial Healthcare System (Memorial), a Florida health system, paid $60,000 and agreed to take corrective actions to settle potential violations of the HIPAA Privacy Rule's Right of Access standard.

OCR initiated an investigation after receiving a complaint from an individual who reported that he was not given timely access to his medical records, despite multiple requests by mail, telephone and online. The individual did not receive access to his medical records until approximately nine

months later, after OCR initiated its investigation. OCR found that Memorial failed to take timely action in response to the patient's right of access requests in accordance with the HIPAA Privacy Rule. In July 2024, OCR issued a Notice of Proposed Determination to propose imposing a civil money penalty, and Memorial Healthcare System subsequently requested a hearing before an Administrative Law Judge. In December 2024, Memorial Healthcare System agreed to a settlement agreement to resolve the pending administrative litigation.

Civil Money Penalty imposed on Warby Parker

OCR imposed a civil money penalty of $1,500,000 against Warby Parker. Warby Parker, headquartered in New York, is a manufacturer and online retailer of prescription and non-prescription eyewear.

In December 2018, OCR initiated an investigation following receipt of a breach report filed by Warby Parker. The report stated that in November 2018, Warby Parker became aware of unusual, attempted log-in activity on its website. Warby Parker reported that between September 25, 2018, and November 30, 2018, unauthorized third parties gained access to Warby Parker customer accounts by using usernames and passwords obtained from other, unrelated websites that were presumably breached. In September 2020, Warby Parker filed an addendum breach report, updating the number of individuals affected by the breach to 197,986. The compromised ePHI included customer names, mailing addresses, email addresses, certain payment card information, and eyewear prescription information. Warby Parker also filed subsequent breach reports (each breach report affecting fewer than 500 persons) in April 2020, and June 2022, following similar attacks.

OCR's investigation found evidence of three potential violations of the HIPAA Security Rule, including a failure to conduct an accurate and thorough risk analysis to identify the potential risks and vulnerabilities to ePHI in Warby Parker's systems, a failure to implement security measures sufficient to reduce the risks and vulnerabilities to ePHI to a reasonable and appropriate level, and a failure to implement procedures to regularly review records of information system activity.

In September 2024, OCR issued a Notice of Proposed Determination seeking to impose a CMP. Warby Parker waived its right to a hearing and did not contest OCR's imposition of a CMP. Accordingly, in December 2024, OCR issued a Notice of Final Determination and imposed a civil money penalty of $1,500,000.

Civil Money Penalty imposed on Oregon Health and Science University

OCR imposed a civil money penalty of $200,000 against Oregon Health and Science University (OHSU). OHSU is a public academic health center and research university.

OCR initiated an investigation of OHSU based on a complaint filed in January 2021 from an individual's personal representative – the second complaint OCR received on this matter. In September 2020, OCR resolved the first complaint (received in May 2020) when OCR notified OHSU of its potential noncompliance with the Privacy Rule Right of Access provisions. Although OHSU provided part of the requested records in April 2019, OHSU did not provide all of the

requested records until August 2021, which was nearly a year after OHSU received OCR's September 2020 letter, and sixteen months after the first request for records in April 2019. OCR's investigation found that OHSU failed to take timely action in response to the right of access requests.

In September 2024, OCR issued a Notice of Proposed Determination seeking to impose a CMP. OHSU waived its right to a hearing and did not contest OCR's imposition of a civil monetary penalty. Accordingly, in December 2024, OCR issued a Notice of Final Determination and imposed a civil money penalty of $200,000.

Resolution Agreement with Health Fitness

Health Fitness paid $227,816 and agreed to take corrective actions to settle potential violations of the HIPAA Security Rule. Health Fitness is a business associate that provides wellness plans throughout the United States and is headquartered in Lake Forest, Illinois.

Between October 2018 and January 2019, Health Fitness filed four breach reports regarding a misconfiguration on its servers that exposed the PHI of approximately 4,304 individuals. OCR's investigation found that Health Fitness did not perform a risk analysis to determine vulnerabilities and risks to confidentiality, integrity, and availability of ePHI that it holds.

This settlement occurred in December 2024. In addition to the monetary settlement, Health Fitness agreed to:

- Annually update its risk analysis to determine the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI;
- Develop and implement a risk management plan to address and mitigate security risks and vulnerabilities identified in the risk analysis;
- Implement a process for evaluating environmental and operational changes that affect the security of ePHI; and
- Develop, maintain, and revise, as necessary, certain written policies and procedures to comply with the HIPAA Rules.