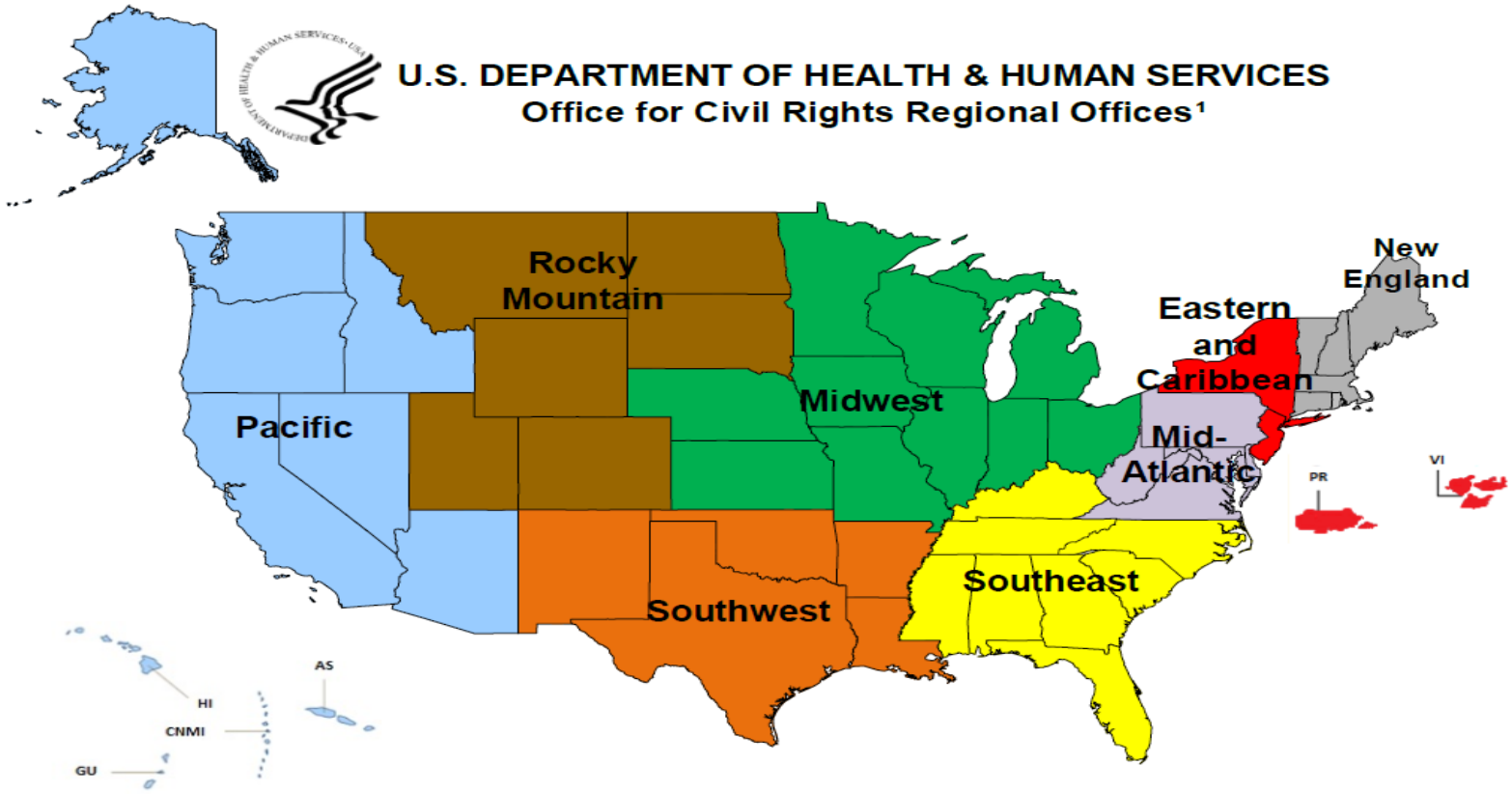
OCR Update and 2024 Priorities

Melanie Fontes Rainer, Director
Office for Civil Rights (OCR)
U.S. Department of Health and Human Services

HIPAA Summit 41
February 27, 2024

Regional Map and Offices



[1] U.S Department of Health and Human Services Regional Offices

New England Region: HHS Region 1
Eastern and Caribbean Region: HHS Region 2
Mid-Atlantic Region: HHS Region 3
Southeast Region: HHS Region 4
Midwest Region: HHS Region 5 and 7
Southwest Region: HHS Region 6
Rocky Mountain Region: HHS Region 8
Pacific Region: HHS Region 9 and 10

2024 Priorities

2024 HIPAA Priorities

- Finalizing 2023 Notice of Proposed Rulemaking on the HIPAA Privacy Rule to Support Reproductive Health Care Privacy and Part 2 Rule
- Prioritizing investigations that follow HIPAA complaint and breach trends:
  - Hacking
  - Ransomware
  - *Right of Access Enforcement Initiative*
  - *Risk Analysis Enforcement Initiative*
- Engaging with Health Care Industry on Cybersecurity
  - Increased presence regionally across the country
  - Videos/Guidance/Newsletters
  - Webinars/Technical Assistance
- Review HIPAA Security Rule

Confidentiality of Substance Use Disorder Patient Records under 42 CFR part 2 ("Part 2") Final Rule

- Final Rule issued on February 8, 2024.
- Modifies Part 2 to increase coordination among providers treating patients for substance use disorders, strengthens confidentiality protections through civil enforcement, and enhances integration of behavioral health information with other medical records to improve patient health outcomes. The final rule includes the following changes :
  - Permits use and disclosure of Part 2 records based on a single patient consent given once for all future uses and disclosures for treatment, payment, and health care operations.
  - Permits redisclosure of Part 2 records by HIPAA covered entities and business associates in accordance with the HIPAA Privacy Rule, with certain exceptions.
  - Provides new rights for patients to obtain an accounting of disclosures and to request restrictions on certain disclosures.
  - Provides HHS with civil enforcement authority, including the potential imposition of civil money penalties for violations of Part 2.
  - Requires breach notification for breaches of Part 2 records.
- Final Rule may be viewed at https://www.federalregister.gov/public-inspection/2024-02544/confidentiality-of-substance-use-disorder-patient-records.
- Fact sheet may be found at https://www.hhs.gov/hipaa/for-professionals/regulatory-initiatives/fact-sheet-42-cfr-part-2-final-rule/index.html.

Proposed Modifications to the HIPAA Privacy Rule to Support Reproductive Health Care Privacy

- Proposes to strengthen privacy protections by prohibiting the use or disclosure of PHI by a regulated entity for either of the following purposes:
  - A criminal, civil, or administrative investigation into or proceeding against any person in connection with seeking, obtaining, providing, or facilitating reproductive health care, where such health care is lawful under the circumstances in which it is provided.
  - The identification of any person for the purpose of initiating such investigations or proceedings.
- Prohibition would apply where the relevant criminal, civil, or administrative investigation or proceeding is in connection with one of the following:
  - Reproductive health care that is sought, obtained, provided, or facilitated **in a state where the health care is lawful and outside of the state where the investigation or proceeding is authorized**.
  - Reproductive health care that is protected, required, or expressly authorized **by federal law**, regardless of the state in which such health care is provided.
  - Reproductive health care that is provided **in the state where the investigation or proceeding is authorized and is permitted by the law of the state in which such health care is provided**.

OCR is reviewing public comments and working on a Final Rule.

NIST's Implementing the HIPAA Security Rule: A Cybersecurity Resource Guide

- This revised publication includes resources to help improve understanding of the HIPAA Security Rule, drive compliance with the law, and bolster cybersecurity.
- Provides an overview of the HIPAA Security Rule, strategies for assessing and managing risks to electronic protected health information, suggestions for cybersecurity measures and solutions that HIPAA covered entities and business associates might consider as part of an information security program, and resources for implementing the Security Rule. Specific topic areas include:
  - Explanations of the HIPAA Security Rule's Risk Analysis and Risk Management requirements.
  - Key Activities to consider when implementing Security Rule requirements.
  - Actionable steps for implementing security measures.
  - Sample questions to determine adequacy of cybersecurity measures to protect ePHI.
- Available at: https://csrc.nist.gov/pubs/sp/800/66/r2/final

HIPAA and The Use of Online Tracking Technologies Bulletin

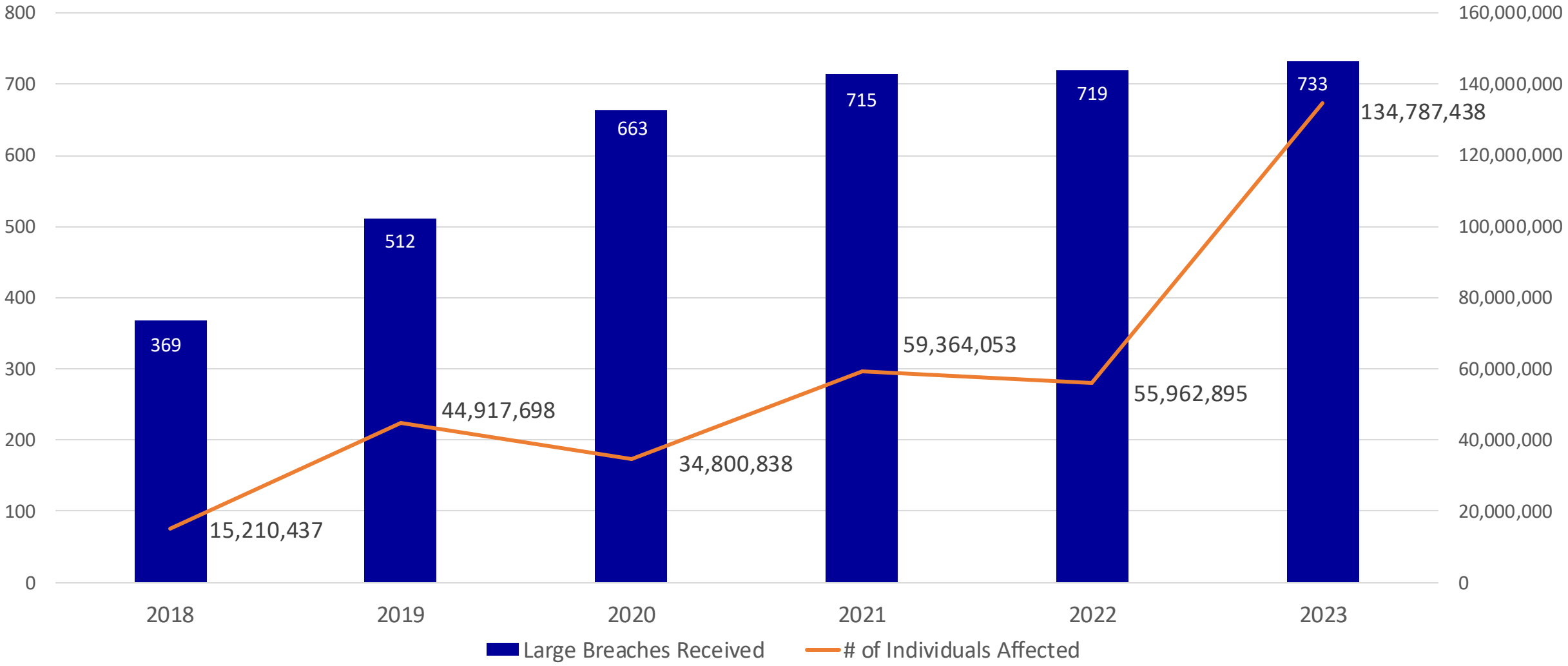
- Highlights HIPAA regulated entities' obligations when using tracking technologies, like Google Analytics and Meta Pixel, to collect and analyze information about how users interact with regulated entities' websites or apps
- Reminds regulated entities they are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules
- Explains what tracking technologies are, how they are used, and what steps regulated entities must take to protect ePHI when using tracking technologies to comply with the HIPAA Rules. Specifically, the Bulletin provides insight and examples of:
  - Tracking on webpages
  - Tracking within mobile apps
  - HIPAA compliance obligations for regulated entities when using tracking technologies
- OCR and the FTC issued a joint letter to warn hospital systems and telehealth providers about privacy and security risks

https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html

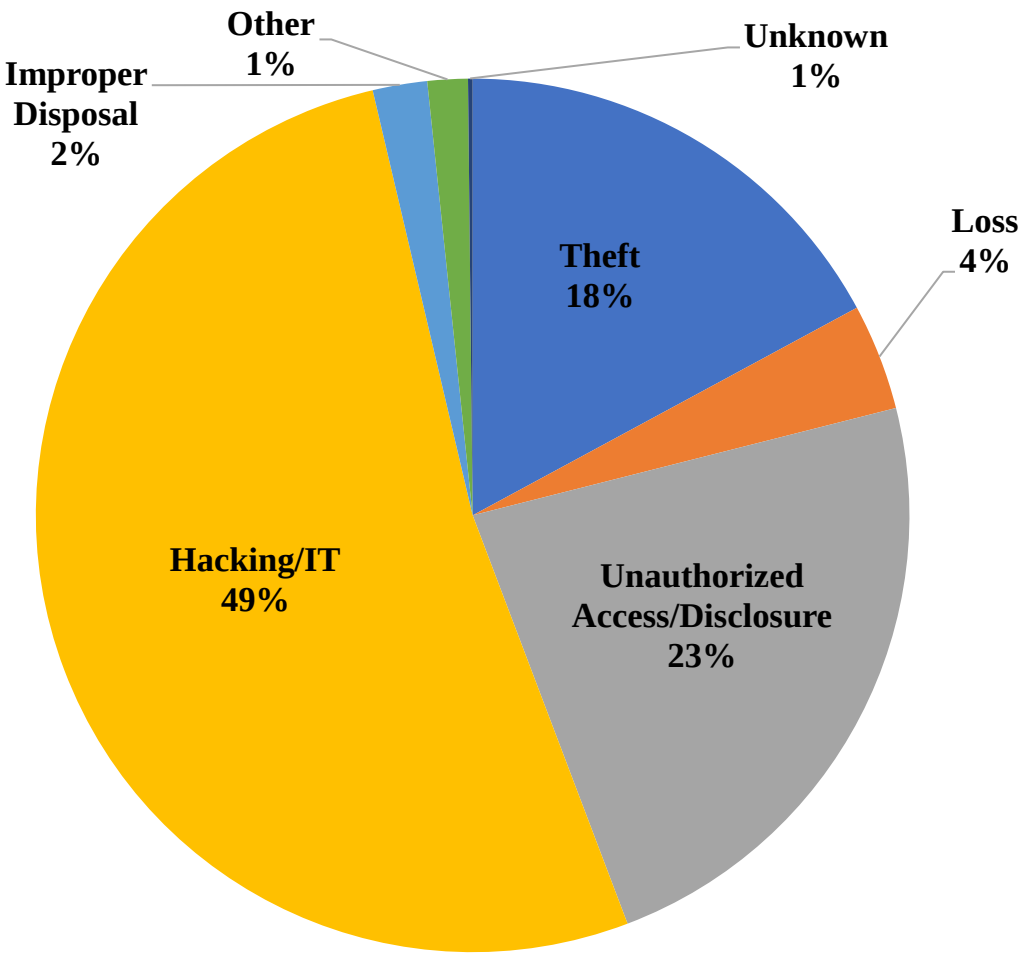
https://www.hhs.gov/about/news/2023/07/20/hhs-office-civil-rights-federal-trade-commission-warn-hospital-systems-telehealth-providers-privacy-security-risks-online-tracking-technologies.html

ENFORCEMENT & BREACH ACTIVITY

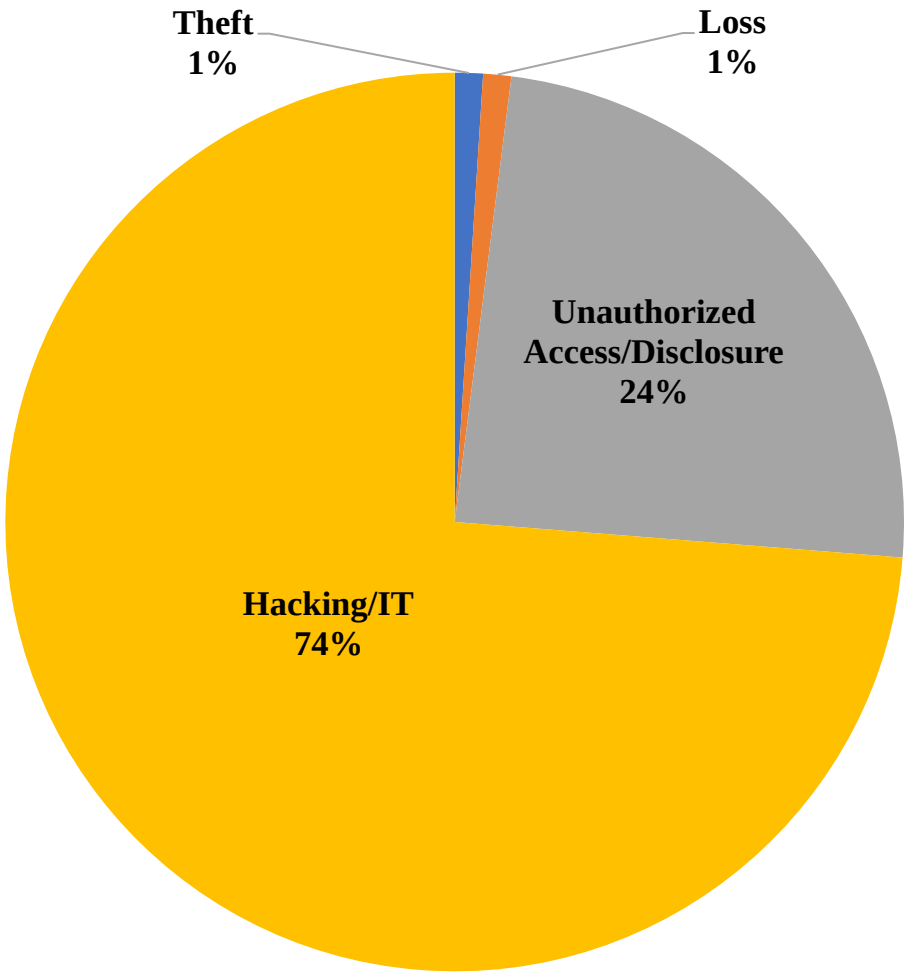
Large Breaches Received and # of Individuals Affected 2018 - 2023



500+ Breaches by Type of Breach



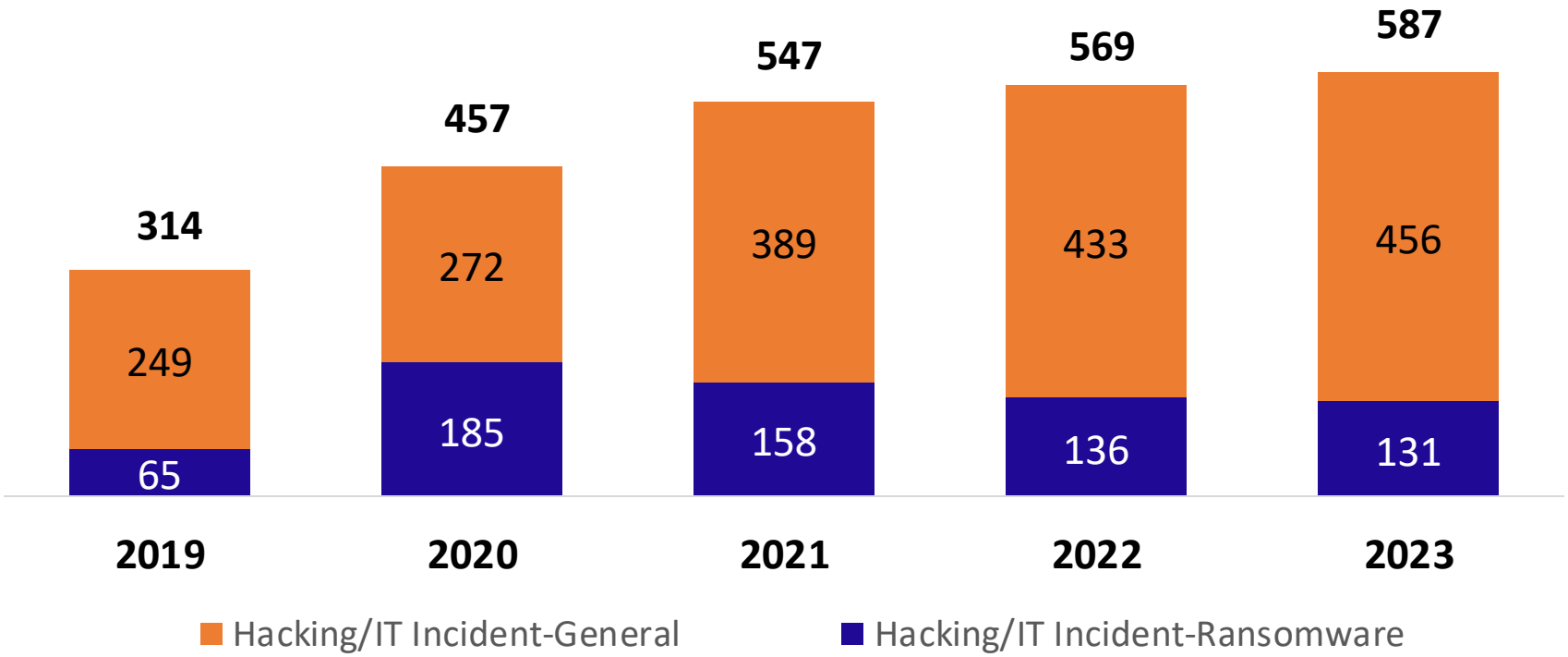
September 23, 2009 through Dec 31, 2023



January 1, 2024 through February 29, 2024

Breaches Affecting 500 or More Individuals
Reports Received Involving Hacking/IT Incidents

Calendar Years 2019 - 2023



General HIPAA Enforcement Highlights

- OCR received 31,731 HIPAA cases in 2023.
- In most cases, entities are able to demonstrate satisfactory compliance through voluntary cooperation and corrective action.
- In some cases, the nature or scope of indicated noncompliance warrants additional enforcement action.
- Resolution Agreements/Corrective Action Plans
  - 136 settlement agreements that include detailed corrective action plans and monetary settlement amounts
- 8 civil money penalties

$4.75 Million Settlement with Montefiore Medical Center

- OCR investigation opened following receipt of a breach report revealing that an employee inappropriately accessed patient the electronic protected health information of 12,517 patients and sold it to an identity theft ring.
- OCR's investigation revealed multiple potential violations of the HIPAA Security Rule, including failures to:
  - Analyze and identify potential risks and vulnerabilities to PHI,
  - Monitor and safeguard its health information systems' activity, and
  - Implement hardware and software and procedural mechanisms that record and examine activity in information systems containing or using ePHI.
- Montefiore paid $4,750,000 to OCR and agreed to implement a corrective action plan with 2 years of OCR monitoring that will improve protections to the security of ePHI.

Phishing Settlement with LaFourche Medical Group

- OCR investigation opened following receipt of a breach report revealing that a hacker gained access to an email account containing ePHI (affected approximately 34,862 individuals).
- OCR's investigation revealed multiple potential violations of the HIPAA Security Rule, including failures to:
  - Analyze and identify potential risks and vulnerabilities to PHI, and
  - Monitor and safeguard its health information systems' activity
- Lafourche paid $480,000 to OCR and agreed to implement a corrective action plan with 2 years of OCR monitoring that will improve protections to the security of ePHI.

Ransomware Settlement with Green Ridge Behavioral Health

- OCR investigation opened following receipt of a breach report revealing network server infected with ransomware (Affected more than 14,000 patients)
- OCR's investigation revealed multiple potential violations of the HIPAA Security Rule, including failures to:
  - Have in place an analysis to determine the potential risks and vulnerabilities to electronic protected health information;
  - Implement security measures to reduce risks and vulnerabilities; and
  - Have sufficient monitoring of its health information systems' activity to protect against a cyber-attack.
- Green Ridge paid $40,000 to OCR and agreed to implement a corrective action plan with 3 years of OCR monitoring to improve their security of ePHI.

Risk Analysis Initiative

- New Enforcement Initiative
- Focus on compliance with key HIPAA Security Rule requirement
- Most OCR large breach investigations reveal a lack of a compliant risk analysis
- Drive better practices to protect electronic protected health information (ePHI)
- Better overall security of data

Recurring HIPAA Compliance Issues

- Individual Right of Access
- Risk Analysis
- Business Associate Agreements
- Access Controls
- Audit Controls
- Information System Activity Review

Right of Access Initiative

- HIPAA Privacy Rule gives individuals a right to timely access to their health records (30 days with a possibility of one 30-day extension), and at a reasonable, cost-based fee
- OCR receives many complaints alleging denial or no access to health records
- Announced Enforcement Initiative in February 2019
  - OCR Enforcement Priority
  - Investigations launched across the country
  - To date; forty-four settlements and two CMPs

Best Practices

- Review all vendor and contractor relationships to ensure BAAs are in place as appropriate and address breach/security incident obligations
- Risk analysis and risk management should be integrated into business processes; conducted regularly and when new technologies and business operations are planned
- Dispose of PHI on media and paper that has been identified for disposal in a timely manner
- Incorporate lessons learned from incidents into the overall security management process
- Provide training specific to organization and job responsibilities and on regular basis; reinforce workforce members' critical role in protecting privacy and security

OCR Common Cyber-Attacks Video

- Video on how the HIPAA Security Rule can help regulated entities defend against common cyber-attacks and an in-depth discussion on the anatomy of a cyber-attack:
  - Gain access via compromised accounts
  - Reconnaissance
  - Elevation of privileges
  - Exfiltration of data and/or deployment of malware/ransomware
- Topics covered include:
  - OCR breach and investigation trend analysis
  - Common attack vectors such as phishing, vulnerability exploitation, and compromised accounts
  - OCR investigations of weaknesses that led to or contributed to breaches
  - How Security Rule compliance can help regulated entities defend against cyber-attacks
- The video may be found on OCR's YouTube channel at: http://youtube.com/watch?v=VnbBxxyZLc8
- The video in Spanish may be found on OCR's YouTube channel at: http://youtube.com/watch?v=3oVarCxLcB8

OCR HIPAA Risk Analysis Webinar

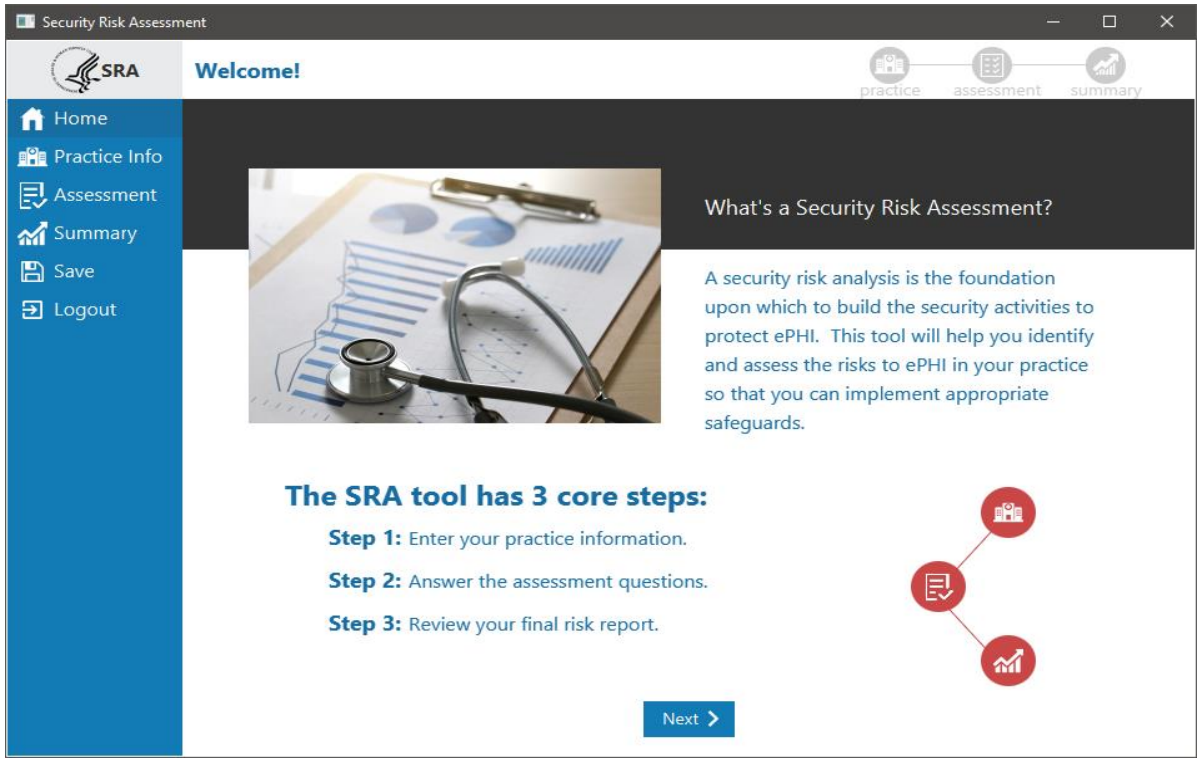
- Video on the HIPAA Security Rule Risk Analysis requirement.
- Discusses what is required to conduct an accurate and thorough assessment of potential risks and vulnerabilities to ePHI and review common risk analysis deficiencies OCR has identified in investigations.
- Topics covered include:
  - How to prepare for a risk analysis
  - How should ePHI be assessed
  - What does it mean to be accurate and thorough
  - What purpose does a risk analysis serve once completed
  - Examples from OCR investigations
  - Resources

The video may be found on OCR's YouTube channel at:
https://www.youtube.com/watch?v=hxfxhokzKEU

Cybersecurity Performance Goals

- In 2023, HHS released voluntary health care specific Cybersecurity Performance Goals (CPGs) to help healthcare organizations implement high-impact cybersecurity practices
- Designed to better protect the healthcare sector from cyberattacks, improve response when events occur, and minimize residual risk.
- Works in tandem with HIPAA Security Rule
- Find the CPGs here: https://hphcyber.hhs.gov/performance-goals.html

SRA Tool



https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool

Designed to assist small to medium sized organizations in conducting an internal security risk assessment to aid in meeting the security risk analysis requirements of the HIPAA Security Rule and the CMS EHR Incentive Program.

The SRA tool guides users through a series of questions based on standards identified in the HIPAA Security Rule. Responses are sorted into Areas of Success and Areas for Review.

Not all areas of risk may be captured by the tool. Risks not identified and assessed via the SRA Tool must be documented elsewhere.

Ransomware Resources

HHS Health Sector Cybersecurity Coordination Center Threat Briefs:

- https://www.hhs.gov/about/agencies/asa/ocio/hc3/products/index.html#sector-alerts

Section 405(d) of the Cybersecurity Act of 2015 Resources:

- Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients https://405d.hhs.gov/Documents/HICP-Main-508.pdf
- 405(d) Products, Publications and Materials https://405d.hhs.gov/resources

OCR Guidance:

- Ransomware https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf
- Cybersecurity https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html
- Risk Analysis https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf

HHS Security Risk Assessment Tool: https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool

CISA Resources:

- https://www.cisa.gov/stopransomware
- https://www.cisa.gov/sites/default/files/publications/CISA_Fact_Sheet-Protecting_Sensitive_and_Personal_Information_from_Ransomware-Caused_Data_Breaches-508C.pdf
- https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C_.pdf

FBI Resources:

- https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware
- https://www.ic3.gov/Media/Y2019/PSA191002

Connect with Us

Office for Civil Rights

U.S. Department of Health and Human Services

www.hhs.gov/hipaa

Join our Privacy and Security listservs at
https://www.hhs.gov/hipaa/for-professionals/list-serve/

@HHSOCR