Cybersecurity Issues

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

Presented to Health Care Controlled Networks

June 18, 2024

Who We Are

As the Department's civil rights, conscience and religious freedom, and health information privacy rights law enforcement agency, OCR investigates complaints and breach reports, enforces rights, and promulgates regulations, develops policy, and provides technical assistance and public education to ensure understanding of and compliance with non-discrimination and health information privacy laws.

Policy

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

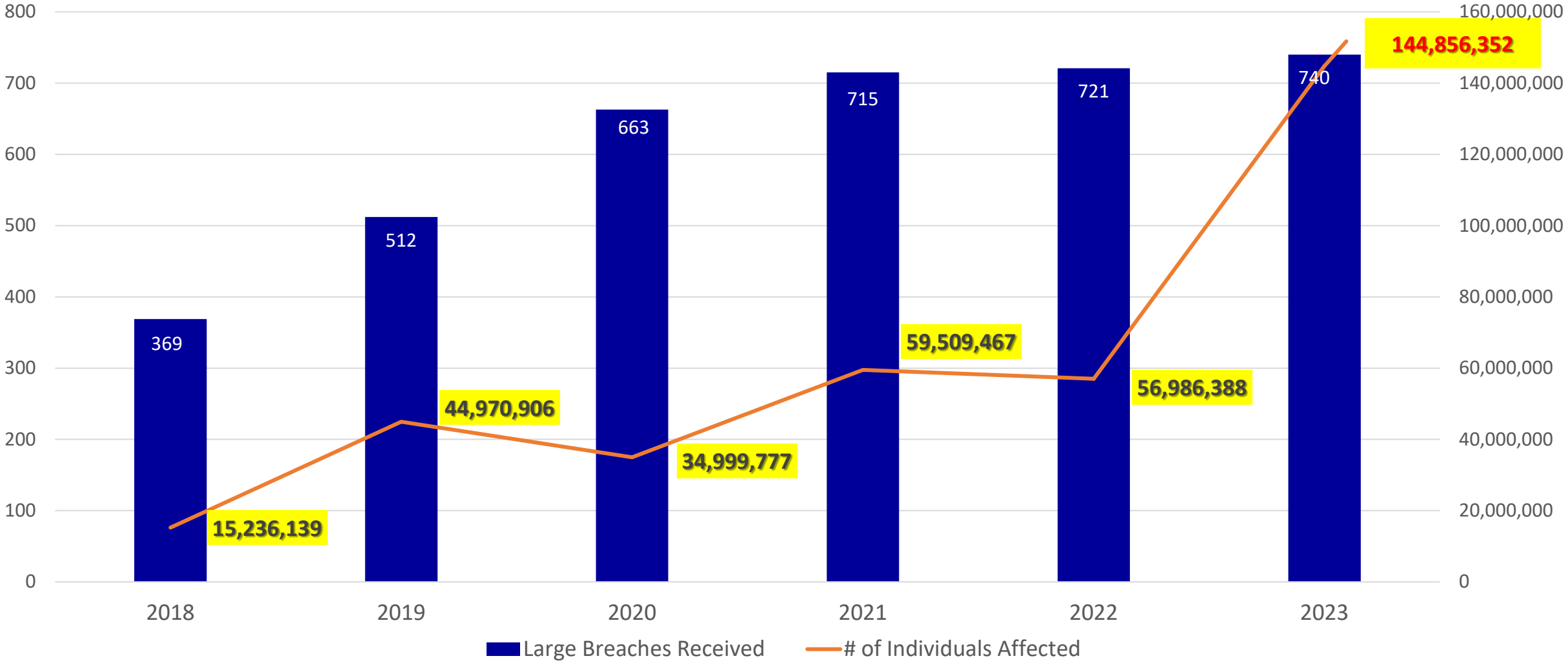
https://www.hhs.gov/about/news/2023/07/20/hhs-office-civil-rights-federal-trade-commission-warn-hospital-systems-telehealth-providers-privacy-security-risks-online-tracking-technologies.html

BREACH HIGHLIGHTS AND RECENT ENFORCEMENT ACTIVITY

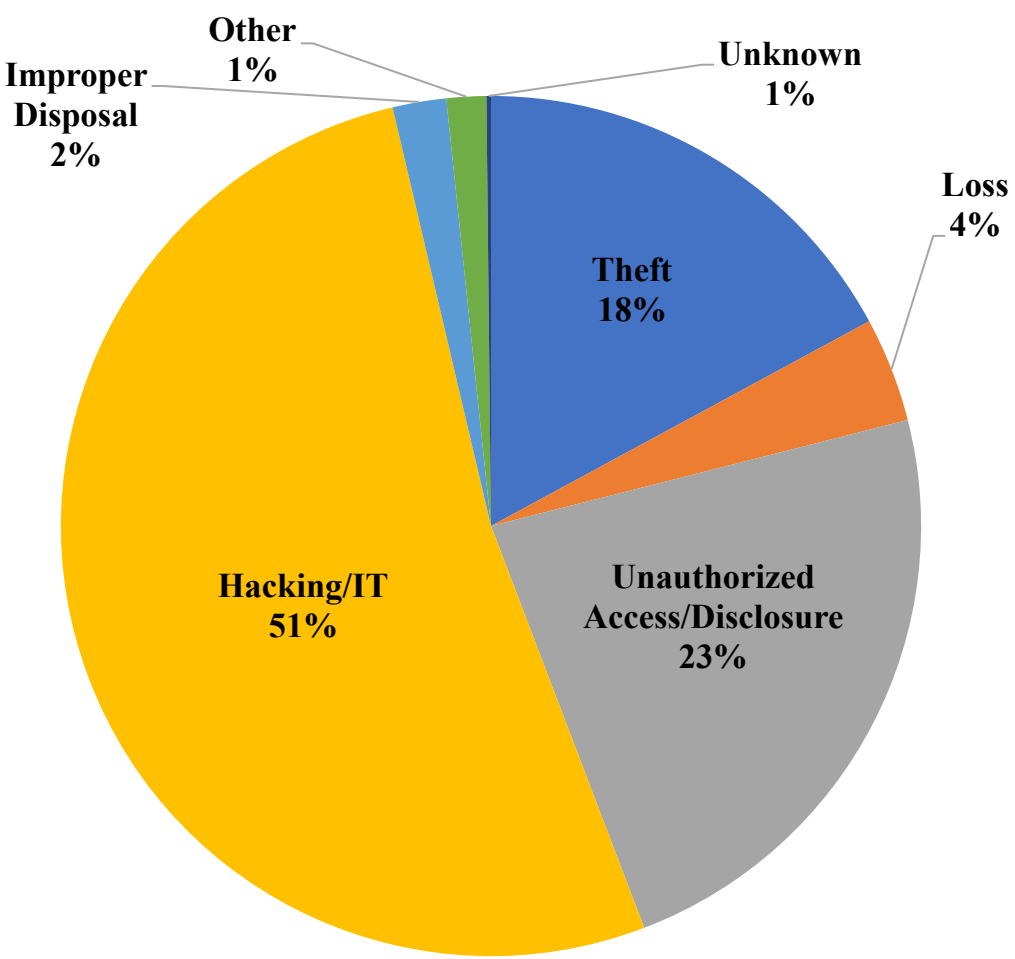
What Happens When OCR Receives a Breach Report

- OCR posts breaches affecting 500+ individuals on OCR website (after verification of report)
  - Public can search and sort posted breaches
  - Received over 700 breach reports affecting 500+ individuals in 2022
- OCR opens investigations into breaches affecting 500+ individuals, and into a number of smaller breaches
- OCR breach investigations examine:
  - Underlying cause of the breach
  - Actions taken to respond to the breach (breach notification) and prevent future incidents
  - Entity's compliance prior to the breach

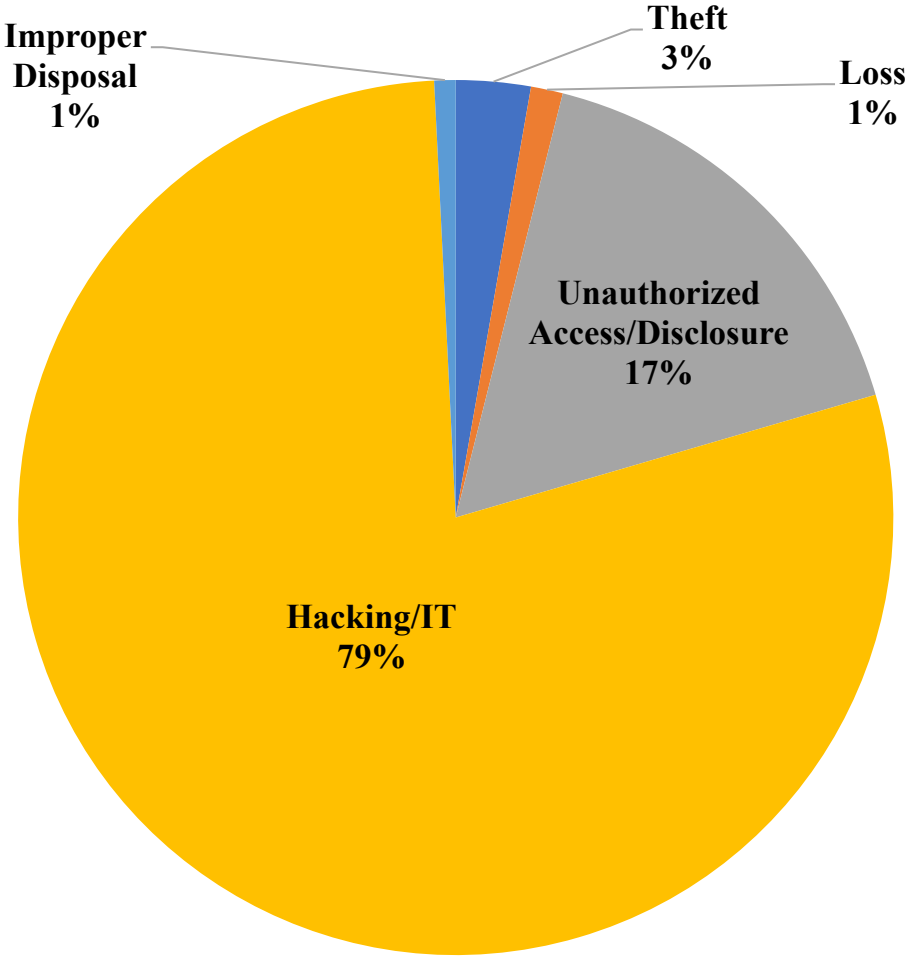
Large Breaches Received and # of Individuals Affected 2018 - 2023



500+ Breaches by Type of Breach

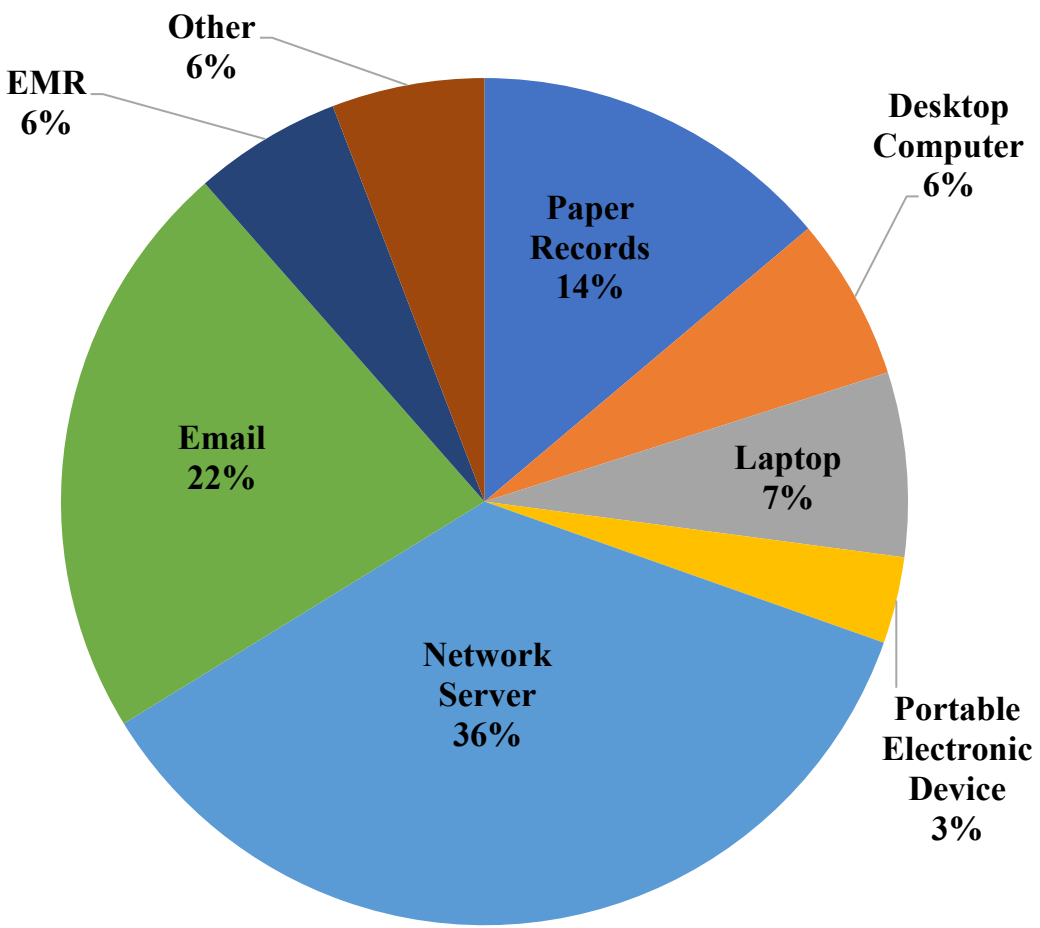


September 23, 2009 through Dec 31, 2023

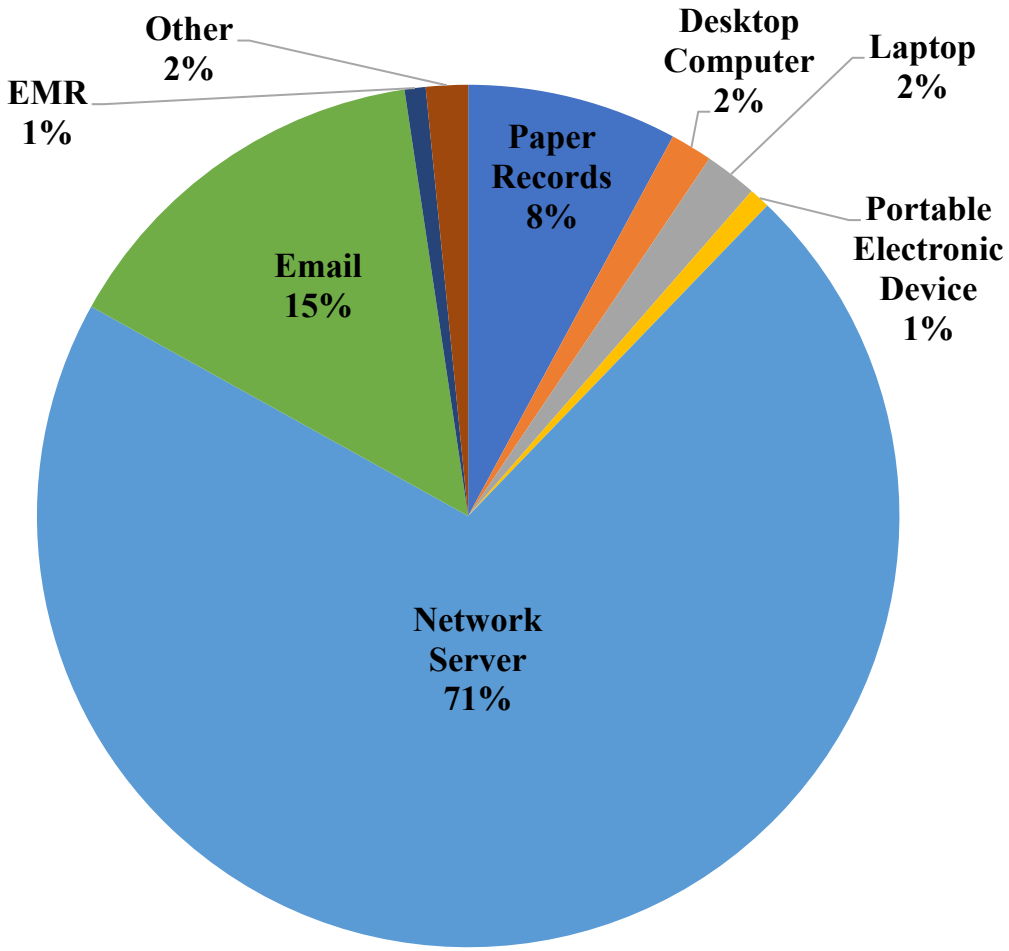


January 1, 2024 through April 30, 2024

500+ Breaches by Location of Breach



September 23, 2009 through Dec 31, 2023

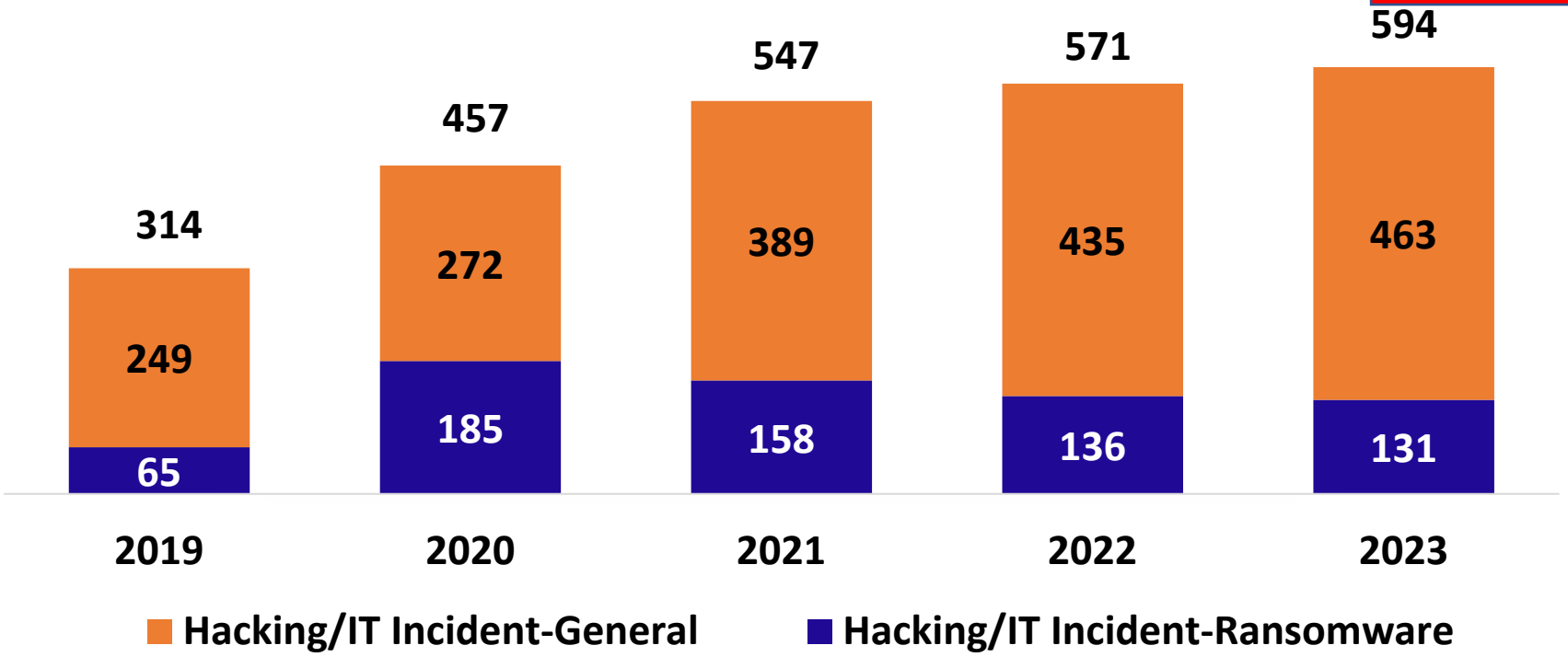


January 1, 2024 through April 30, 2024

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

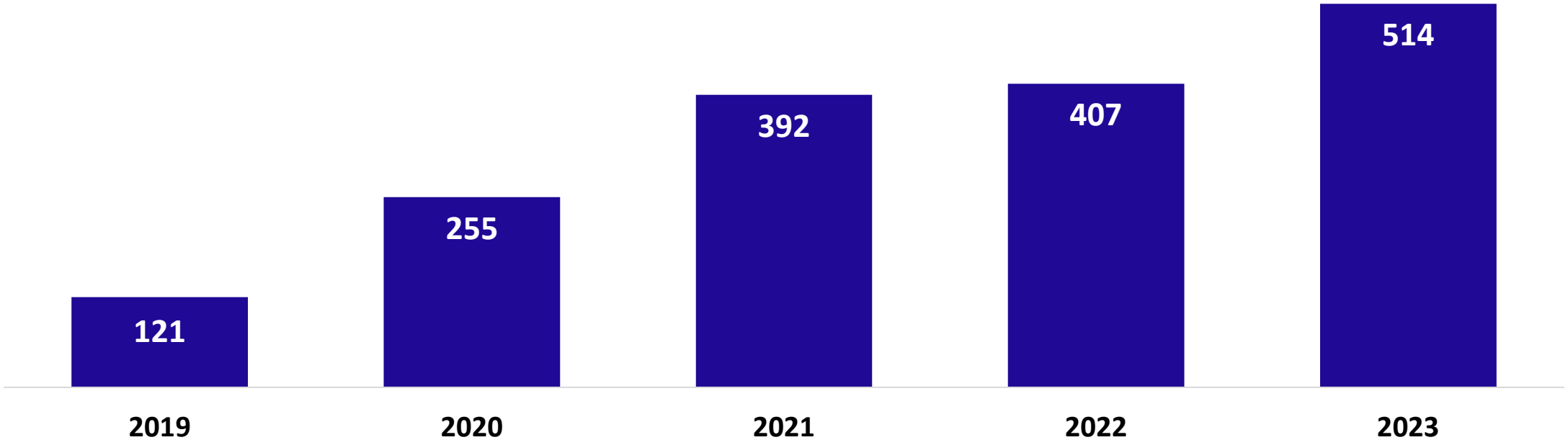
Calendar Years 2019 - 2023

2019 - 2023
89% increase in hacking
102% increase in ransomware



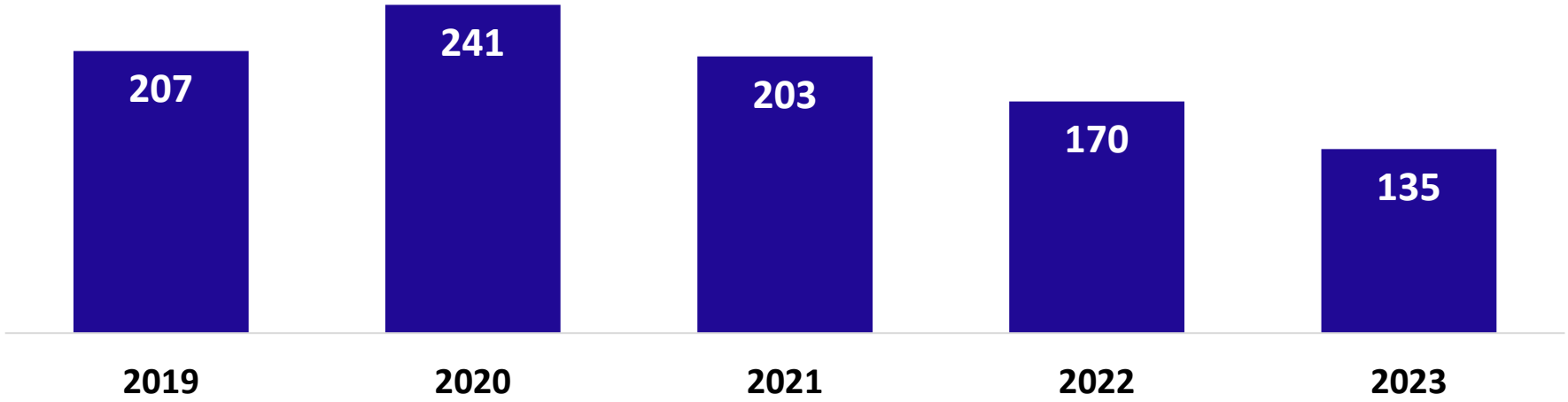
Breaches Affecting 500 or More Individuals
Reports Received of Breaches Involving Network Servers

Calendar Years 2019 - 2023



Breaches Affecting 500 or More Individuals
Reports Received of Breaches Involving Email Accounts

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
  - 138 settlement agreements that include detailed corrective action plans and monetary settlement amounts
- 9 civil money penalties

Recent Announced OCR HIPAA Enforcement Actions

May-23	David Mente, MA, LPC	$15,000
May-23	MedEvolve, Inc.	$350,000
June-23	Manasa Health Center	$30,000
June-23	Yakima Valley Memorial Hospital	$240,000
June-23	iHealth Solutions, LLC	$75,000
Aug-23	United Healthcare Insurance Company	$80,000
Sep-23	LA Care Health Plan	$1,300,000
Oct-23	Doctors' Management Services	$100,000
Nov-23	St. Joseph's Medical Center	$80,000
Dec-23	Lafourche Medical Group	$480,000
Jan-24	Optum Medical Care of New Jersey	$160,000
Feb-24	Montefiore Medical Center	$4,750,000
Feb-24	Green Ridge Behavioral Health, LLC	$40,000
Mar-24	Phoenix Healthcare	$35,000
Apr-24	Essex Residential Care, LLC	$100,000

$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.

Recurring Compliance Issues

- Business Associate Agreements
- Risk Analysis
- Failure to Manage Identified Risk, e.g. Encrypt
- Lack of Transmission Security
- Lack of Appropriate Auditing
- No Patching of Software
- Insider Threat
- Lack of Access controls
- Improper Disposal
- Insufficient Data Backup and Contingency Planning

Lack of Business Associate Agreements

HIPAA generally requires that covered entities and business associates enter into agreements with their business associates to ensure that the business associates will appropriately safeguard protected health information. *See 45 CFR § 164.308(b).* Examples of Potential Business Associates:

- A collections agency providing debt collection services to a health care provider which involve access to protected health information.
- An independent medical transcriptionist that provides transcription services to a physician.
- A subcontractor providing remote backup services of PHI data for an IT contractor-business associate of a health care provider.

Incomplete or Inaccurate Risk Analysis

- Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (ePHI) held by the [organization]. *See 45 CFR § 164.308(a)(1)(ii)(A).*

- Organizations frequently underestimate the proliferation of ePHI within their environments. When conducting a risk analysis, an organization must identify all of the ePHI created, maintained, received or transmitted by the organization.

- Examples: Applications like EHR, billing systems; documents and spreadsheets; database systems and web servers; fax servers, backup servers; etc.); Cloud based servers; Medical Devices Messaging Apps (email, texting, ftp); Media

The Risk Analysis Process: Key Activities Required by the Security Rule

- **Inventory** to determine where ePHI is stored
- **Evaluate** probability and criticality of potential risks
- **Adopt** reasonable and appropriate security safeguards based on results of risk analysis
- **Implement/Modify** security safeguards to reduce risk to a reasonable and appropriate level
- **Document** safeguards and rationale
- **Evaluate** effectiveness of measures in place
- **Maintain** continuous security protections
- **Repeat**

Failure to Manage Identified Risk

- The Risk Management Standard requires the "[implementation of] security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with [the Security Rule]." *See 45 CFR § 164.308(a)(1)(ii)(B).*
- Investigations conducted by OCR regarding several instances of breaches uncovered that risks attributable to a reported breach had been previously identified as part of a risk analysis, but that the organization failed to act on its risk analysis and implement appropriate security measures.
- In some instances, encryption was included as part of a remediation plan; however, activities to implement encryption were not carried out or were not implemented within a reasonable timeframe as established in a remediation plan.

Lack of Transmission Security

- When electronically transmitting ePHI, a mechanism to encrypt the ePHI must be implemented unless not reasonable and appropriate. *See 45 CFR § 164.312(e)(2)(ii).*
- Applications for which encryption should be considered when transmitting ePHI may include:
  - Email
  - Texting
  - Application sessions
  - File transmissions (e.g., ftp)
  - Remote backups
  - Remote access and support sessions (e.g., VPN)

Lack of Appropriate Auditing

- The HIPAA Rules require the "[implementation] of hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information." *See 45 CFR § 164.312(b).*

- Once audit mechanisms are put into place on appropriate information systems, procedures must be implemented to "regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports." *See 45 CFR § 164.308(a)(1)(ii)(D).*

- Activities that could warrant additional investigation:
  - Access to PHI during non-business hours or during time off
  - Access to an abnormally high number of records containing PHI
  - Access to PHI of persons for which media interest exists
  - Access to PHI of employees
  - Failed log-in attempts

No Patching of Software

- The use of unpatched or unsupported software on systems that access ePHI could introduce additional risk into an environment.
- Continued use of such systems must be included within an organization's risk analysis and appropriate mitigation strategies implemented to reduce risk to a reasonable and appropriate level.
- In addition to operating systems, EMR/PM systems, and office productivity software, software that should be monitored for patches and vendor end-of-life for support include:
  - Router and firewall firmware
  - Anti-virus and anti-malware software
  - Multimedia and runtime environments (e.g., Adobe Flash, Java, etc.)

Insider Threat

- Organizations must "[i]mplement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information … and to prevent those workforce members who do not have access … from obtaining access to electronic protected health information," as part of its Workforce Security plan. *See 45 CFR § 164.308(a)(3).*
- Appropriate workforce screening procedures could be included as part of an organization's Workforce Clearance process (e.g., background and OIG LEIE checks). *See 45 CFR § 164.308(a)(3)(ii)(B).*
- Termination Procedures should be in place to ensure that access to PHI is revoked as part of an organization's workforce exit or separation process. *See 45 CFR § 164.308(a)(3)(ii)(C).*

Disposal

- When an organization disposes of electronic media which may contain ePHI, it must implement policies and procedures to ensure that proper and secure disposal processes are used. *See 45 CFR § 164.310(d)(2)(i).*
- The implemented disposal procedures must ensure that "[e]lectronic media have been cleared, purged, or destroyed consistent with *NIST Special Publication 800–88: Guidelines for Media Sanitization*, such that the PHI cannot be retrieved."
- Electronic media and devices identified for disposal should be disposed of in a timely manner to avoid accidental improper disposal.
- Organizations must ensure that all electronic devices and media containing PHI are disposed of securely; including non-computer devices such as copier systems and medical devices.

Insufficient Backup and Contingency Planning

- Organizations must ensure that adequate contingency plans (including data backup and disaster recovery plans) are in place and would be effective when implemented in the event of an actual disaster or emergency situation. *See 45 CFR § 164.308(a)(7).*
- Leveraging the resources of cloud vendors may aid an organization with its contingency planning regarding certain applications or computer systems, but may not encompass all that is required for an effective contingency plan.
- As reasonable and appropriate, organizations must periodically test their contingency plans and revise such plans as necessary when the results of the contingency exercise identify deficiencies. *See 45 CFR § 164.308(a)(7)(ii)(D).*

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

Resources

HITECH Amendment on Recognized Security Practices and Video

- 2021 HITECH Amendment requires OCR to consider whether a regulated entity has adequately demonstrated that recognized security practices were “in place” for the prior 12 months.
- Can mitigate civil money penalties, other remedies in settlement agreements, or early, favorable termination of audits.
- No liability for electing not to implement recognized security practices.
- OCR published a video in October 2022 that covers:
    - The 2021 HITECH Amendment
    - How regulated entities can adequately demonstrate that RSPs are in place
    - How OCR is requesting evidence of RSPs
    - Resources for information about RSPs
    - OCR’s 2022 Request for Information on RSPs
- The video may be found on OCR’s YouTube channel at: https://youtu.be/e2wG7jUiRjE

OCR Common Cyber-Attacks Video

- Video on how the HIPAA Security Rule can help regulated entities defend against common cyber-attacks
- Topics covered include:
  - OCR breach and investigation trend analysis
  - Common attack vectors
  - OCR investigations of weaknesses that led to or contributed to breaches
  - How Security Rule compliance can help regulated entities defend against cyber-attacks

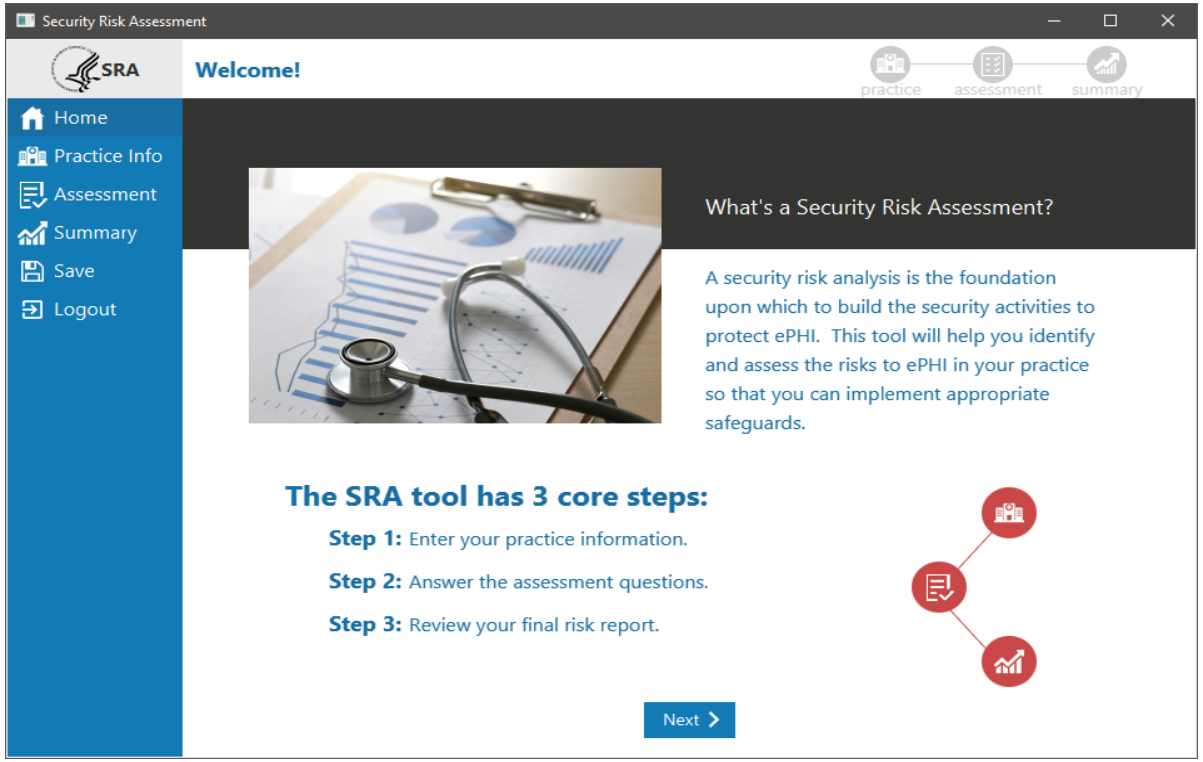
- The video may be found on OCR's YouTube channel at: http://youtube.com/watch?v=VnbBxxyZLc8
- The video in Spanish may be found on OCR's YouTube channel at: http://youtube.com/watch?v=3oVarCxLcB8

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

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.

Resources for Mobile Health App Developers

- Mobile Health Apps Interactive Tool
- Health App Use Scenarios & HIPAA
- HIPAA Right of Access, Apps, and APIs
- Health Information Technology FAQs

https://www.hhs.gov/hipaa/for-professionals/special-topics/health-apps/index.html

Cloud Guidance

- OCR released guidance clarifying that a Cloud Service Provider (CSP) is a business associate – and therefore required to comply with applicable HIPAA regulations – when the CSP creates, receives, maintains or transmits identifiable health information (referred to in HIPAA as electronic protected health information or ePHI) on behalf of a covered entity or business associate.
- When a CSP stores and/or processes ePHI for a covered entity or business associate, that CSP is a business associate under HIPAA, even if the CSP stores the ePHI in encrypted form and does not have the key.
- CSPs are not likely to be considered "conduits," because their services typically involve storage of ePHI on more than a temporary basis.
- http://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html
- http://www.hhs.gov/hipaa/for-professionals/faq/2074/may-a-business-associate-of-a-hipaa-covered-entity-block-or-terminate-access/index.html

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

Cybersecurity Guidance Material

OCR has a Cybersecurity Guidance Material webpage, including a Cybersecurity Checklist and Infographic, which explain the steps for a HIPAA covered entity or its business associate to take in response to a cyber-related security incident.

- Cybersecurity Checklist - PDF
- Cybersecurity Infographic [GIF 802 KB]

https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html

Cybersecurity Newsletters

- Recent Topics Include:
  - Cybersecurity Authentication
  - Security Incident Procedures
  - Defending Against Common Cyber-Attacks
  - Securing Your Legacy [System Security]
  - Controlling Access to ePHI
  - HIPAA and IT Asset Inventories
  - Preventing, Mitigating, and Responding to Ransomware
  - Advanced Persistent Threats and Zero Day Vulnerabilities
  - Managing Malicious Insider Threats
  - Phishing
- Sign up for the OCR Listserv:

  http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html

Cybersecurity Newsletters

- Recent Topics Include:
  - Cybersecurity Authentication
  - Security Incident Procedures
  - Defending Against Common Cyber-Attacks
  - Securing Your Legacy [System Security]
  - Controlling Access to ePHI
  - HIPAA and IT Asset Inventories
  - Preventing, Mitigating, and Responding to Ransomware
  - Advanced Persistent Threats and Zero Day Vulnerabilities
  - Managing Malicious Insider Threats
  - Phishing
- Sign up for the OCR Listserv:

  http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html

Cybersecurity Newsletters

- Recent Topics Include:
  - Cybersecurity Authentication
  - Security Incident Procedures
  - Defending Against Common Cyber-Attacks
  - Securing Your Legacy [System Security]
  - Controlling Access to ePHI
  - HIPAA and IT Asset Inventories
  - Preventing, Mitigating, and Responding to Ransomware
  - Advanced Persistent Threats and Zero Day Vulnerabilities
  - Managing Malicious Insider Threats
  - Phishing
- Sign up for the OCR Listserv:

  http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html

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

Contact Us

Office for Civil Rights

U.S. Department of Health and Human Services

ocrmail@hhs.gov
www.hhs.gov/ocr

Voice: (800) 368-1019
TDD: (800) 537-7697
Fax: (202) 519-3818

200 Independence Avenue, S.W.
H.H.H Building, Room 509-F
Washington, D.C. 20201

Contact me

steven.mitchell@hhs.gov

(816)426-7278