HIPAA Enforcement Trends

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

UNITED STATES
Department of Health and Human Services
U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
Office for Civil Rights

HIPAA Priorities

- 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 and Update HIPAA Security Rule

Policy

Protecting the Privacy and Security of Your Health Information When Using Your Personal Cell Phone or Tablet Guidance

- The HIPAA Rules generally do not protect the privacy or security of your health information when it is accessed through or stored on your personal cell phones or tablets
- The Guidance provides best practices about steps an individual can take to decrease how their cell phone or tablet collects and shares their health and other personal information without the individual's knowledge
- For example, the Guidance:
  - Explains how to turn off the location services on Apple and Android devices
  - Identifies best practices for selecting apps, browsers, and search engines that are recognized as supporting increased privacy and security

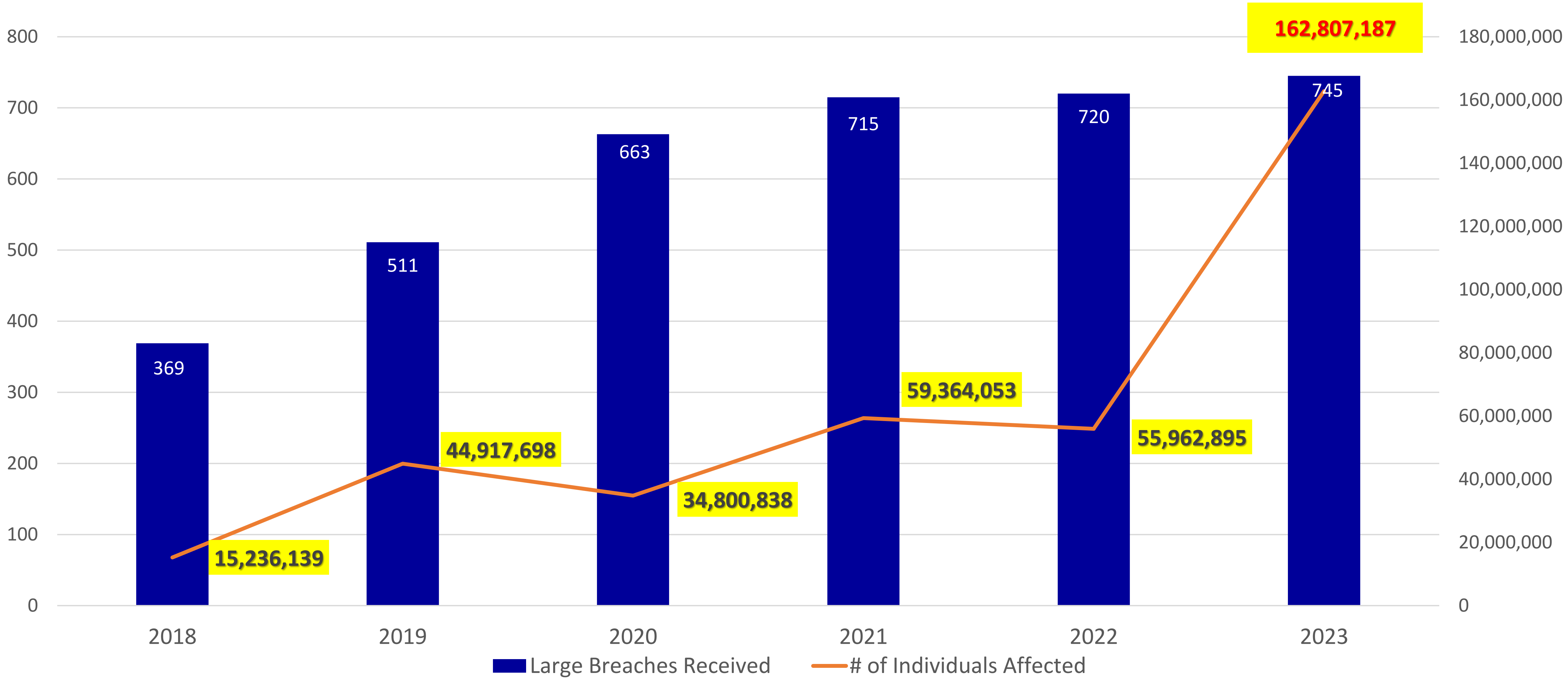
https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/cell-phone-hipaa/index.html

BREACH HIGHLIGHTS AND RECENT ENFORCEMENT ACTIVITY

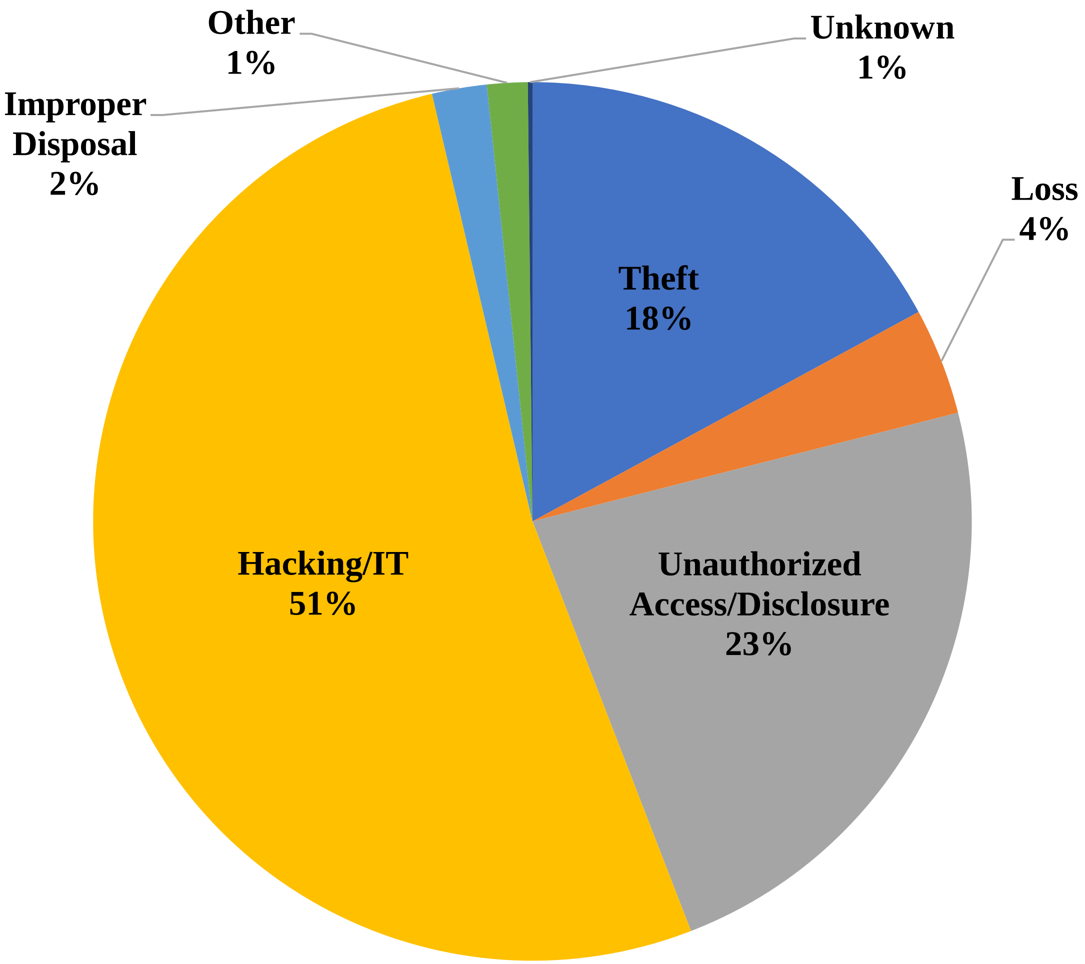
What Happens When OCR Receives a Breach Report

- 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 2023
- 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

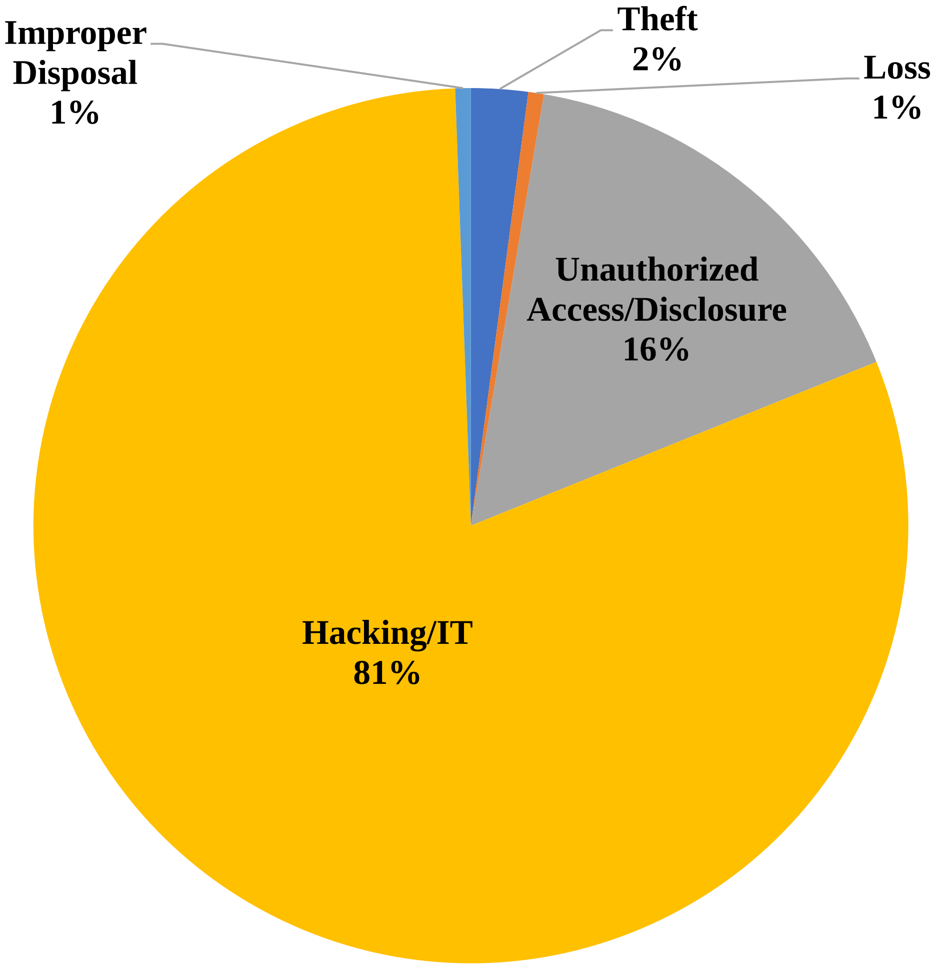
Large Breaches Received and # of Individuals Affected 2018 - 2023



500+ Breaches by Type of Breach

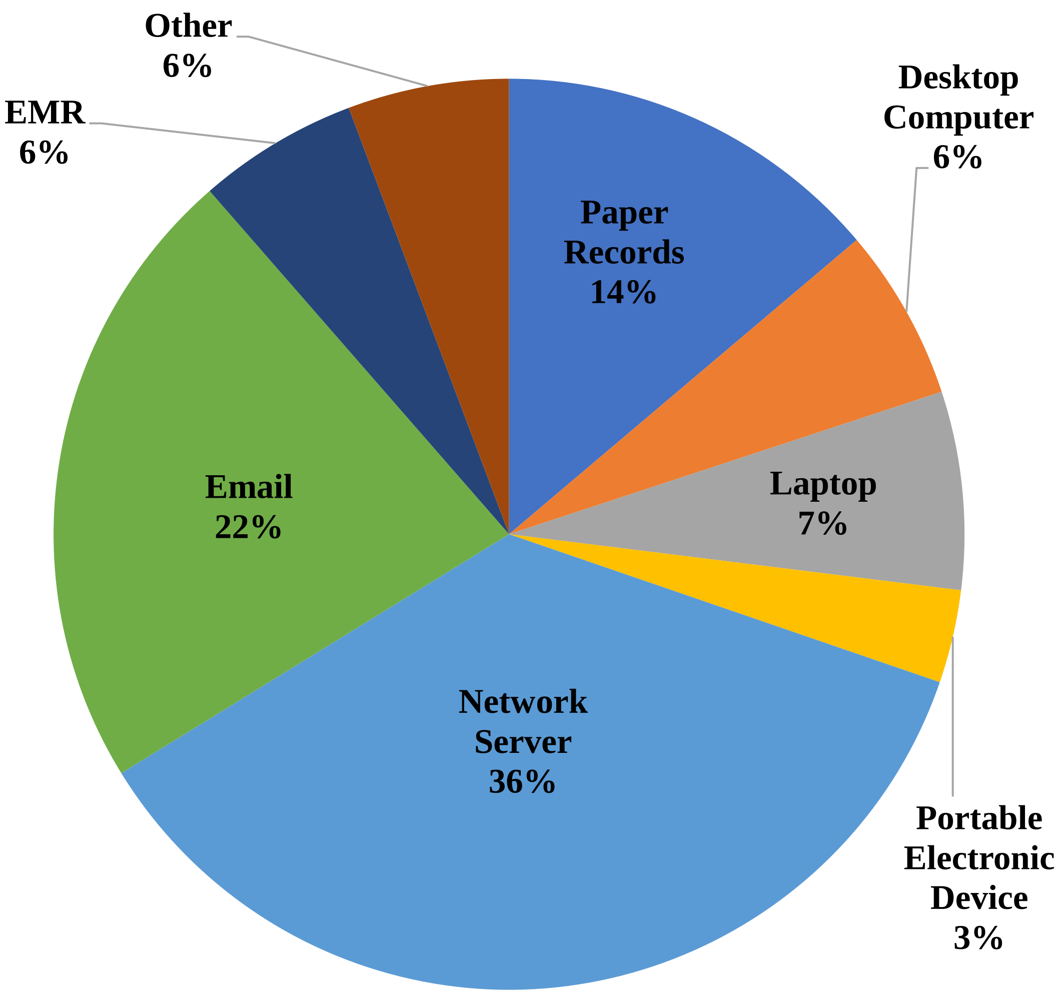


September 23, 2009 through Dec 31, 2023

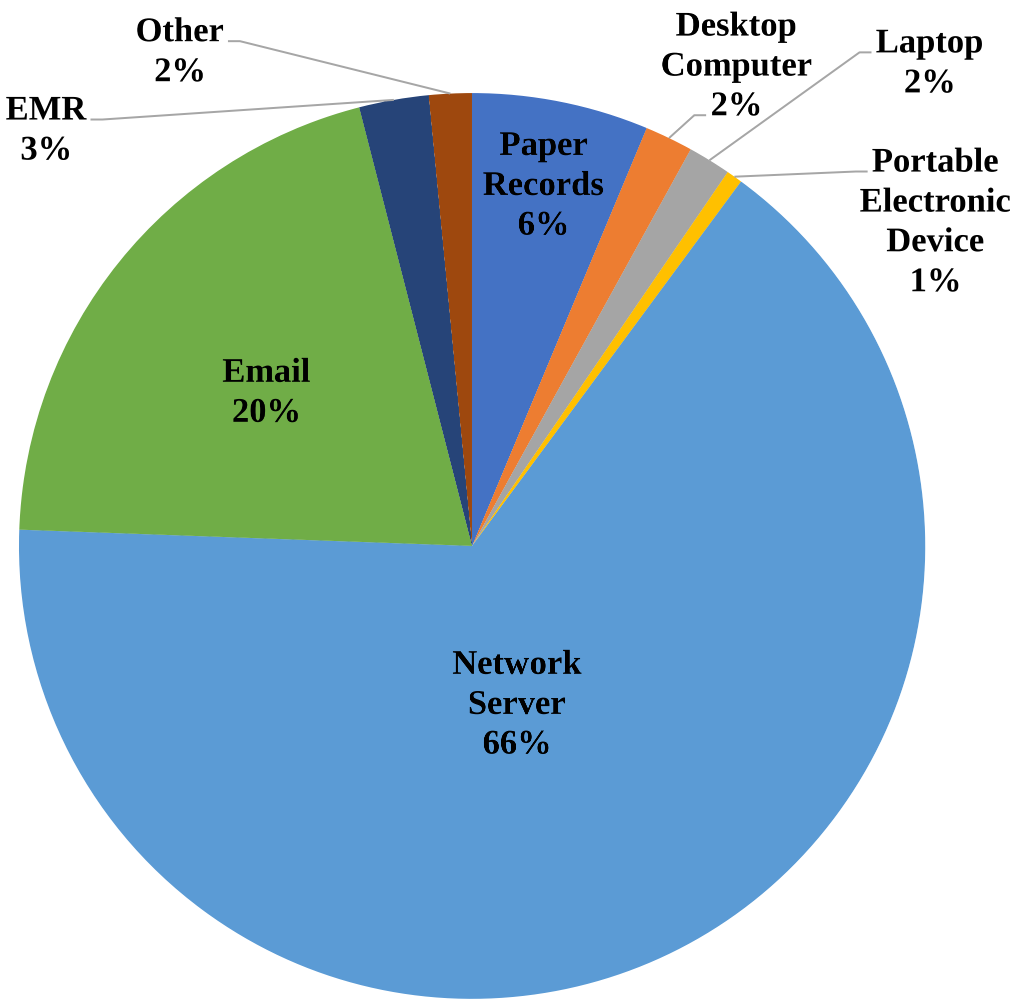


January 1, 2024 through September 30, 2024

500+ Breaches by Location of Breach



September 23, 2009 through Dec 31, 2023

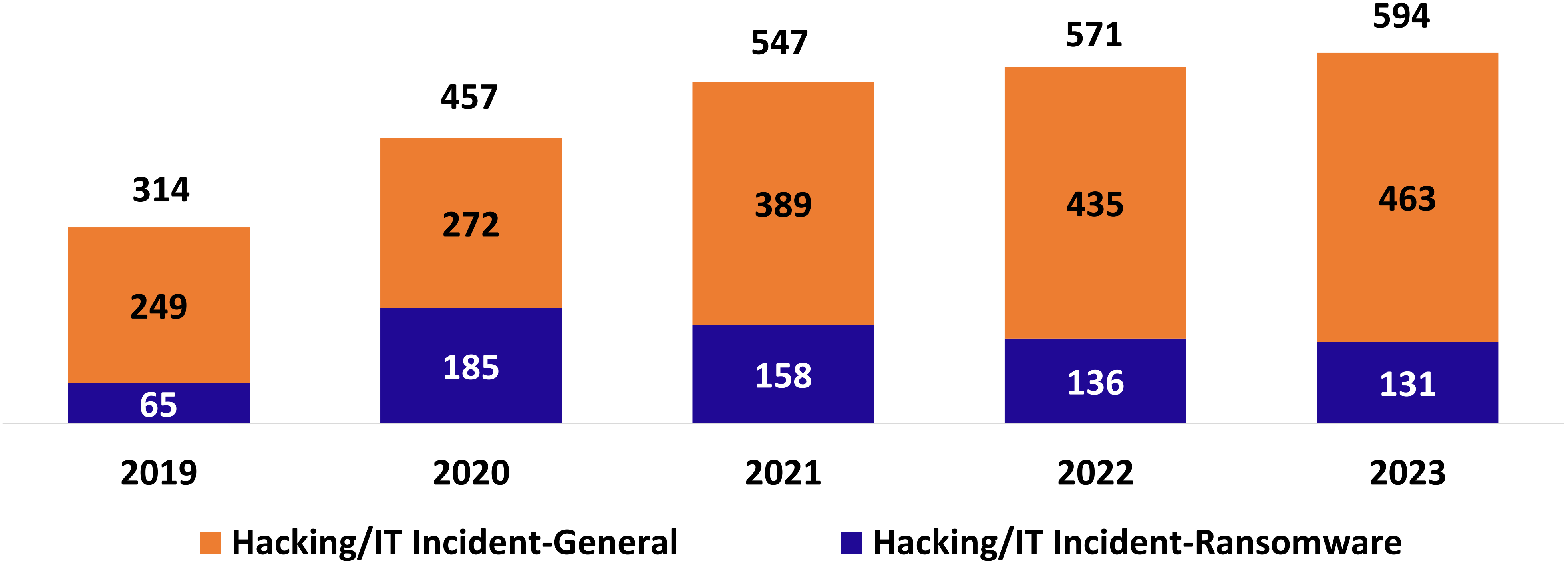


January 1, 2024 through September 30, 2024

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

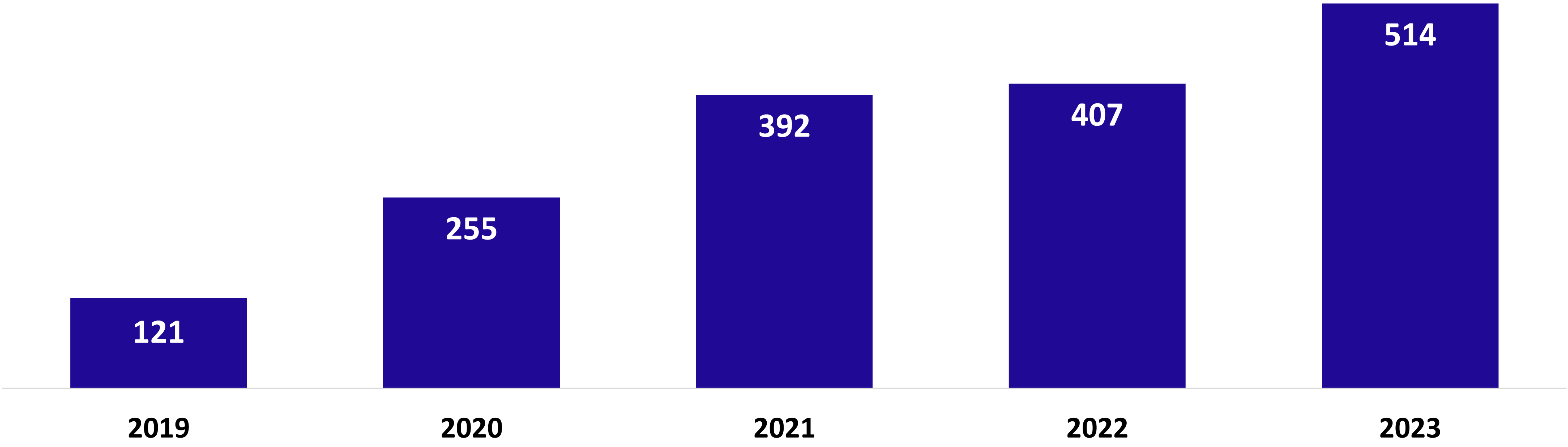
Calendar Years 2019 - 2023

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



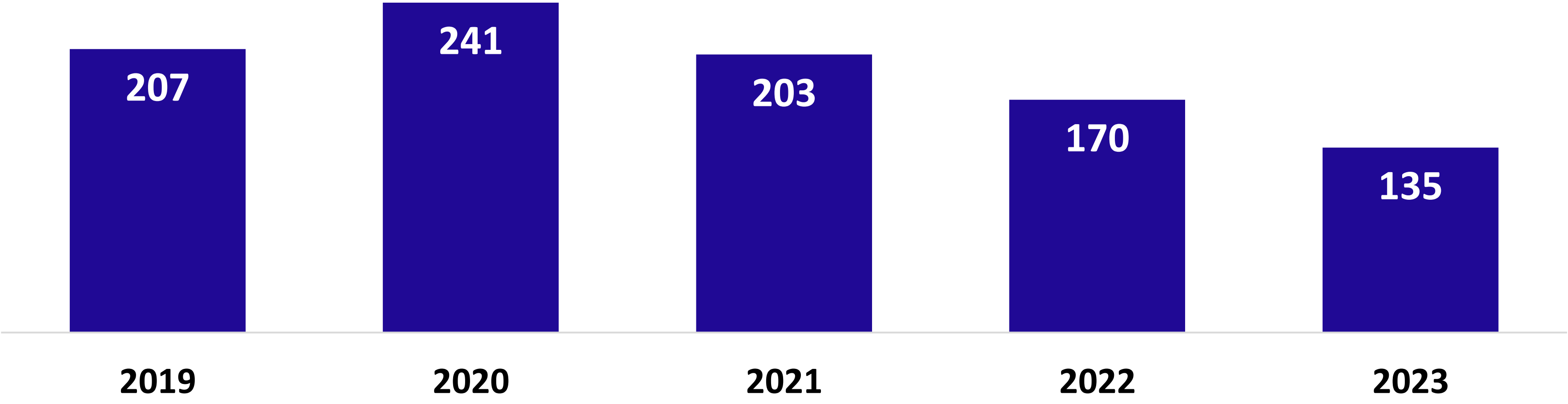
Breaches Affecting 500 or More Individuals
Reports Received of Breaches Involving Network Servers

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
  - 140 settlement agreements that include detailed corrective action plans and monetary settlement amounts
- 12 civil money penalties

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.
  - Investigations launched across the country.
  - To date: forty-five settlements and five CMPs.
- More information on HIPAA right of access available at: https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html

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

Ransomware

- What is ransomware:
  - Ransomware is a type of malicious software (malware) that threatens to deny access to data or a computer system, usually by encrypting it, until the victim pays a ransom fee to the attacker
  - Phishing emails and vulnerability exploitation (e.g., exploiting unpatched operating system or application vulnerabilities) continue to be the most common attack vectors.

- Who is at Risk?
  - Any device connected to the internet risks becoming the next target.

- How can HIPAA help prevent infections of malware/ransomware:
  - security management process, which includes conducting a risk analysis to identify threats and vulnerabilities to electronic protected health information (ePHI) and implementing security measures to mitigate or remediate those identified risks;
  - procedures to guard against and detect malicious software
  - training users on malicious software protection so they can assist in detecting malicious software and know how to report such detections; and
  - access controls to limit access to ePHI to only those requiring access

Indicators of a ransomware attack could include:

- a user's realization that a link that was clicked on, a file attachment opened, or a website visited may have been malicious in nature;

- an increase in activity in the central processing unit (CPU) of a computer and disk activity for no apparent reason (due to the ransomware searching for, encrypting and removing data files);

- an inability to access certain files as the ransomware encrypts, deletes and re-names and/or relocates data; and

- detection of suspicious network communications between the ransomware and the attackers' command and control server(s) (this would most likely be detected by IT personnel via an intrusion detection or similar solution)

Phishing

- One of the most common way for attackers to enter a network or system is through phishing.
- Phishing is a type of cyber-attack used to trick individuals into divulging sensitive information via electronic communication, such as email, by impersonating a trustworthy source.
- Almost half of ransomware attacks involved phishing.
- All regulated entities' workforce members should understand they have an important role in protecting the ePHI their organization holds from cyber-attacks. Part of that role involves being able to detect and take appropriate action if one encounters suspicious email. To ensure workforce members can take appropriate action, regulated entities should train their workforce members to recognize phishing attacks and implement a protocol on what to do when such attacks or suspected attacks occur (*e.g.*, report suspicious emails to appropriate IT personnel).

Recognizing and reporting phishing

Some warning signs that an email might be a phish include:

1) They create a sense of urgency or claim to need help.
2) They ask for your personal info.
3) They want you to download a file or click on a link.

Cybercriminals are crafty and may send emails that look legit but aim to steal your information. Trust your gut, stay cautious, and report those phishing emails. Think before you click! For more tips on avoiding phishing scams, visit the CyberCARE homepage.

Prevention

- The Security Rule requires regulated entities to implement a security awareness and training program for all workforce members.
- A regulated entity’s training program should be an ongoing, evolving process and be flexible enough to educate workforce members on new and current cybersecurity threats (*e.g.*, ransomware, phishing) and how to respond.
- Management personnel should also participate, as senior executives may have greater access to ePHI and are often targeted in phishing email attacks.
- In addition to education, regulated entities can mitigate the risk of phishing attacks by implementing anti-phishing technologies.

Recovery/Mitigation

- Contingency planning is key!
    - Contingency planning ensures healthcare organizations return to normal operations as quickly as possible and the confidentiality, integrity, and availability of PHI is safeguarded.
- Because ransomware denies access to data, maintaining **frequent backups** and ensuring the ability to recover data from backups is crucial to recovering from a ransomware attack.
    - Test restorations should be periodically conducted to verify the integrity of backed up data and provide confidence in an organization's data restoration capabilities.
    - Consider maintaining backups offline and unavailable from their networks
- Backup logs should be reviewed regularly, and test restorations of backups conducted periodically
- Because some malware, including some ransomware variants, are known to delete or otherwise disrupt online backups, regulated entities should consider maintaining at least some of their backups offline and unavailable from their networks.

Security Incident Procedures

- in some cases, an entity’s workforce may notice early indications of a ransomware attack that has evaded the entity’s security measures
- Identifying and responding to suspected security incidents is crucial to mitigating potential harm following an intrusion.
- Quick isolation and removal of infected devices from the network and deployment of anti-malware tools can help to stop the spread of ransomware and to reduce the harmful effects of such ransomware.
- Response procedures should be written with sufficient details and be disseminated to proper workforce members so that they can be implemented and executed effectively.
- organizations may consider testing their security incident procedures from time to time to ensure they remain effective.

Examples of Security Incident Procedures

- Designating appropriate personnel (qualified internal resources and/or external third parties) to be members of the security incident response team
- A communication plan and contact information for notifying all members of the security incident response team, and others as required (*e.g.*, management) when a security incident occurs
- Processes to identify and determine the scope of security incidents
- Instructions for managing the security incident
- Creating and maintaining a list of assets (computer systems and data) to prioritize when responding to a security incident
- Conducting a forensic analysis to identify the extent and magnitude of the security incident
- Reporting the security incident to appropriate internal and external entities (*e.g.*, the regulated entity's IT and legal departments, local FBI Cyber Taskforce Field Office, federal and state regulatory authorities, and other individuals or entities as required)
- Processes for collecting and maintaining evidence of the security incident (*e.g.*, log files, registry keys, and other artifacts) to determine what was accessed during the security incident
- Processes for conducting regular tests of the security incident response process

Access Controls

- Implementing effective access controls (see 45 C.F.R. § 164.312(a)(1) (access control)) to stop or impede an attacker's movements and access to sensitive data; e.g., by segmenting networks to limit unauthorized access and communications. (Limiting access to ePHI to only those persons or software programs requiring access)
- Because attacks frequently seek elevated privileges (e.g., administrator access), entities may consider solutions that limit the scope of administrator access, as well as solutions requiring stronger authentication mechanisms when granting elevated privileges or access to administrator accounts.

My entity just experienced a cyber-attack! What do we do now?

- Execute response and reporting and contingency plans
- Report crime to criminal law enforcement
- If it is determined to be a breach:
  - Must report the breach to OCR as soon as possible, but no later than 60 days after the discovery of a breach affecting 500 or more individuals and notify affected individuals and the media unless a law enforcement official has requested a delay in the reporting. OCR presumes all cyber-related security incidents where protected health information was accessed, acquired, used, or disclosed are reportable breaches unless the information was encrypted by the entity at the time of the incident or the entity determines, through a written risk assessment, that there was a low probability that the information was compromised during the breach.

General 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

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

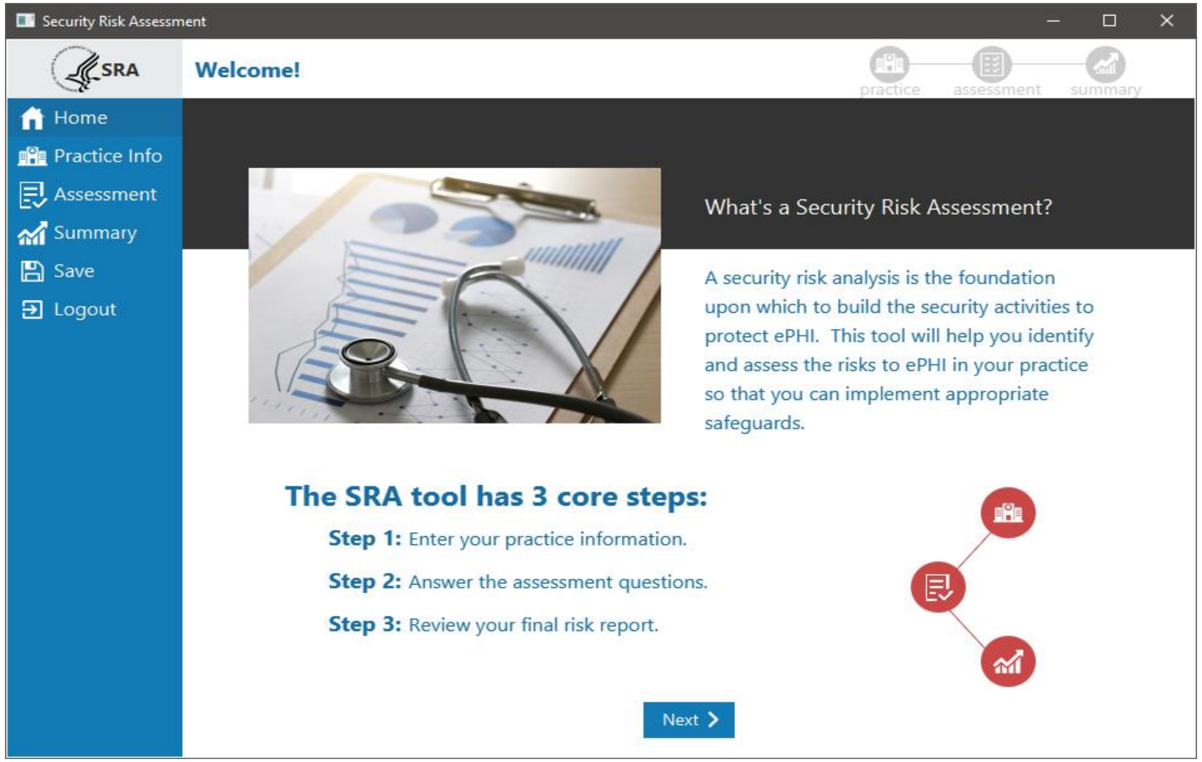
The video may be found on OCR's YouTube channel at: https://www.youtube.com/watch?v=hxfxhokzKEU

OCR Ransomware and the HIPAA Security Rule Video

- Updates 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.
- Topics covered include:
  - OCR breach and ransomware trend analysis
  - Review of prior OCR ransomware guidance and materials
  - Analysis of the ransomware attack chain
  - Explore how Security Rule compliance can combat ransomware

The video may be found on OCR’s YouTube channel at: https://www.youtube.com/watch?v=nBKUIAy1OFA

SRA Tool



What's a Security Risk Assessment?

A security risk analysis is the foundation upon which to build the security activities to protect ePHI. This tool will help you identify and assess the risks to ePHI in your practice so that you can implement appropriate safeguards.

The SRA tool has 3 core steps:

Step 1: Enter your practice information.

Step 2: Answer the assessment questions.

Step 3: Review your final risk report.

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.

Cybersecurity Newsletters

- Recent Topics Include:
  - Facility Access Controls
  - Sanction Policies
  - 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
- Sign up for the OCR Listserv: http://www.hhs.gov/hipaa/for-professionals/security/guidance/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/topics/cybersecurity-best-practices/healthcare

FBI Resources:

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

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
Office for Civil Rights

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

UNITED STATES
Department of Health and Human Services
U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
Office for Civil Rights

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