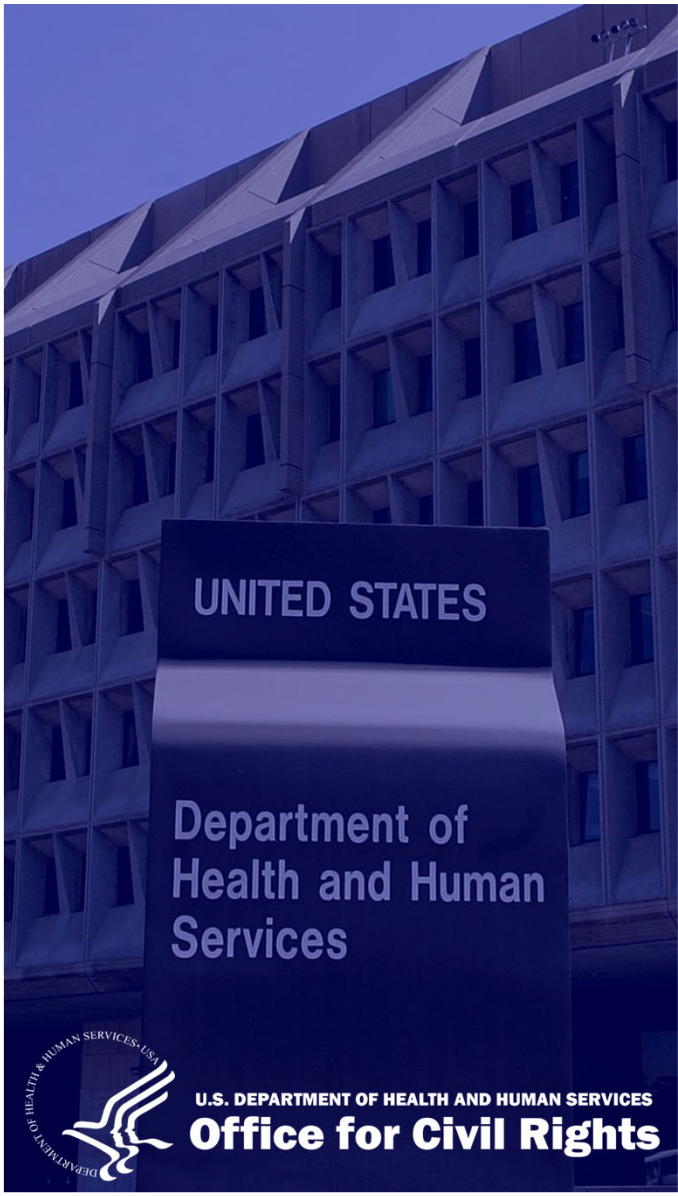
# Office for Civil Rights (OCR)
# U.S. Department of Health and Human Services



# What Is the Office for Civil Rights (OCR)?

- Part of the U.S. Department of Health and Human Services.
- Enforces a number of civil rights laws as they relate to recipients of Federal financial assistance (FFA) from HHS, public entities, and programs & activities conducted by HHS.
- Only Federal agency in charge of enforcing the HIPAA Privacy, Security, and Breach Notification Rules.
- Headquarters in D.C. supported by regional offices.

# Who We Are and What We Do

- OCR is the Department's civil rights, and health information privacy rights law enforcement agency.

- OCR's responsibilities include:
  - investigating complaints from the public;
  - initiating compliance reviews;
  - securing voluntary corrective action;
  - providing technical assistance;
  - conducting public outreach; and
  - issuing regulations and guidance.

# Complaint Process

- Informal review may resolve issue fully without formal investigation
  - Many complaints will be resolved at this stage
- If not, begin investigation
  - Voluntary resolution may be possible through
    - Education
    - Training
- Technical Assistance
- Some cases may require formal enforcement

# HIPAA Privacy Rule Overview

# Scope: Who is Covered?

Limited by HIPAA to:

- Covered entities (CE)
  - Health care providers who transmit health information electronically in connection with a transaction for which there is a HIPAA standard (e.g., billing insurance electronically)
  - Health plans
  - Health care clearinghouses
- Business associates (BA)

# Scope: What is Covered?

- Protected Health Information (PHI):
  - Individually identifiable health information (IIHI)
  - Transmitted or maintained in any form or medium
- Not PHI:
  - De-identified information
  - Employment records
  - Family Educational Rights and Privacy Act (FERPA) education records

# Uses and Disclosures: Key Points

- No use or disclosure of PHI unless permitted or required by the Privacy Rule
- *Required* Disclosures:
  - To the individual who is the subject of the PHI
  - To the Secretary of HHS in order to determine compliance
- All other uses and disclosures in the Privacy Rule are *permissive*
- Covered entities may provide greater protections

# Permitted Uses and Disclosures

Examples (conditions apply):

- To the individual or personal representative
- For treatment, payment, and health care operations (TPO)
- With the opportunity to agree or object
- For specific public priorities
- “Incident to” a permitted use or disclosure
- Limited data sets, with a data use agreement
- As authorized by the individual

# Administrative Requirements

- Covered entities must:
  - Designate a Privacy Officer
  - Designate a contact person or office to receive complaints and provide further information
  - Provide privacy training to all workforce members
  - Develop and apply sanction policy for workforce members who fail to comply
  - Implement policies and procedures designed to comply with standards

# Administrative Requirements (cont.)

- Covered entities must:
  - Implement administrative, technical, and physical safeguards to protect privacy of PHI
  - Mitigate any harmful effect of a violation known to the covered entity to the extent practicable
  - Provide an internal complaint process for individuals
  - Refrain from intimidating and retaliatory acts
  - Not require individuals to waive their rights

# Compliance Challenges

# 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.

# 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).*

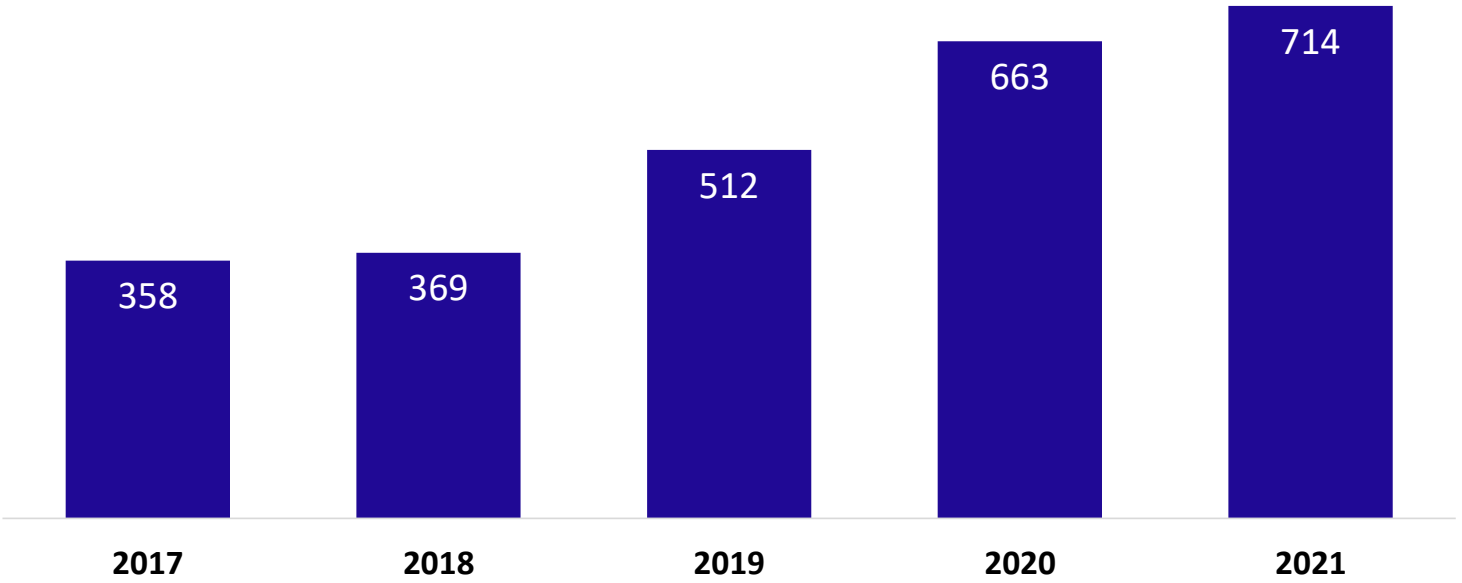
# BREACH HIGHLIGHTS AND RECENT ENFORCEMENT ACTIVITY

# What Happens When OCR Receives a Breach Report

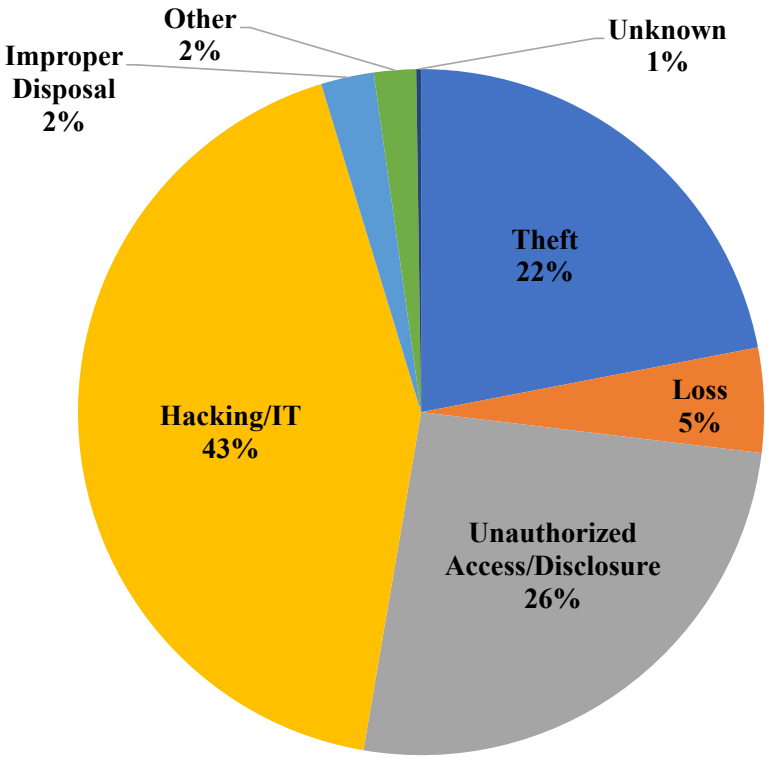
- OCR posts breaches affecting 500+ individuals on OCR website (after verification of report)
  - Public can search and sort posted breaches
  - Received over 700 breach reports affecting 500+ individuals in 2021
- OCR opens investigations into breaches affecting 500+ individuals, and into a number of 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

# Breaches Affecting 500 or More Individuals
# Reports Received by Year

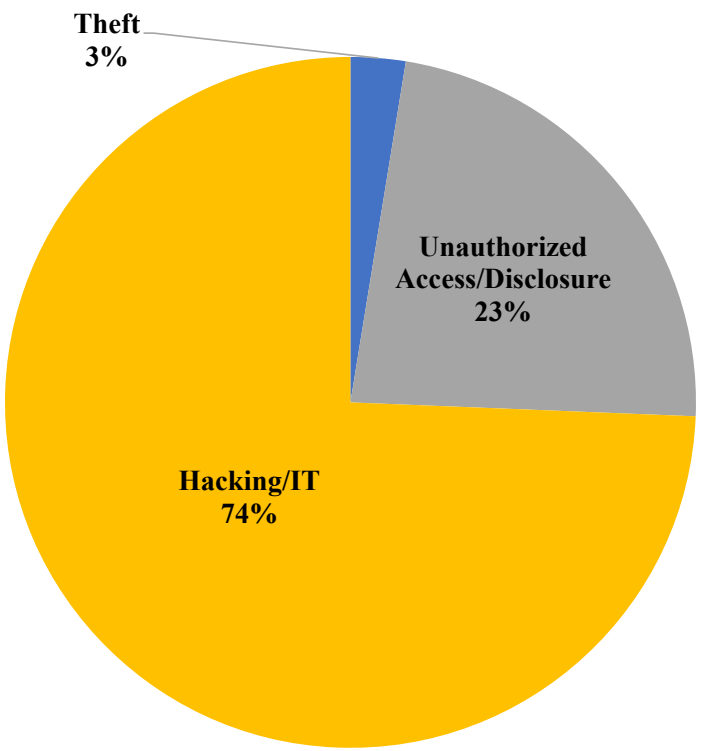
Calendar Years 2017 - 2021



# 500+ Breaches by Type of Breach

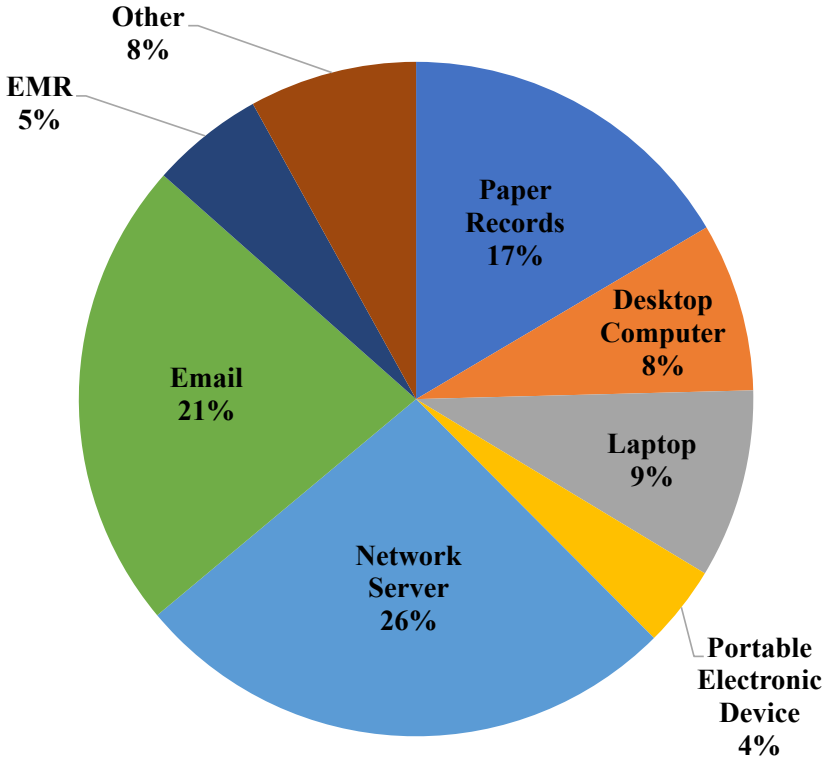



September 23, 2009 through Dec 31, 2021

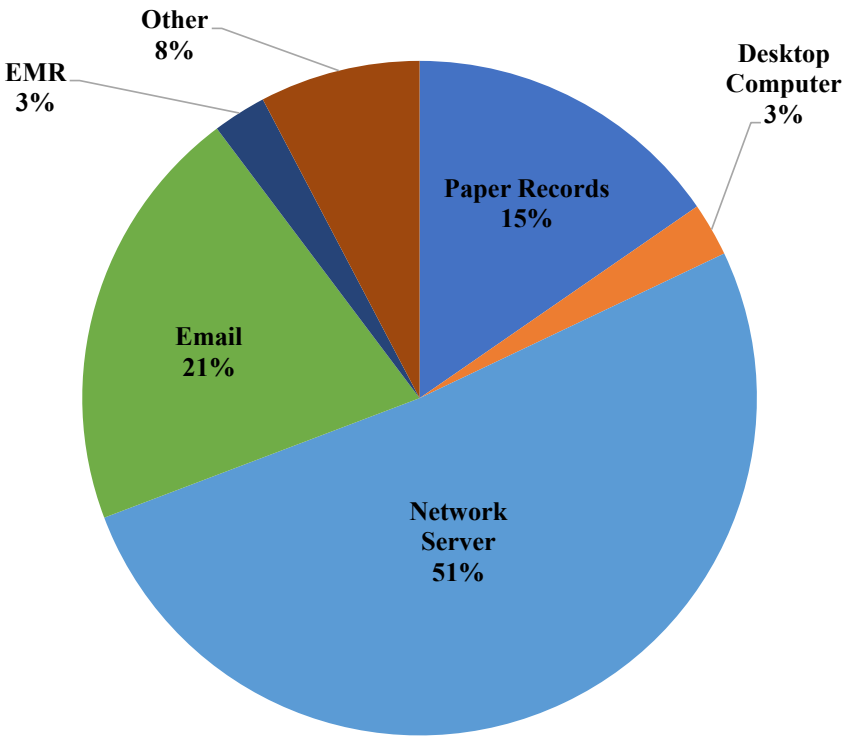



January 1, 2022 through January 31, 2022

# 500+ Breaches by Location of Breach



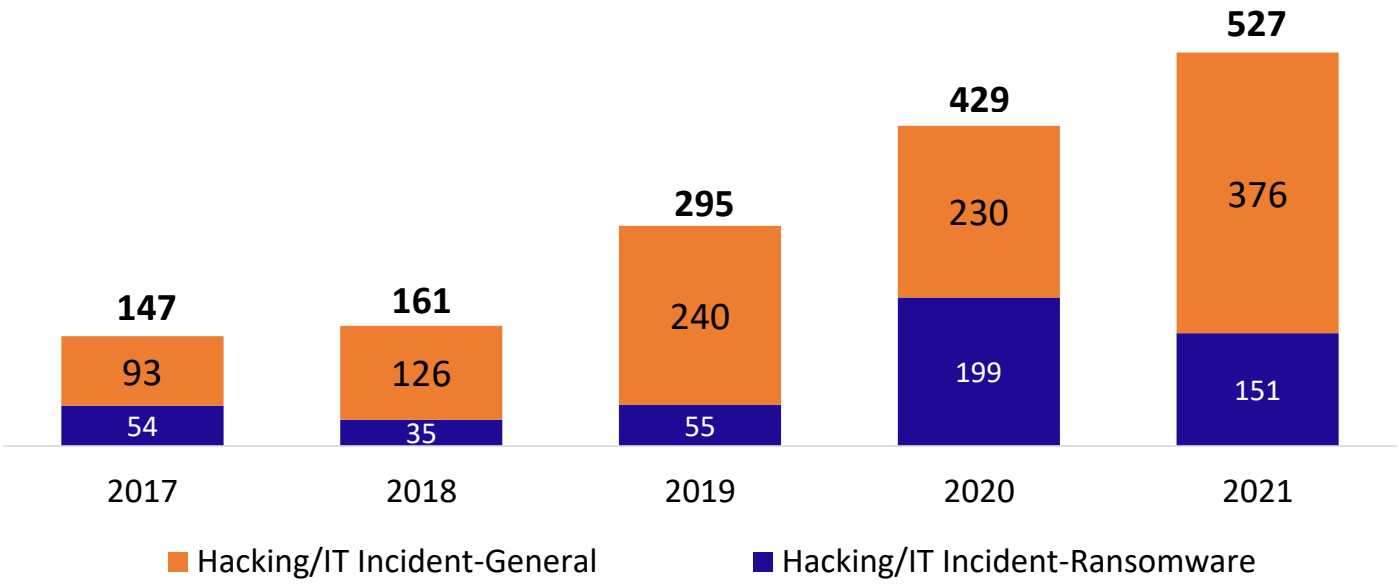

September 23, 2009 through Dec 31, 2021




January 1, 2022 through January 31, 2022

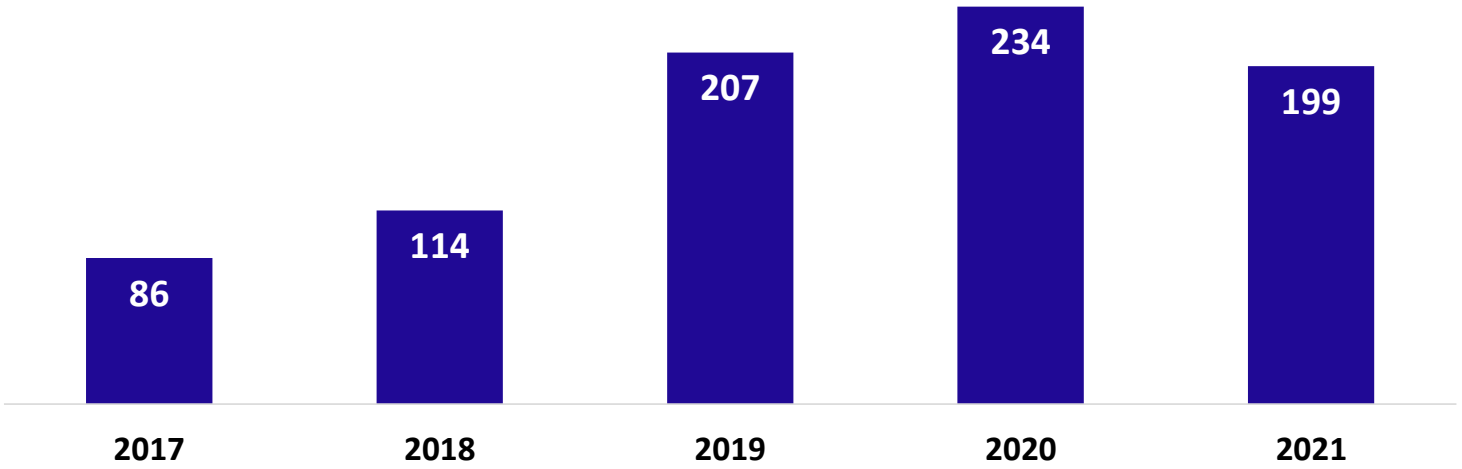
# Breaches Affecting 500 or More Individuals
# Reports Received Involving Hacking/IT Incidents

Calendar Years 2017 - 2021



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

Calendar Years 2017 - 2021



# General HIPAA Enforcement Highlights

- OCR expects to receive over 28,000 complaints this year.
- 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
  - 100 settlement agreements that include detailed corrective action plans and monetary settlement amounts
- 6 civil money penalties

**As of January 31, 2022**

# Recurring HIPAA Compliance Issues

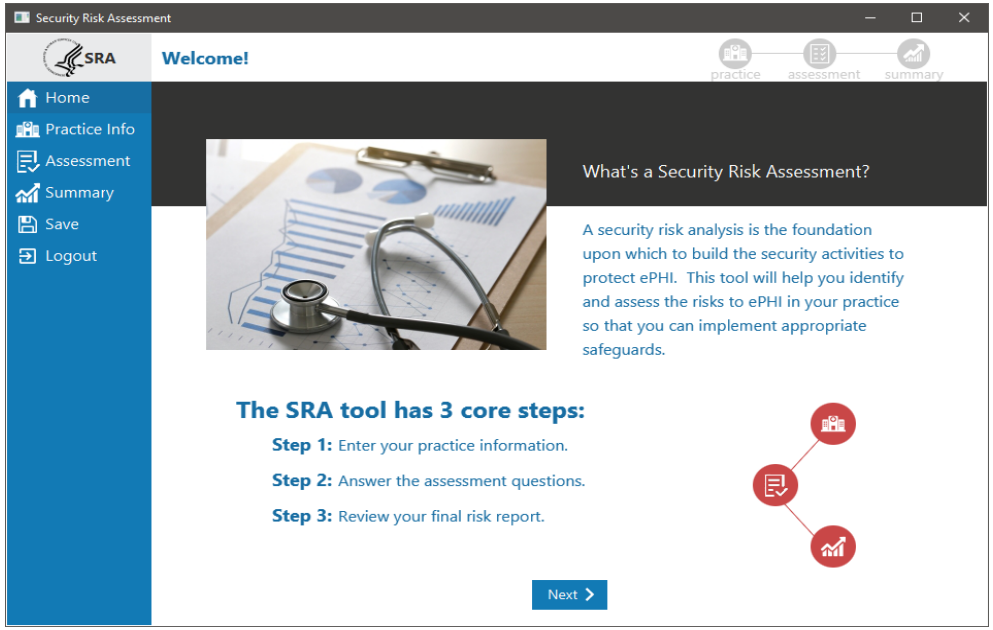
- Business Associate Agreements
- Risk Analysis
- Failure to Manage Identified Risk, e.g. Encrypt
- Lack of Transmission Security
- Lack of Appropriate Auditing
- No Patching of Software
- Insider Threat
- Improper Disposal
- Insufficient Data Backup and Contingency Planning
- Individual Right to Access

# Best Practices

## Some 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

# 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.

# Cybersecurity Newsletters

- Recent Topics Include:
  - 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
  - Software Vulnerabilities and Patching
  - Securing Electronic Media and Devices
- 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

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

- Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients https://www.phe.gov/Preparedness/planning/405d/Pages/hic-practices.aspx
- Cybersecurity Reports and Tools https://www.phe.gov/Preparedness/planning/405d/Pages/reportandtools.aspx

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


# 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