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

Agenda

- Tracking Technologies
- Ransomware
- Recognizing suspicious activity
- Mitigation strategies
- Recent Enforcement Trends
- Best practices
- Questions

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

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 ransomware victim.

- 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)

Recognizing and reporting phshing

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.

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.

Security incident procedure examples

- 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.

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

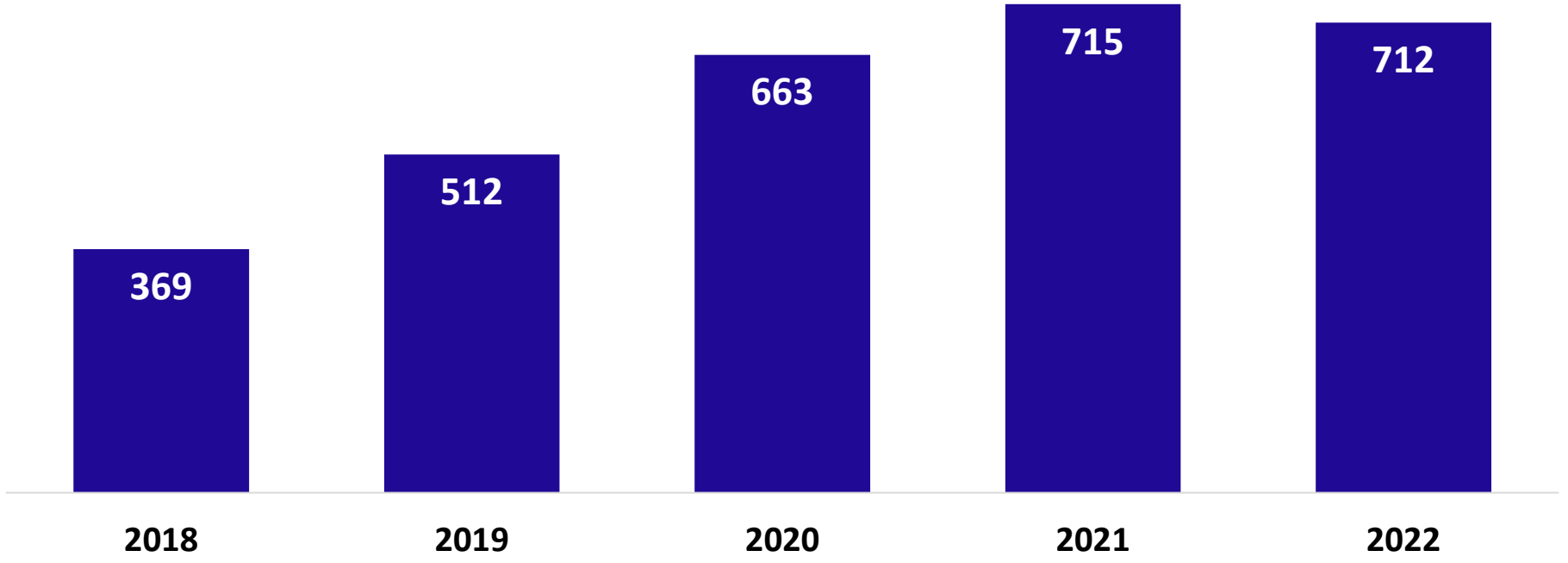
BREACH HIGHLIGHTS AND RECENT ENFORCEMENT ACTIVITY

What Happens When OCR Receives a Breach Report

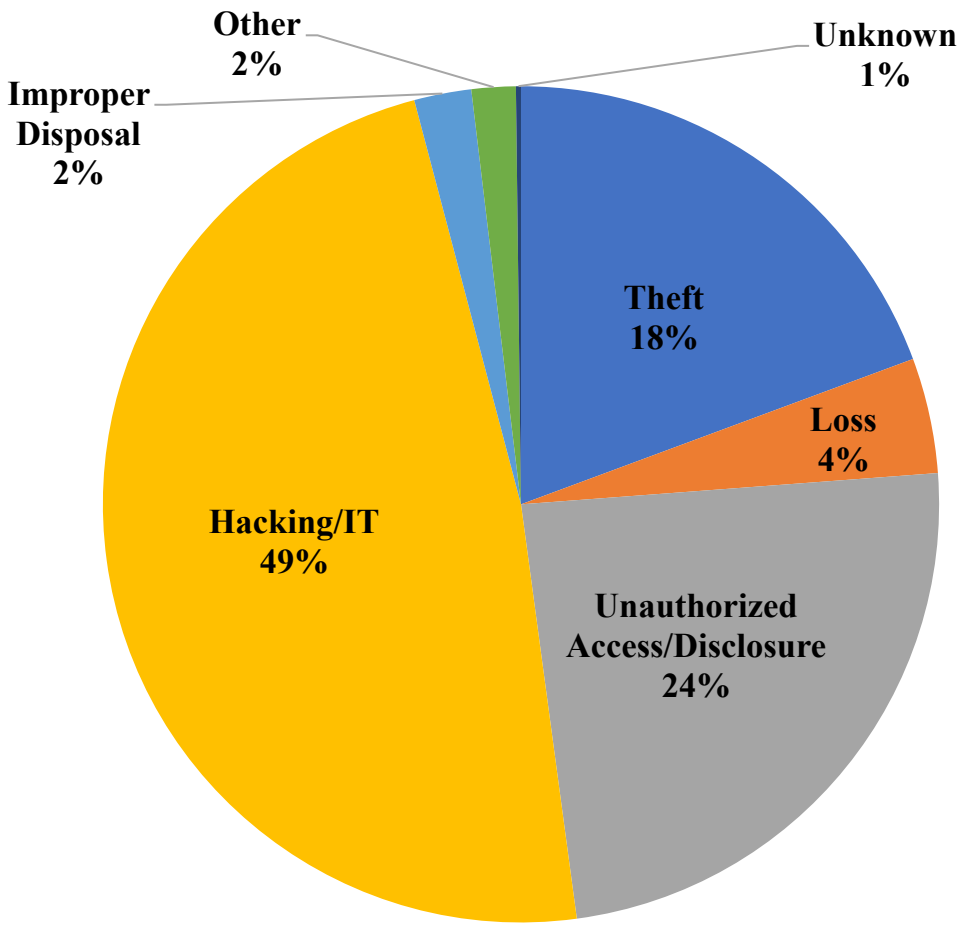
- OCR posts breaches affecting 500+ individuals on OCR website (after verification of report)
  - Public can search and sort posted breaches
  - Received over 700 breach reports affecting 500+ individuals in 2022
- OCR opens investigations into breaches affecting 500+ individuals, and into a number of 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

Breaches Affecting 500 or more Individuals
Reports Received by Year

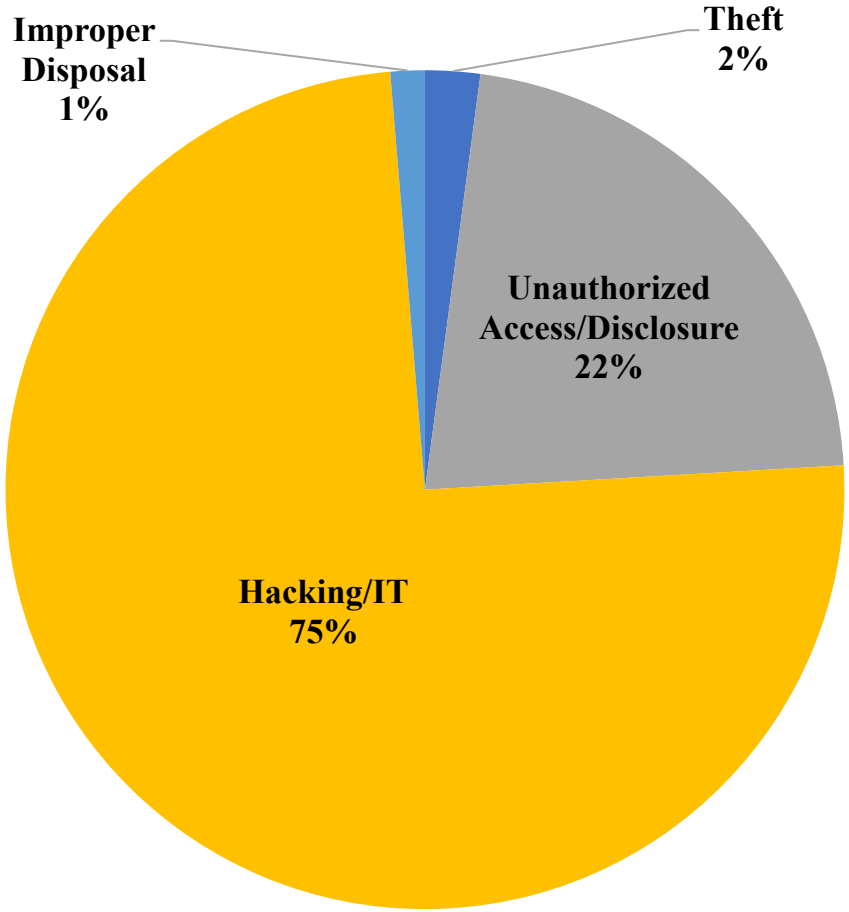
Calendar Years 2018 - 2022



500+ Breaches by Type of Breach

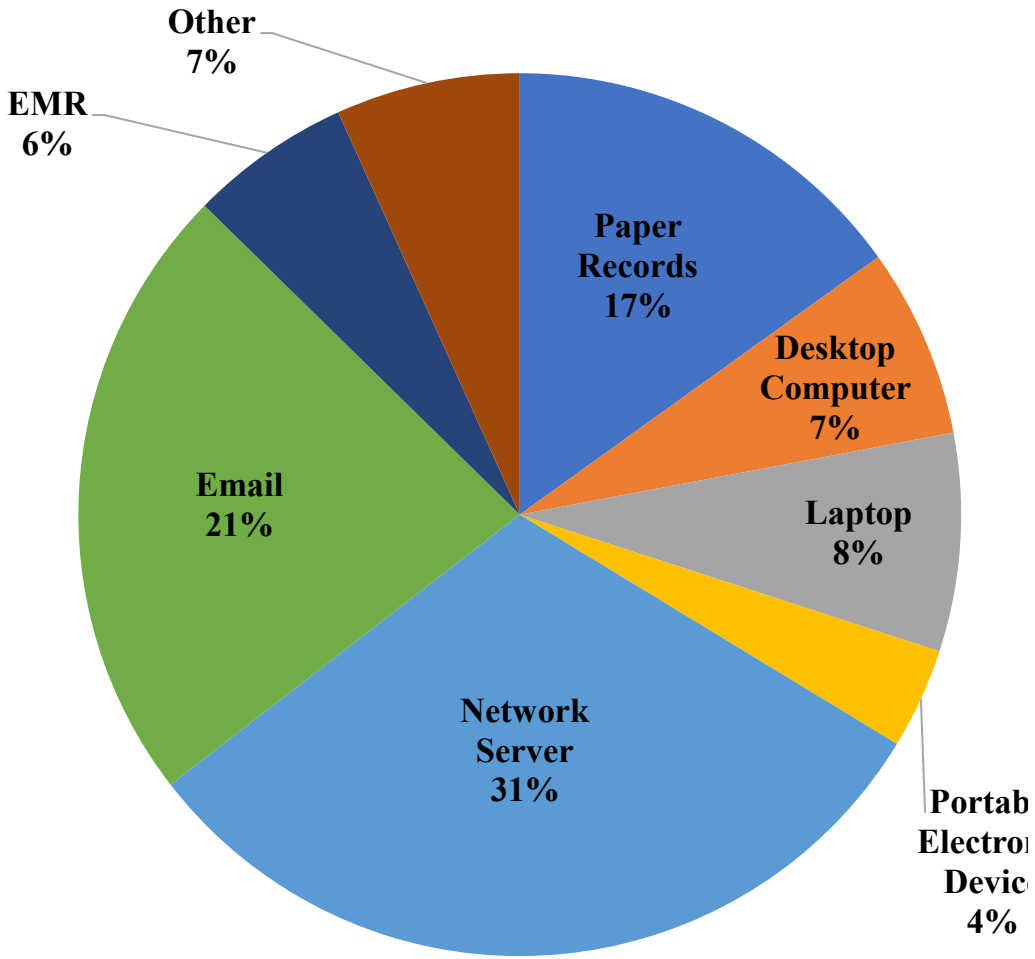


September 23, 2009 through Dec 31, 2022

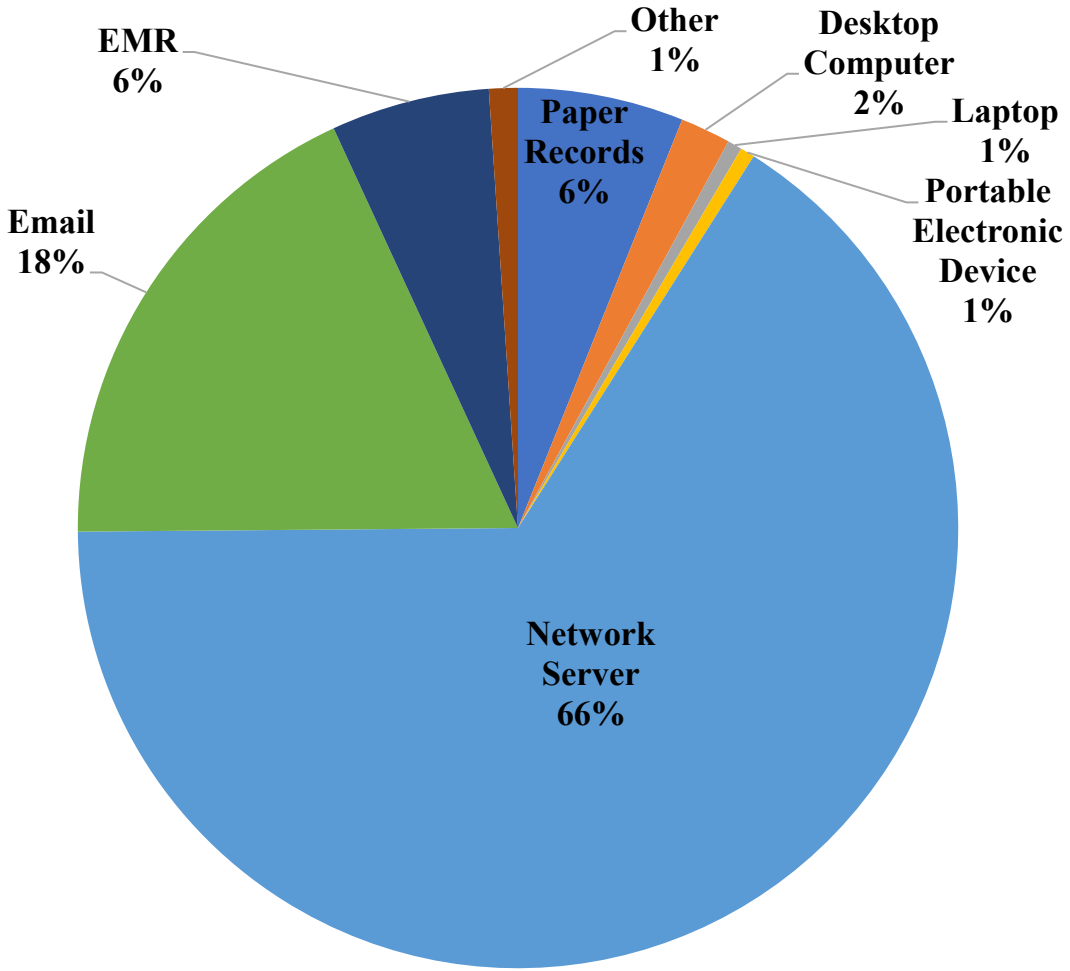


January 1, 2023 through July 31, 2023

500+ Breaches by Location of Breach



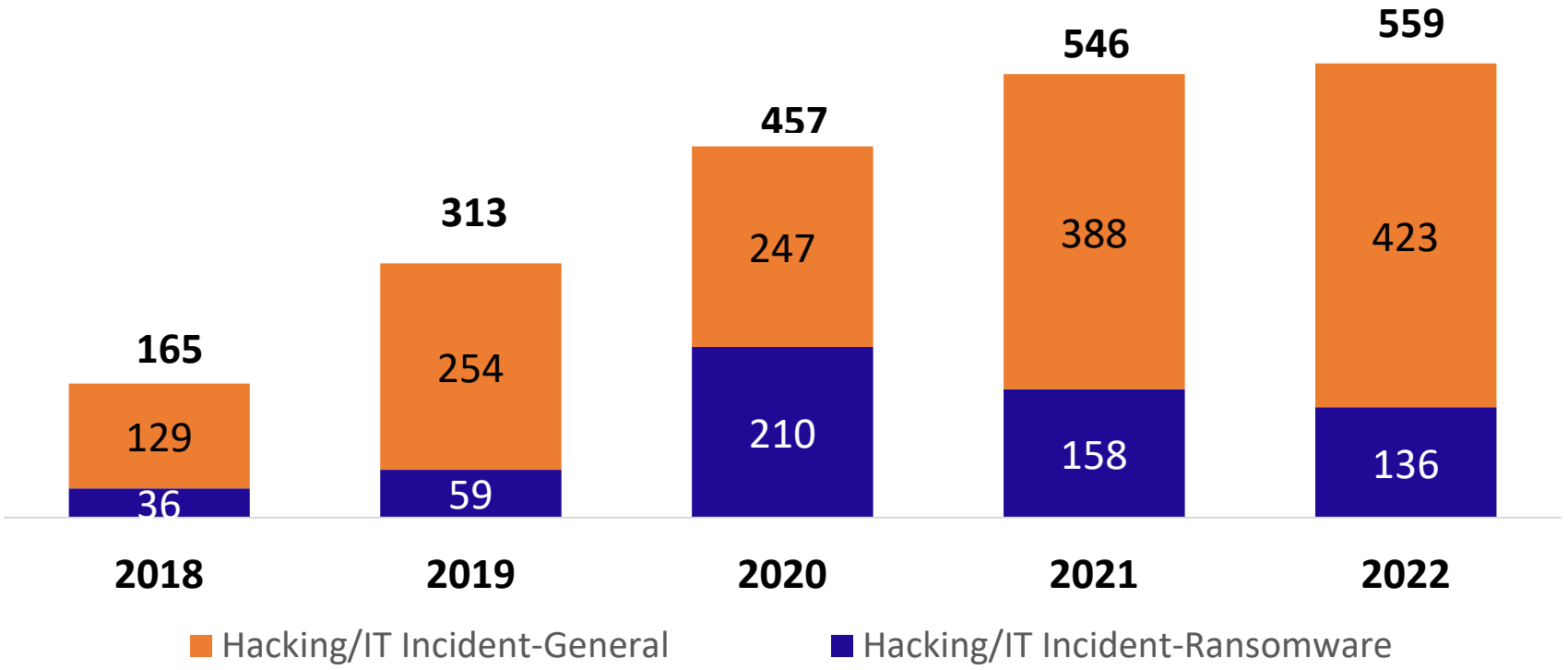
September 23, 2009 through Dec 31, 2022



January 1, 2023 through July 31, 2023

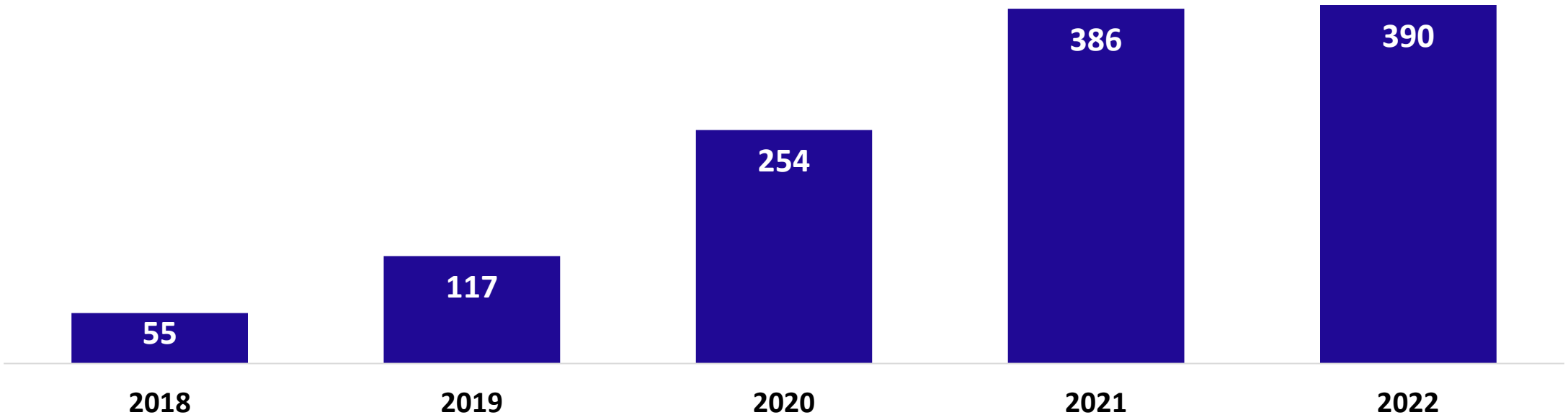
Breaches Affecting 500 or More Individuals
Reports Received Involving Hacking/IT Incidents

Calendar Years 2018 - 2022



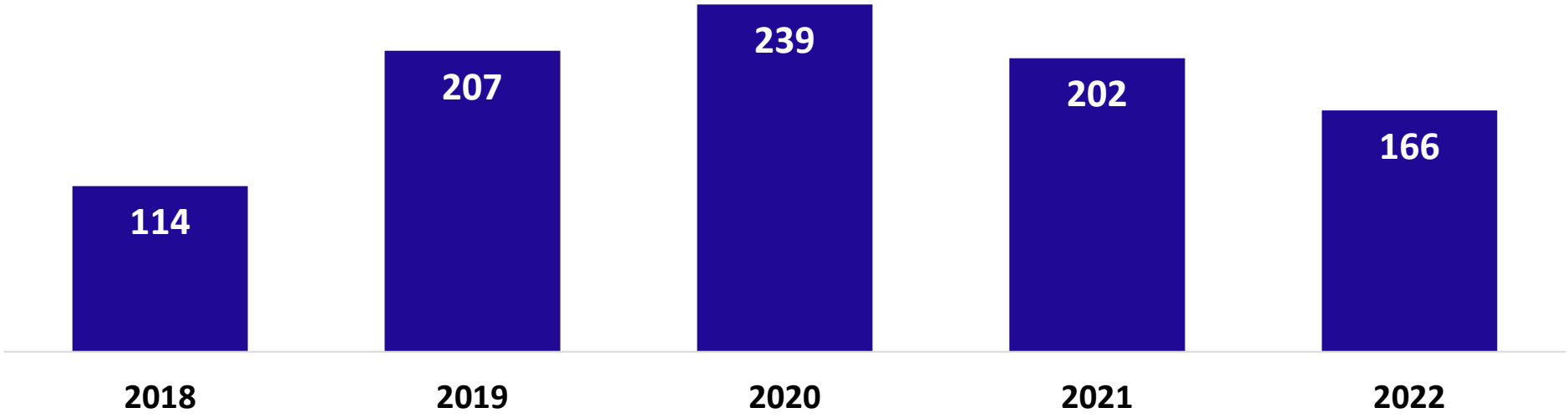
Breaches Affecting 500 or More Individuals
Reports Received of Breaches Involving Network Servers

Calendar Years 2018 - 2022



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

Calendar Years 2018 - 2022



General HIPAA Enforcement Highlights

- OCR expects to receive over 33,000 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
  - 128 settlement agreements that include detailed corrective action plans and monetary settlement amounts
- 8 civil money penalties

Recent OCR HIPAA Enforcement Actions

July-22	ACPM Podiatry	$100,000 **(CMP)**
July-22	Associated Retina Specialists	$22,500
July-22	Lawrence Bell Jr., D.D.S	$5,000
July-22	Coastal Ear, Nose, and Throat	$20,000
July-22	Danbury Psychiatric Consultants	$3,500
July-22	Erie County Medical Center Corporation	$50,000
July-22	Fallbrook Family Health Center	$30,000
July-22	Hillcrest Commons Nursing and Rehabilitation	$55,000
July-22	Melrose Wakefield Healthcare	$55,000
July-22	Memorial Hermann Health System	$240,000
July-22	Southwest Surgical Associates	$65,000
July-22	Oklahoma State University	$875,000
Aug-22	New England Dermatology and Laser Center	$300,640
Sep-22	Family Dental	$30,000
Sep-22	Great Expressions Dental Center of Georgia	$80,000
Sep-22	Paradise Family Dental	$25,000
Dec-22	New Vision Dental	$23,000
Dec-22	Health Care Specialists of Central Florida	$20,000
Dec-22	Life Hope Labs	$16,500
Jan-23	Banner Health	$1,250,000
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

Recurring HIPAA Compliance Issues

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

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

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