HIPAA Update from the Office for Civil Rights

Timothy Noonan
Deputy Director for Health Information Privacy, Data, and Cybersecurity
HHS Office for Civil Rights

Agenda

- Rulemaking and Guidance
- Trends in Health Data Breach Reporting
- Recent HIPAA Enforcement Activity

Rulemaking and Guidance

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 working on a Final Rule.

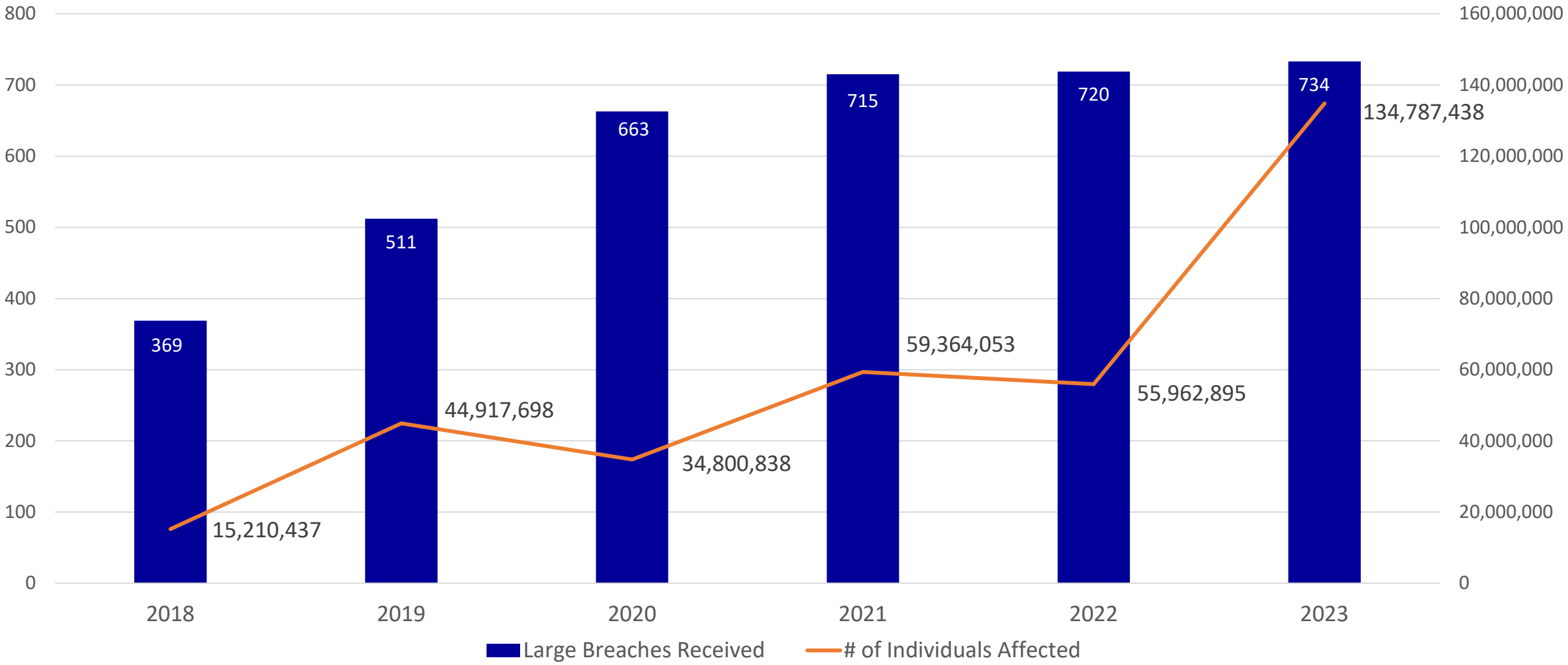
HIPAA and The Use of Online Tracking Technologies Bulletin

- Updated on March 18, 2024.
- Reminds regulated entities that they can use online tracking technologies provided that the entities comply with their obligations under the HIPAA Rules.
- Explains what tracking technologies are, how they are used, and a general overview of how the HIPAA Rules apply to regulated entities' use of tracking technologies. Updates include:
  - New examples of when visits to an unauthenticated webpage may or may not involve the disclosure of ePHI.
  - Additional tips for complying with the HIPAA Rules when using online tracking technologies.
  - Guidance about OCR's enforcement priorities in online tracking investigations.

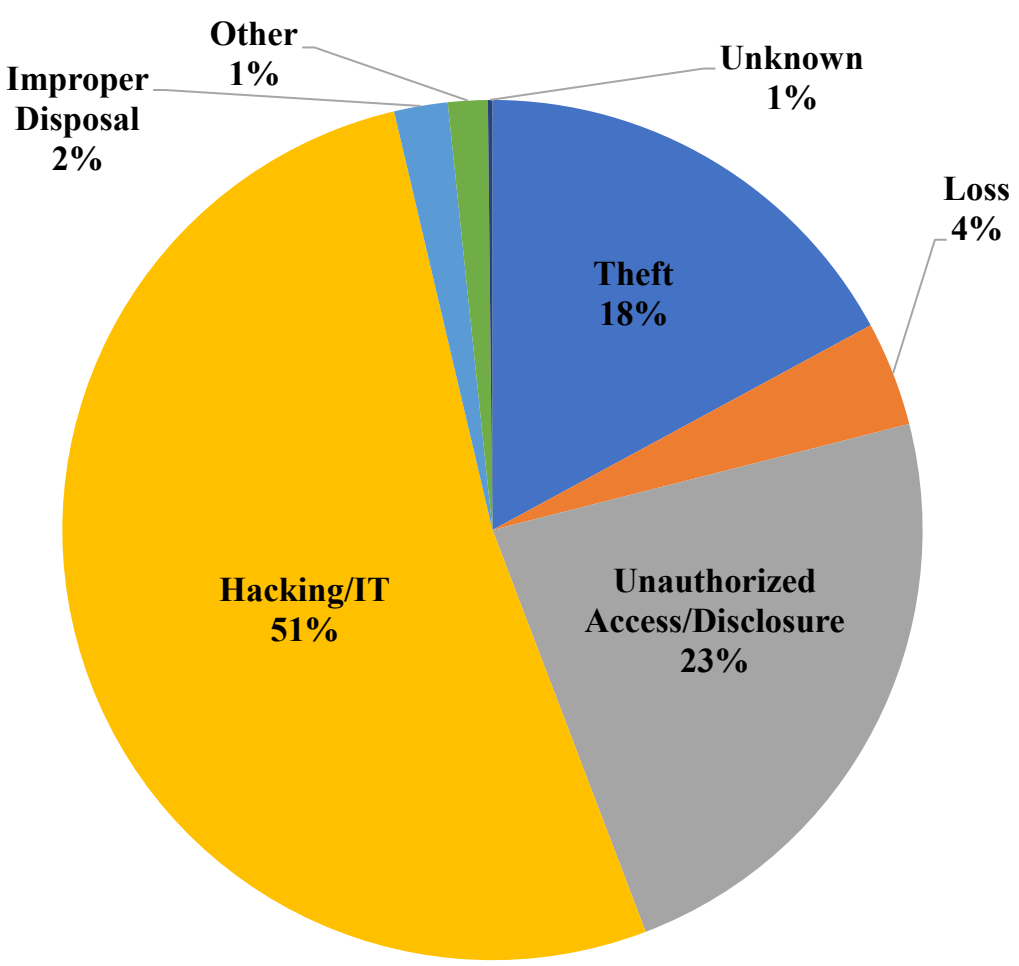
https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html

Trends in Health Data Breach Reporting

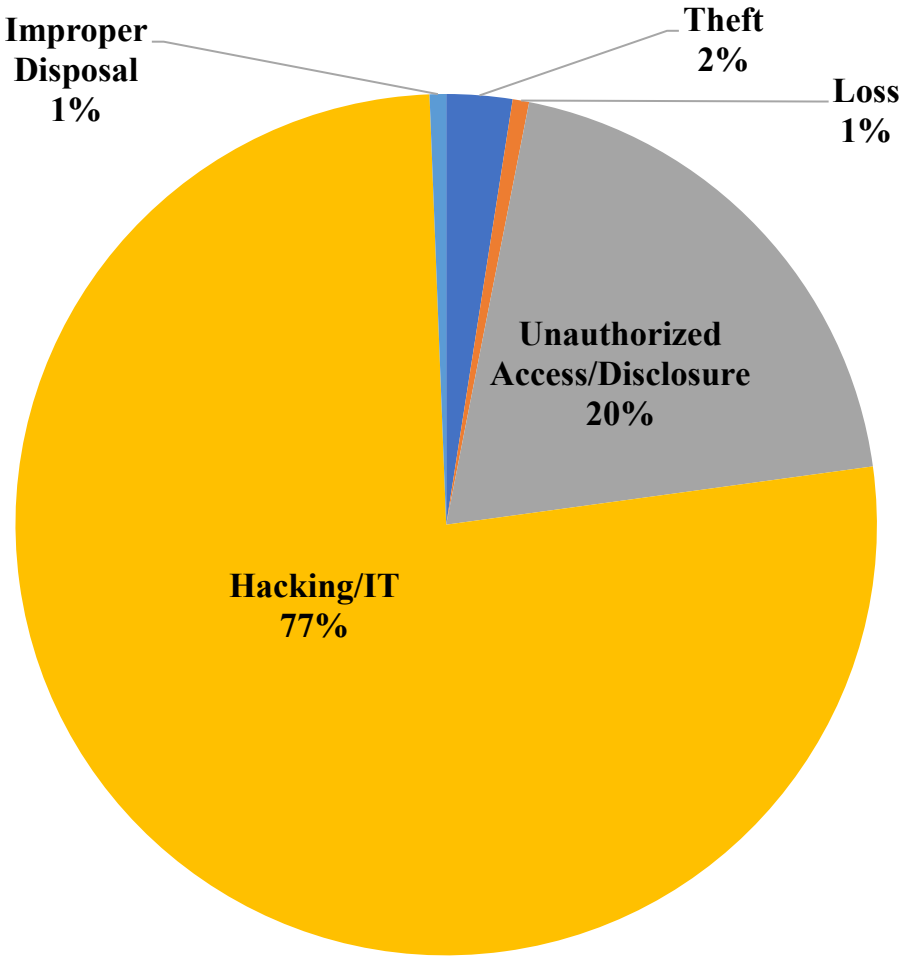
Large Breaches Received and # of Individuals Affected 2018 - 2023



500+ Breaches by Type of Breach



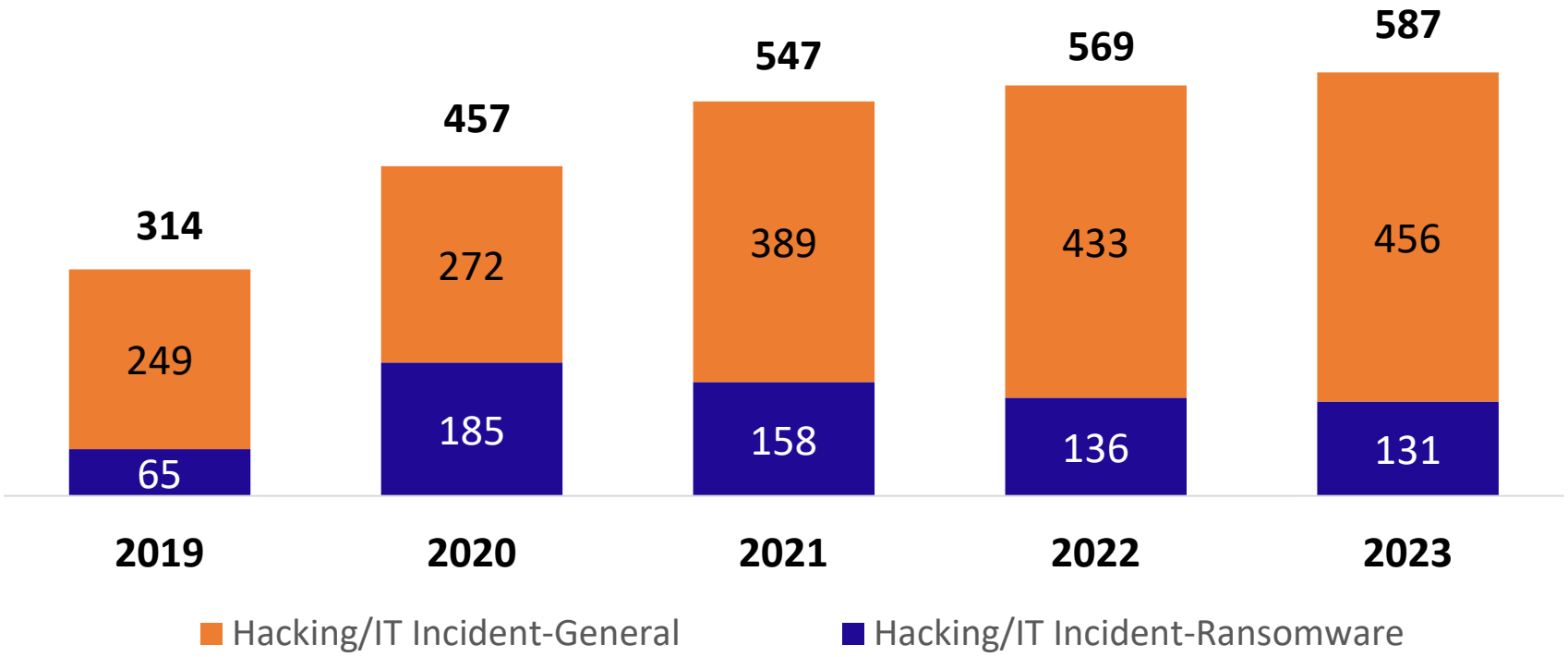
September 23, 2009 through Dec 31, 2023



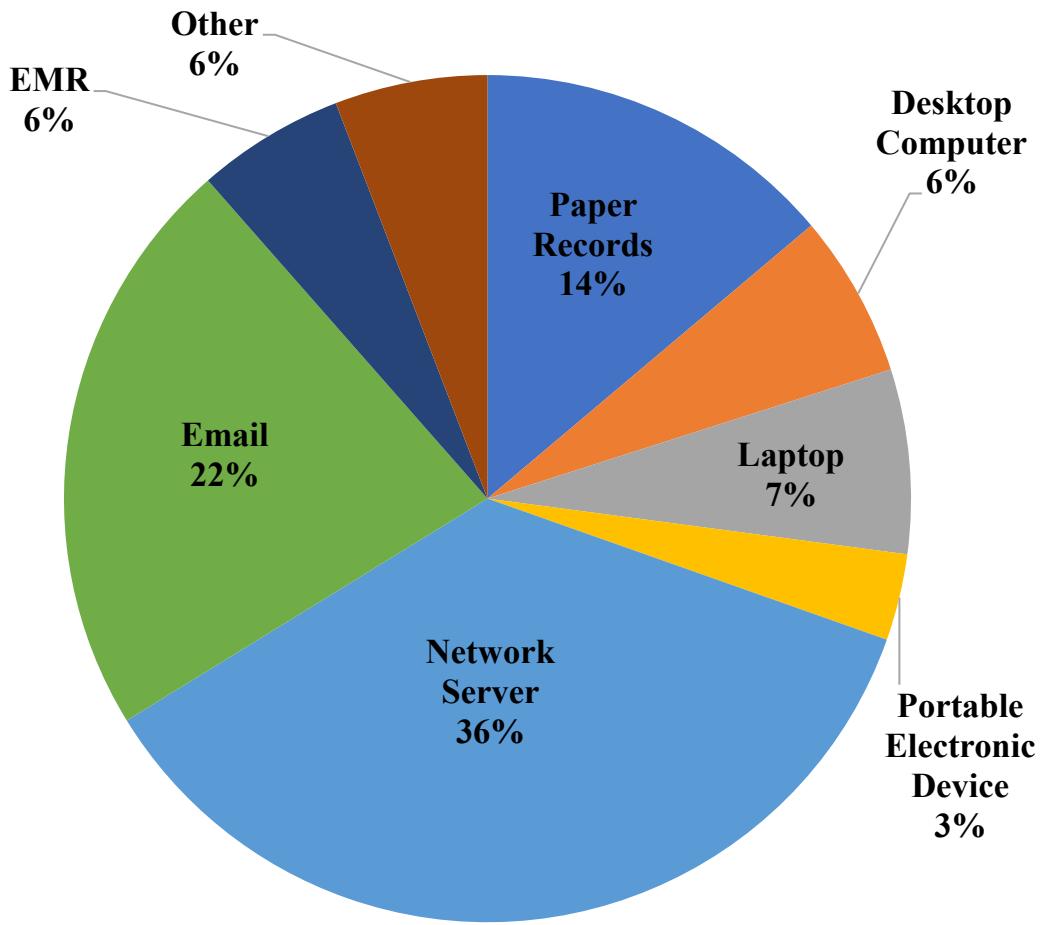
January 1, 2024 through March 31, 2024

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

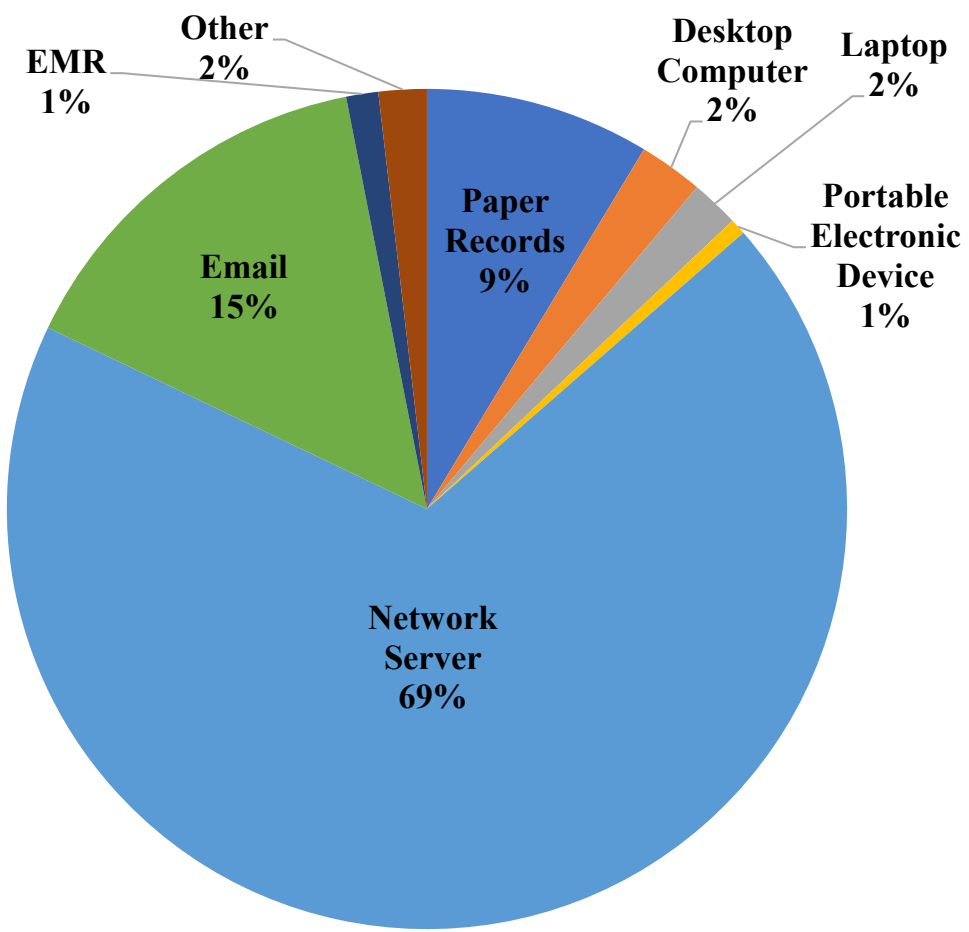
Calendar Years 2019 - 2023



500+ Breaches by Location of Breach



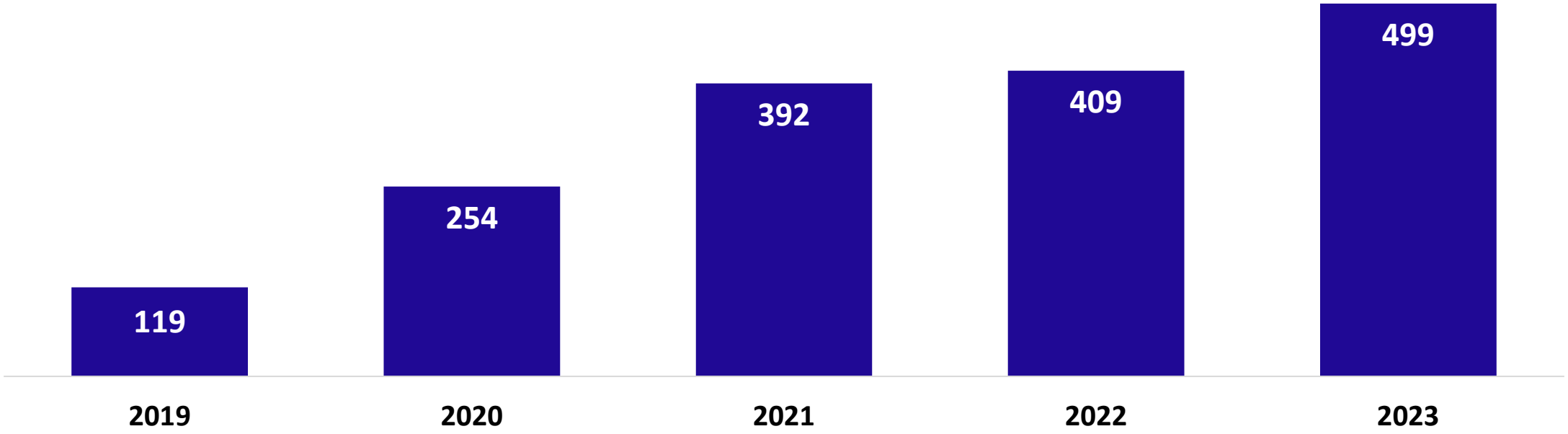
September 23, 2009 through Dec 31, 2023



January 1, 2024 through March 31, 2024

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

Calendar Years 2019 - 2023



RECENT HIPAA ENFORCEMENT ACTIVITY

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

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 three 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.
- Better overall security of data.