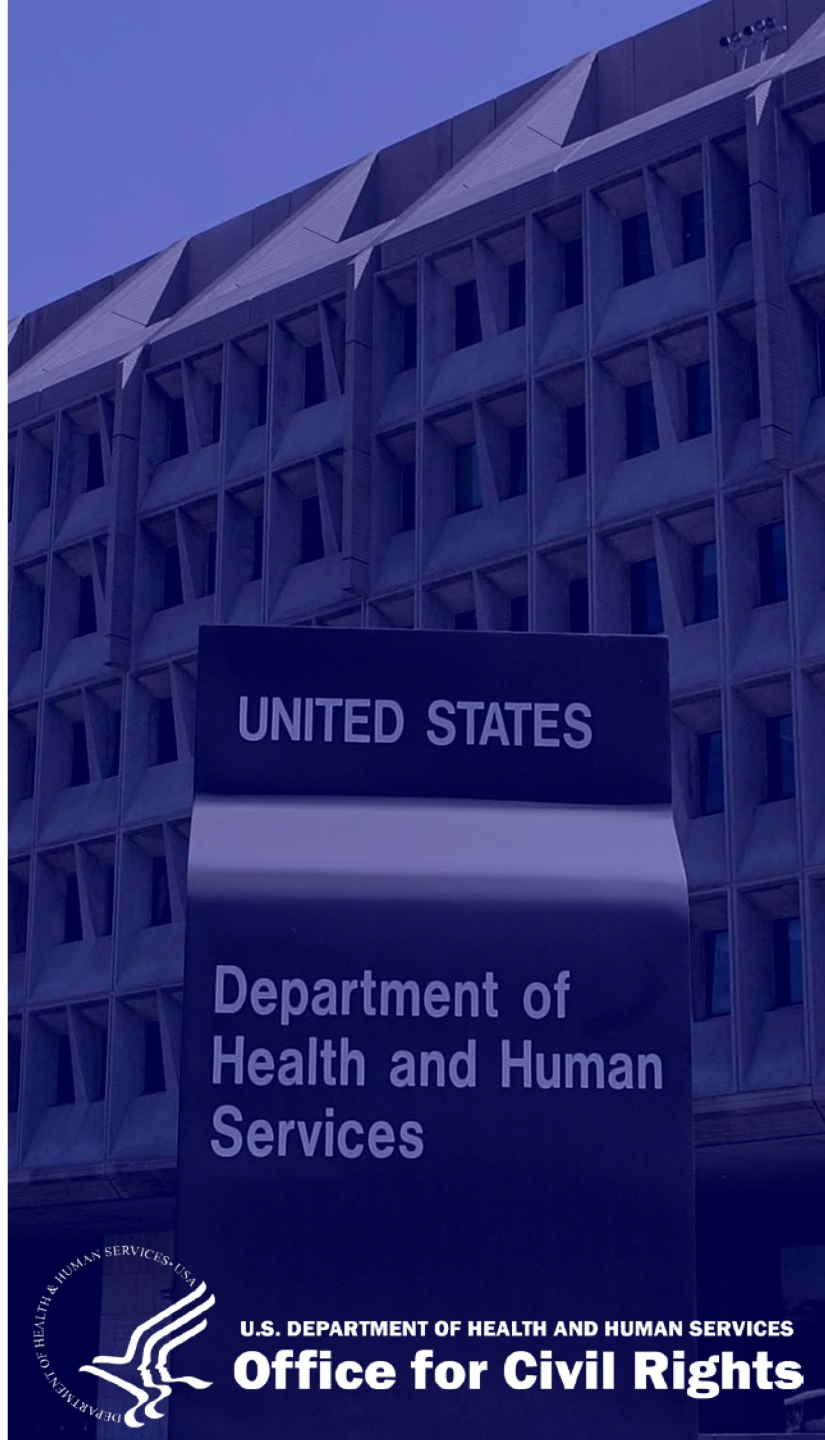
Federal Perspectives on Security Infrastructure and Enterprise-wide Risk Management in Healthcare

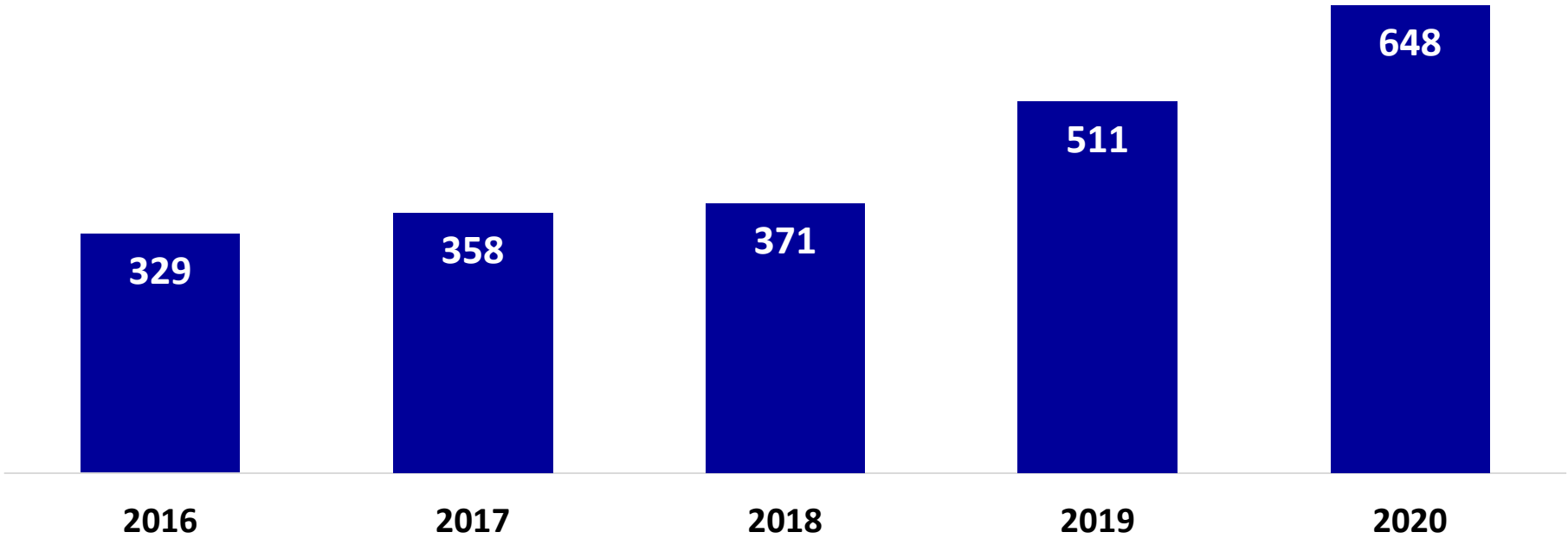
Timothy Noonan
Deputy Director for Health Information Privacy
HHS Office for Civil Rights

National Committee on Vital and Health Statistics
July 14, 2021

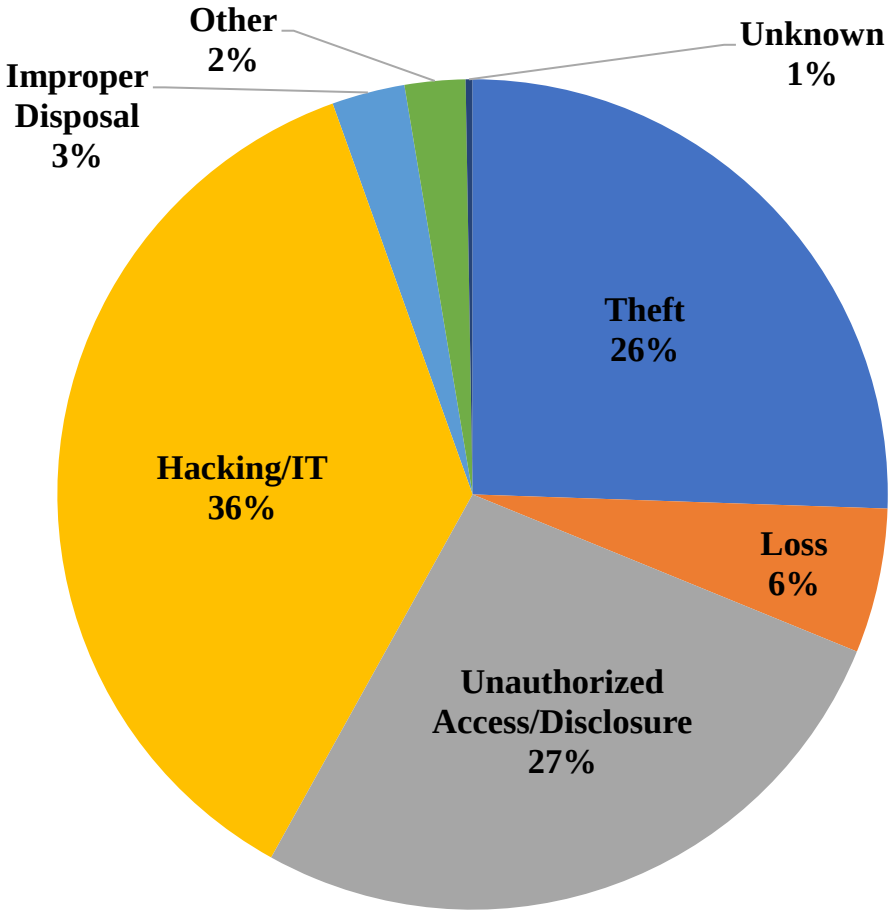


Breaches Affecting 500 or More Individuals
Reports Received by Year

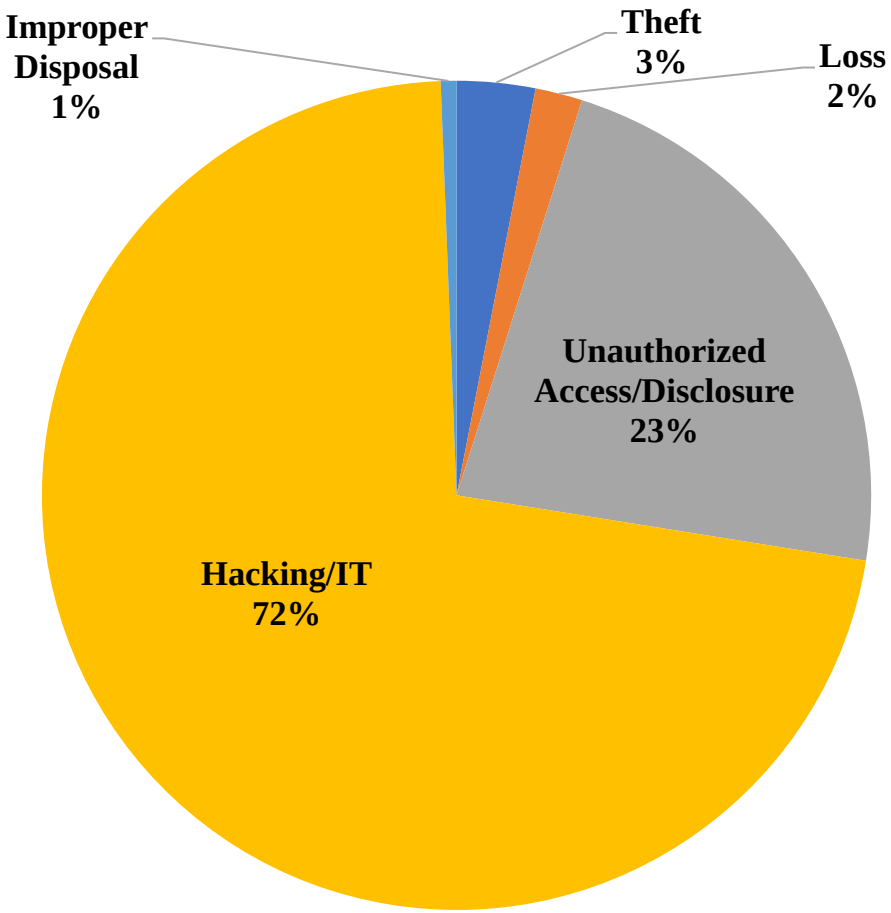
Calendar Years 2016 - 2020



500+ Breaches by Type of Breach

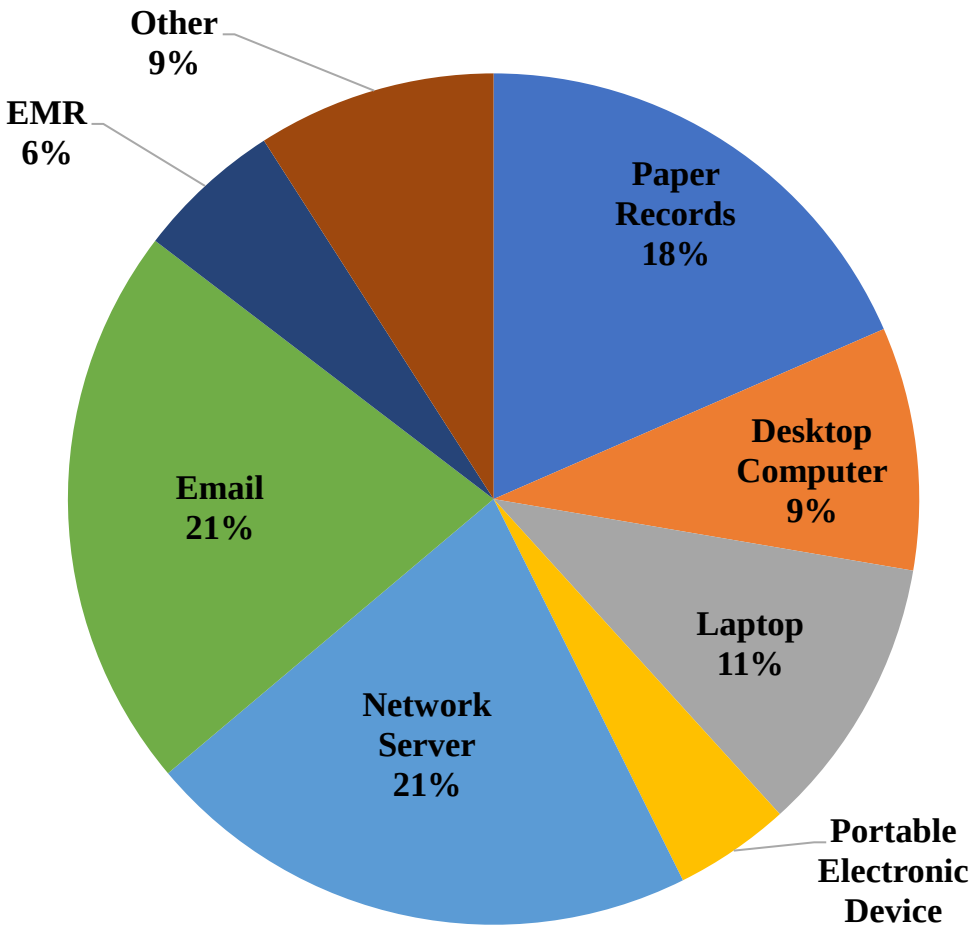


September 23, 2009 through December 31, 2020

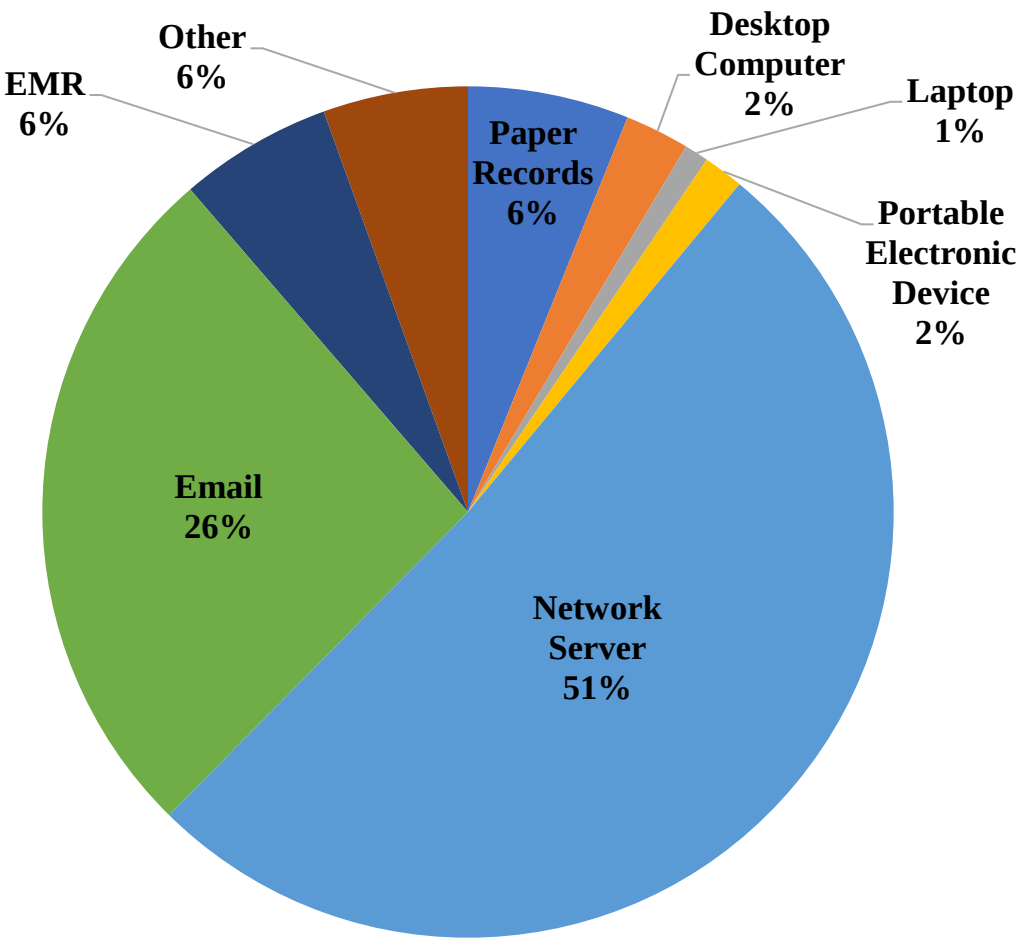


January 1, 2021 through June 30, 2021

500+ Breaches by Location of Breach



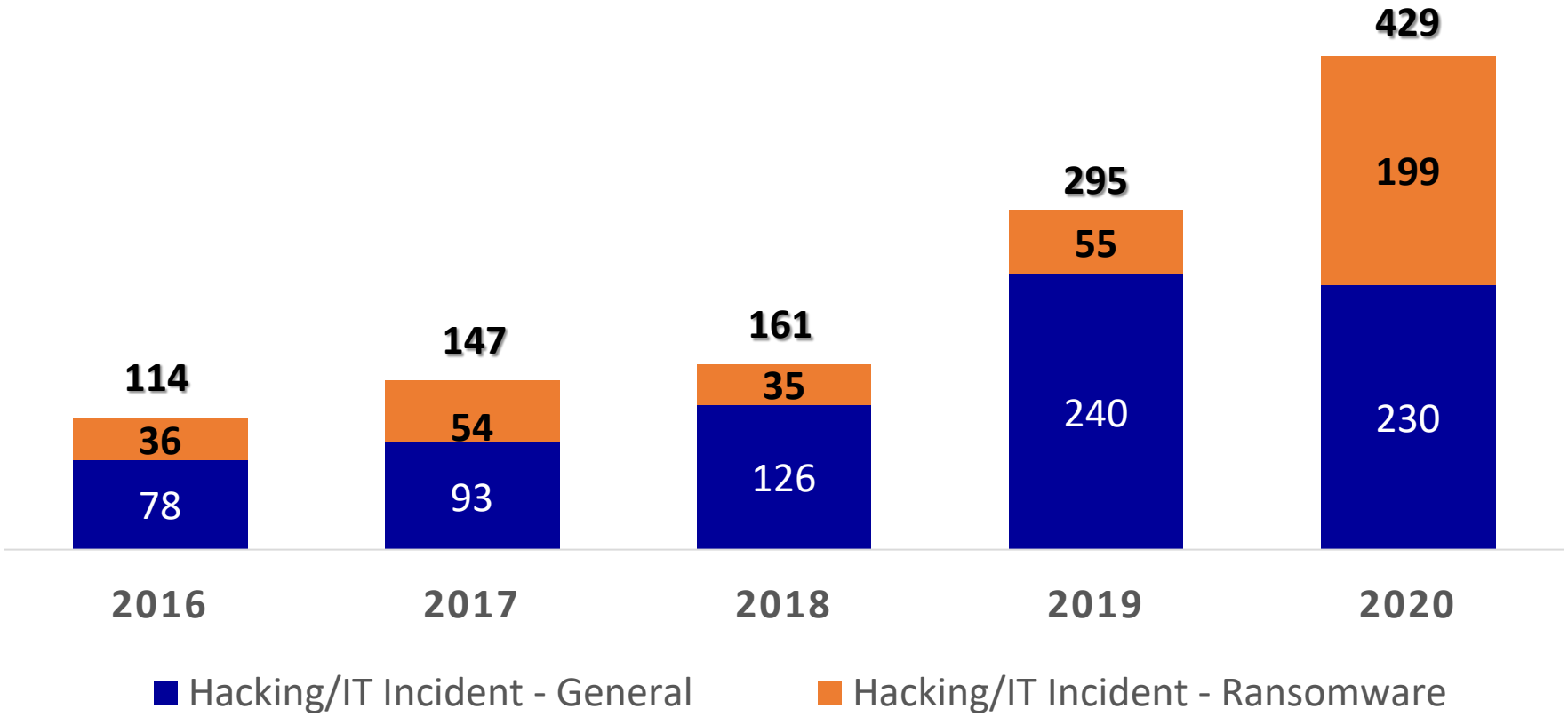
September 23, 2009 through December 31, 2020



January 1, 2021 through June 30, 2021

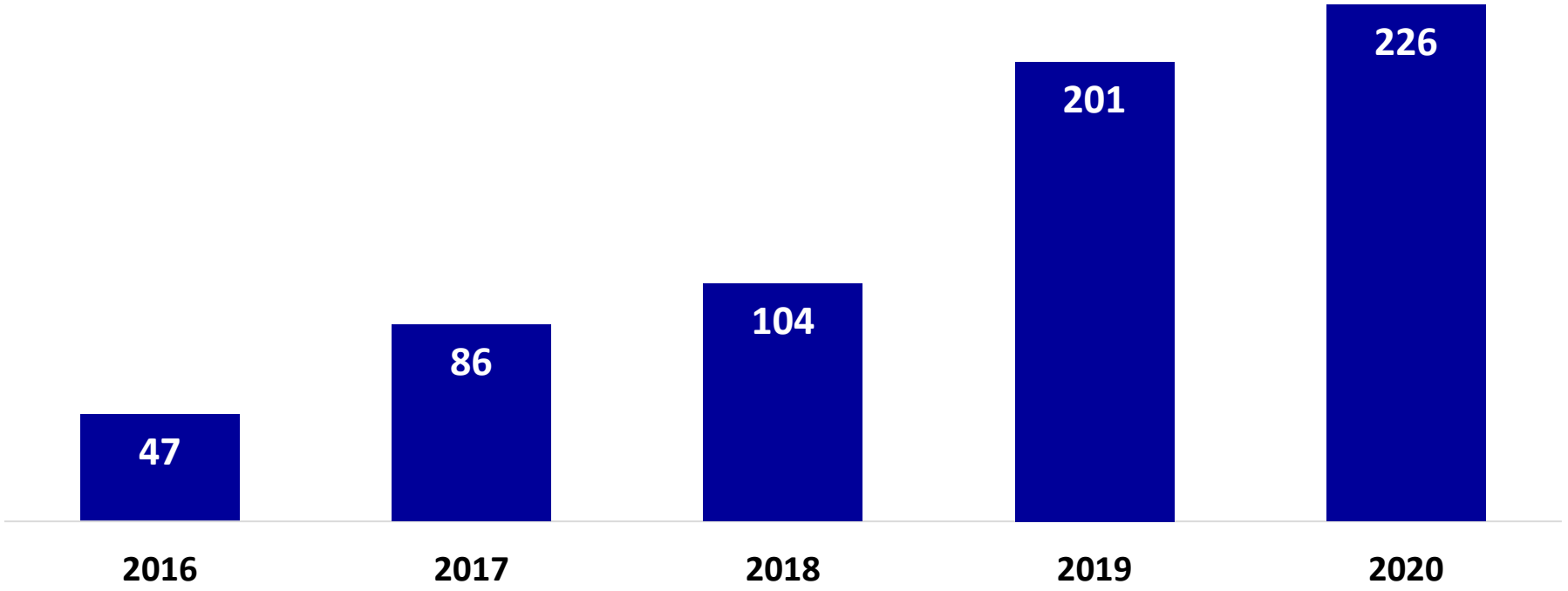
Breaches Affecting 500 or More Individuals
Reports Received Involving Hacking/IT Incidents

Calendar Years 2016 - 2020



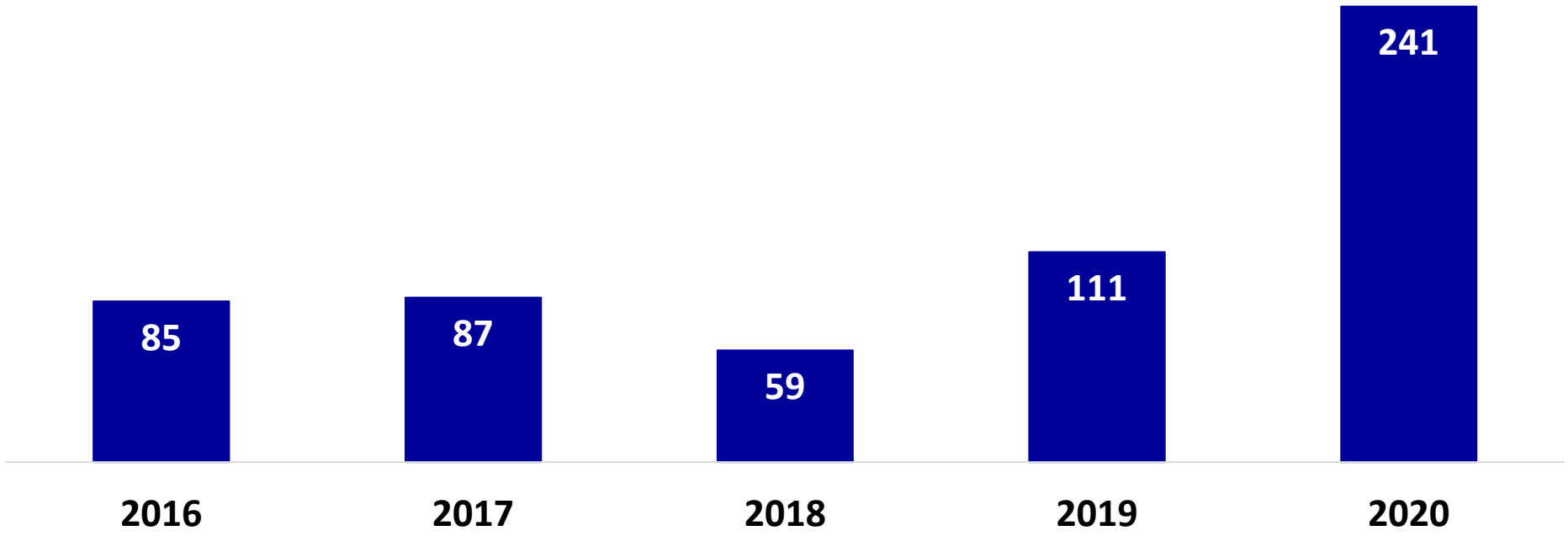
Breaches Affecting 500 or More Individuals
Reports Received of Breaches Involving Email Accounts

Calendar Years 2016 - 2020

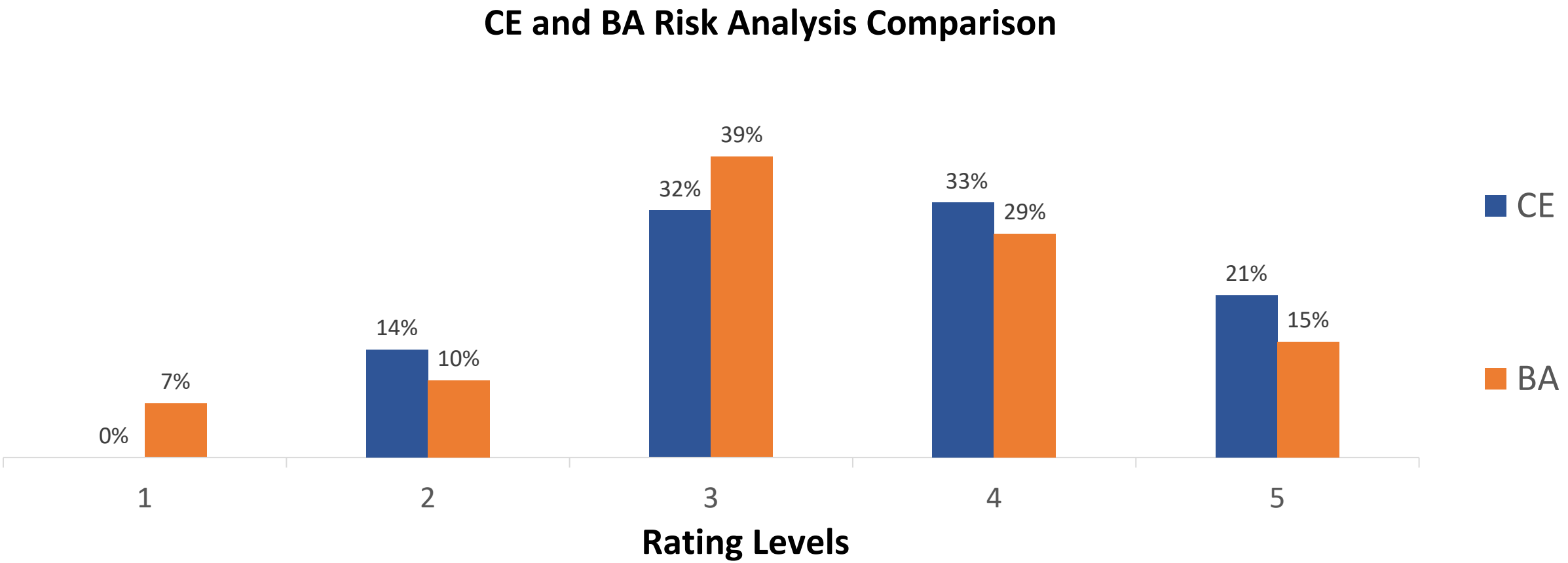


Breaches Affecting 500 or More Individuals
Reports Received of Breaches Involving Network Servers

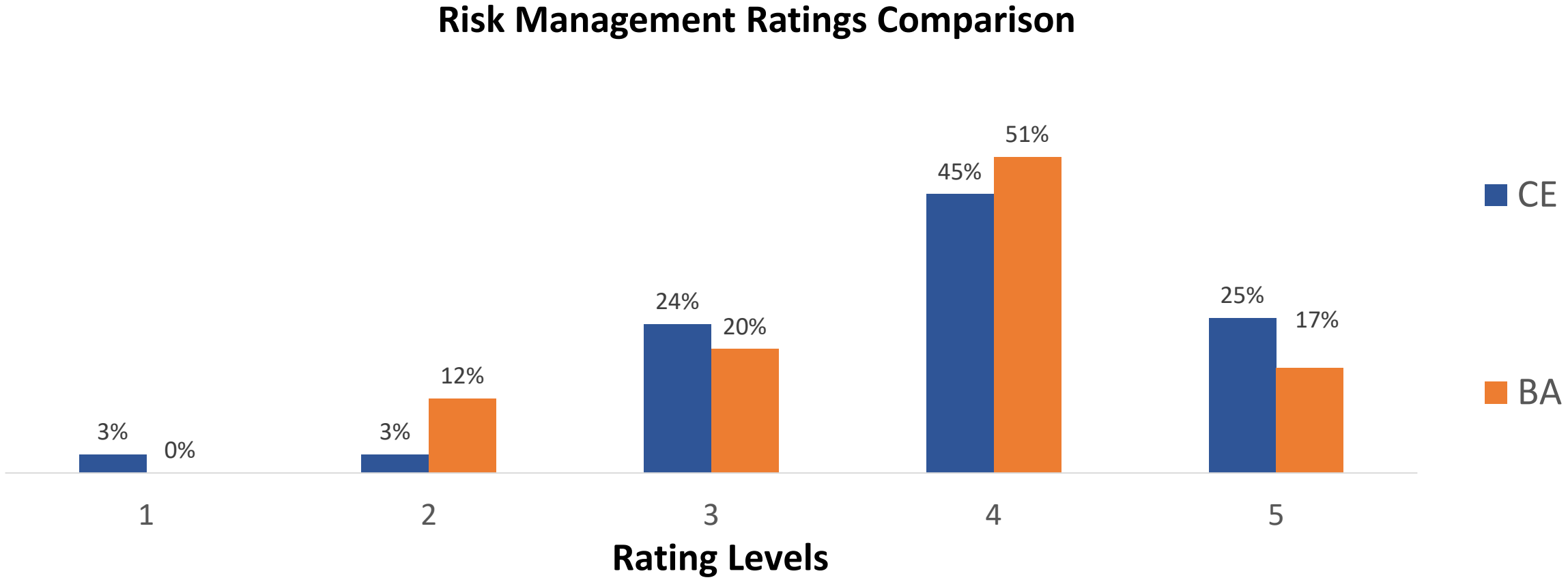
Calendar Years 2016 - 2020



2016-2018 HIPAA Audits: Risk Analysis



2016-2018 HIPAA Audits: Risk Management



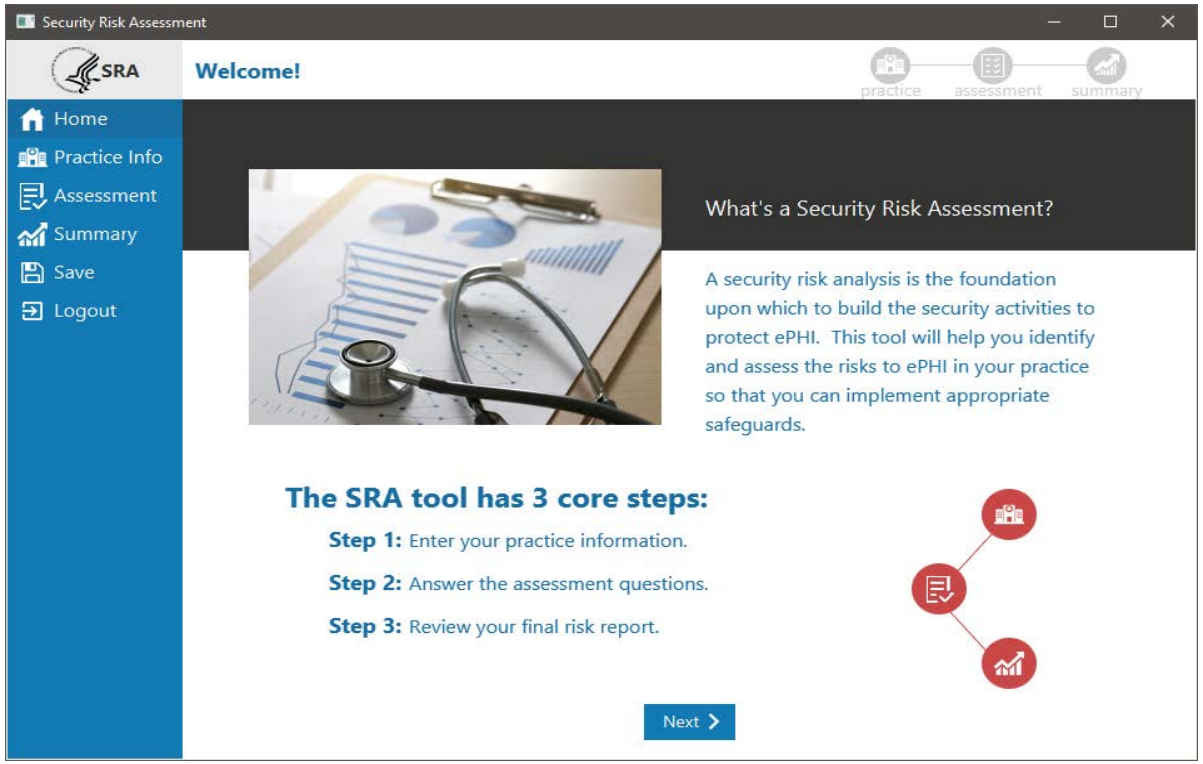
Recent OCR HIPAA Security Rule Enforcement Actions

Feb-20	Dr. Porter	$100,000
Mar-20	Metro Community Health	$25,000
Mar-20	Premera Blue Cross	$6,850,000
Mar-20	CHPSC	$2,300,000
Jun-20	Lifespan	$1,040,000
Jul-20	Athens Orthopedic Clinic PA	$1,500,000
Oct-20	Aetna	$1,000,000
Oct-20	City of New Haven, CT	$202,400
Jan-21	Excellus Health Plan	$5,100,000
Apr-21	Peachstate	$25,000

Best Practices

- Risk analysis and risk management should be integrated into business processes; conducted regularly and when new technologies and business operations are planned
- Conduct regular information system activity review (*e.g.,* audit logs, access reports, security incident tracking reports)
- Ensure access controls and authentication procedures are in place (*e.g.,* multi-factor authentication)
- Implement audit controls that record and examine activity in information systems
- 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:
  - 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

- HIPAA Security Rule Guidance Materials:
  http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html


Questions?