HIPAA Enforcement: Trends and Patterns

Serena Mosley-Day

Senior Advisor

HIPAA Compliance and Enforcement

Office for Civil Rights (OCR)
U.S. Department of Health and Human Services
March 3, 2020

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
  - 69 settlement agreements that include detailed corrective action plans and monetary settlement amounts
- 6 civil money penalties

Notification of Enforcement Discretion Regarding HIPAA Civil Money Penalties Announced April 26, 2019

Enforcement Notice			
Culpability	Low/violation*	High/violation*	Annual limit*
No Knowledge	$100	$50,000	$25,000
Reasonable Cause	$1,000	$50,000	$100,000
Willful – Corrected	$10,000	$50,000	$250,000
Willful – Not corrected	$50,000	$50,000	$1,500,000

https://www.federalregister.gov/documents/2019/04/30/2019-08530/enforcement-discretion-regarding-hipaa-civil-money-penalties

*The Department of Health and Human Services may make annual adjustments to the CMP amounts pursuant to the Federal Civil Penalties Inflation Adjustment Act Improvement Act of 2015. The annual inflation amounts are found at 45 CFR § 102.3.

Civil Money Penalty Amounts

OCR's HIPAA jurisdiction contains authority for the issuance of monetary penalties, including a specific schedule for the calculation of penalties depending on the type of violation.

	For violations occurring prior to 11/3/2015	For violations occurring on or after 11/3/2015*
Penalty Amount Per Violation	**$100 to $50,000 per violation**	**$119 to $59,522* per violation**
Calendar Year Cap For Violations of Identical Requirement or Prohibition	**$25,000-$1,500,000****	**$25,000-$1,785,651****

*The Department of Health and Human Services *may* make annual adjustments to the CMP amounts pursuant to the Federal Civil Penalties Inflation Adjustment Act Improvement Act of 2015. The annual inflation amounts are found at 45 CFR § 102.3.
**Pursuant to HHS's Notification of Enforcement Discretion, https://www.federalregister.gov/documents/2019/04/30/2019-08530/enforcement-discretion-regarding-hipaa-civil-money-penalties

In determining the amount of a CMP, OCR considers the following factors, which may be mitigating or aggravating as appropriate: (a) the nature and extent of the violation; (b) the nature and extent of the harm resulting from the violation; (c) the history of prior compliance with the administrative simplification provisions, including violations, by the covered entity or business associate; (d) the financial condition of the covered entity or business associate; and (e) such other matters as justice may require. See 45 C.F.R. § 160.408.

Breach Notification Requirements

- Covered entity must notify affected individuals, HHS, and in some cases, the media
- Business associate must notify covered entity of a breach
- Notification to be provided without unreasonable delay (but no later than 60 calendar days) after discovery of breach
  - Annual reporting to HHS of smaller breaches (affecting less than 500 individuals) permitted

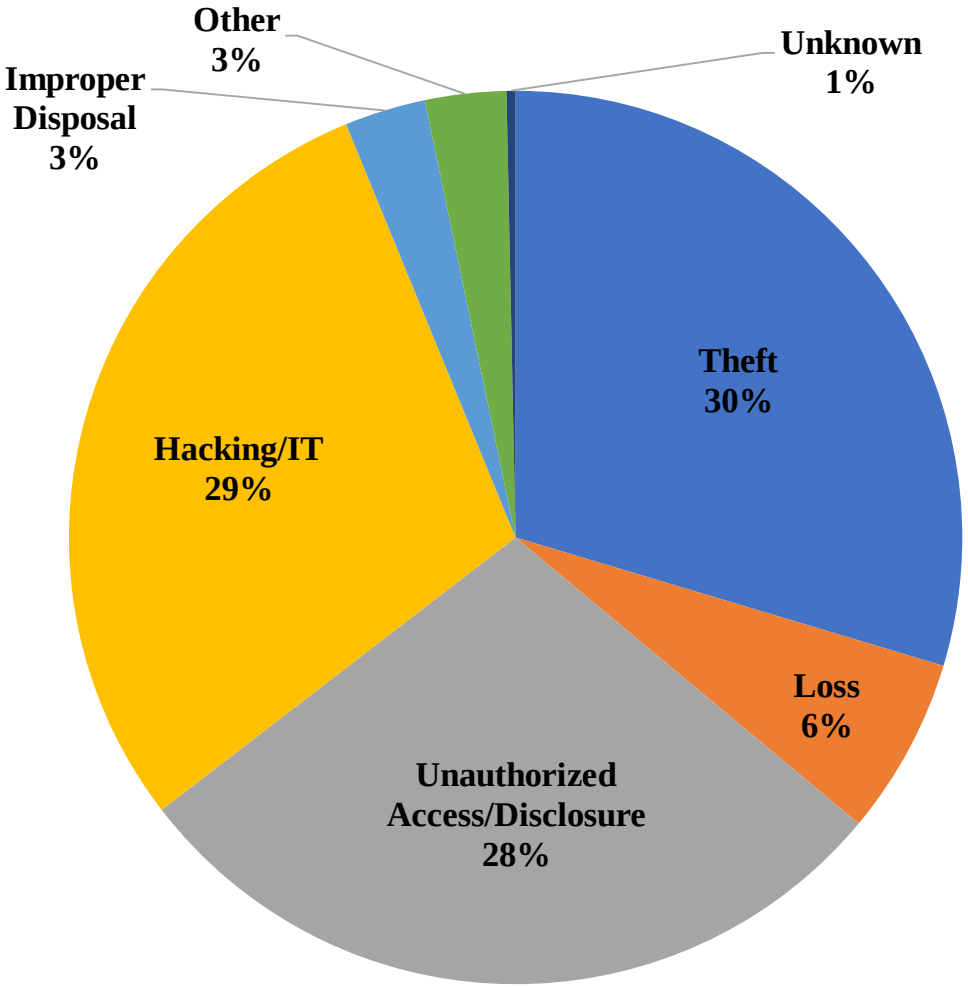
Breach Portal:

https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

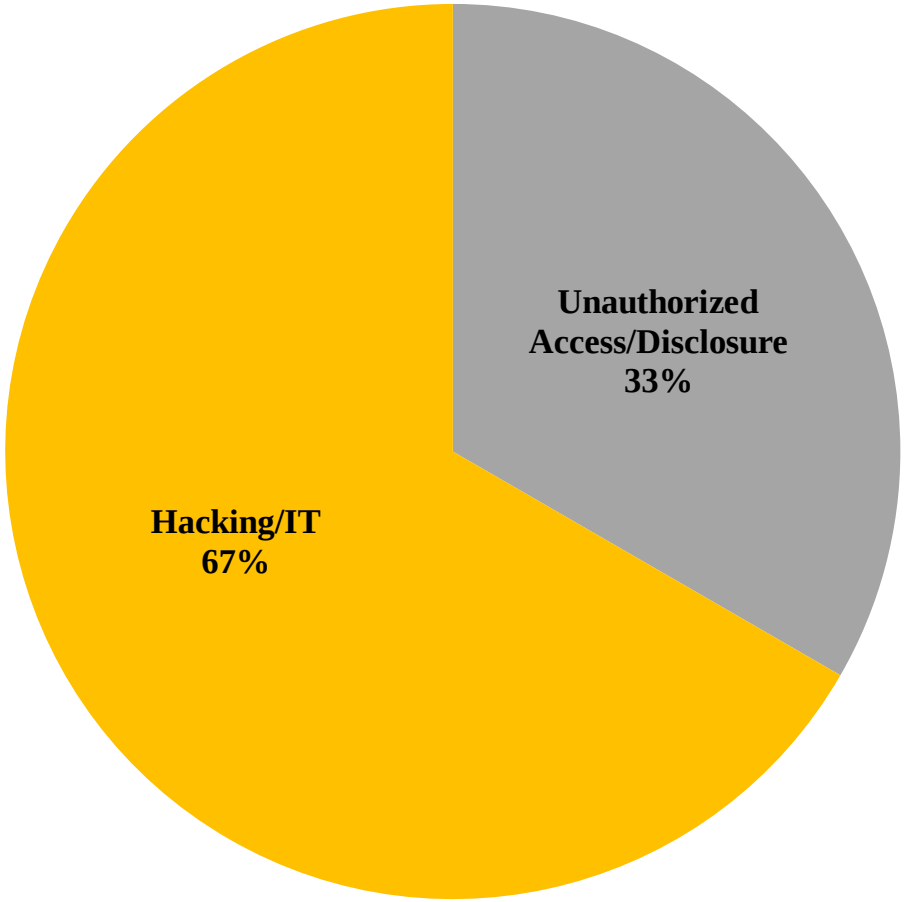
What Happens When HHS OCR Receives a Breach Report

- OCR posts breaches affecting 500+ individuals on OCR website (after verification of report)
  - Public can search and sort posted breaches
  - Receive over 350 breach reports affecting 500 individuals or more per year
- 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

500+ Breaches by Type of Breach

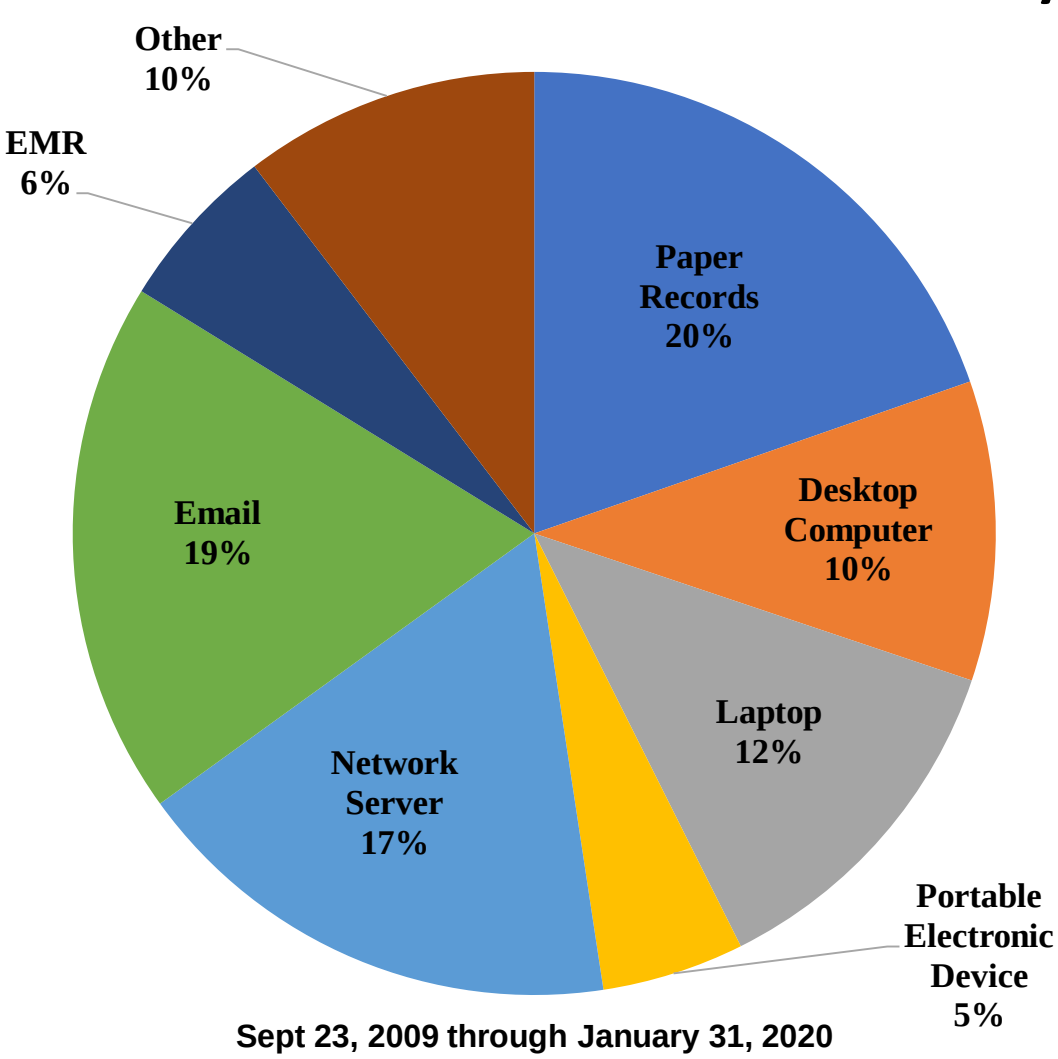


Sept 23, 2009 through January 31, 2020

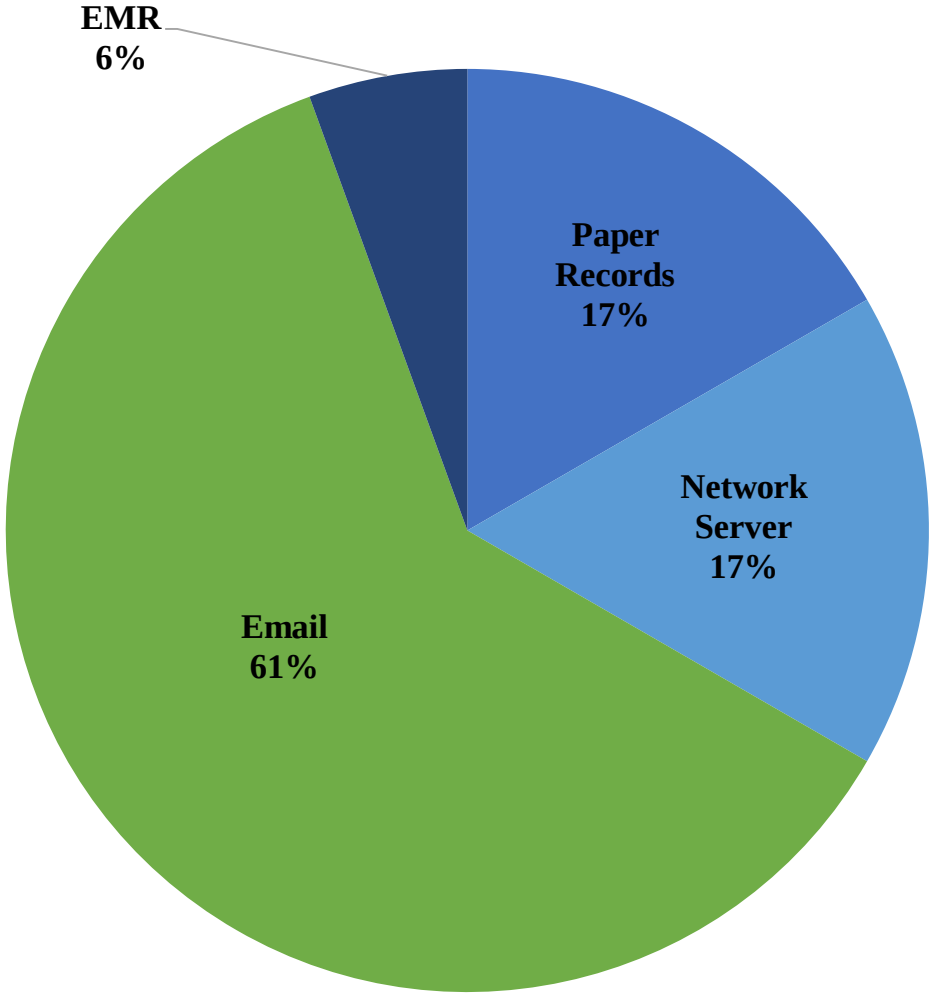


January 1, 2020 through January 31, 2020

500+ Breaches by Location of Breach



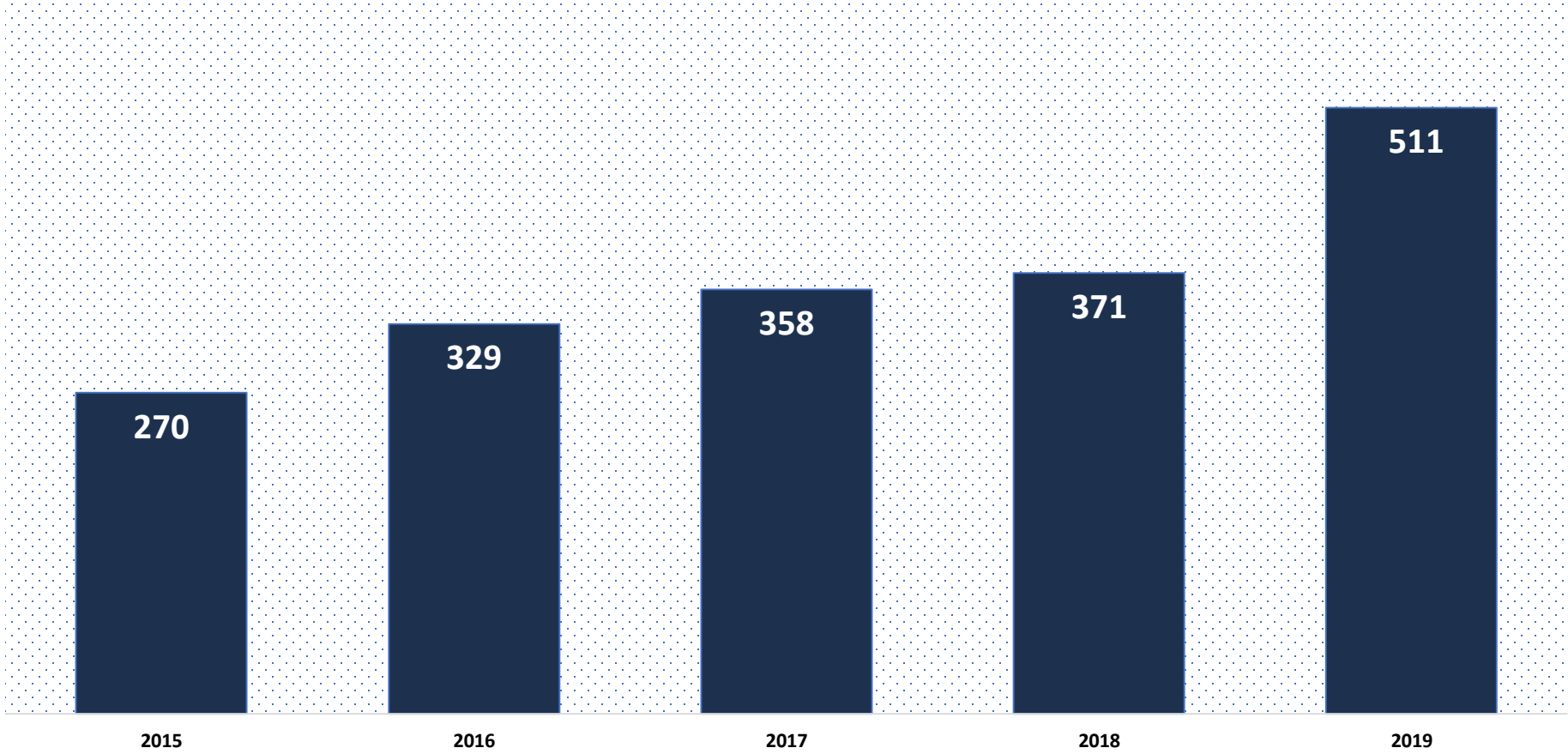
Sept 23, 2009 through January 31, 2020



January 1, 2020 through January 31, 2020

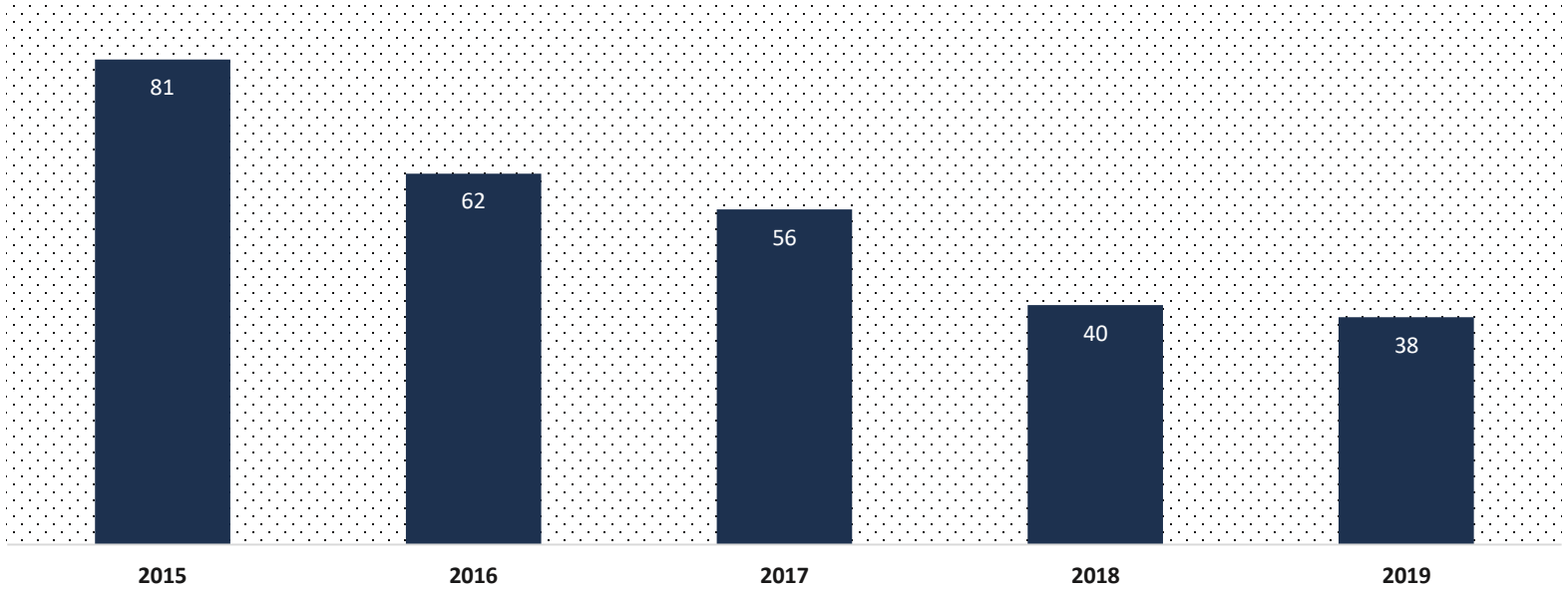
Breaches Affecting 500 or More Individuals
Reports Received by Year

Calendar Years 2015 - 2019



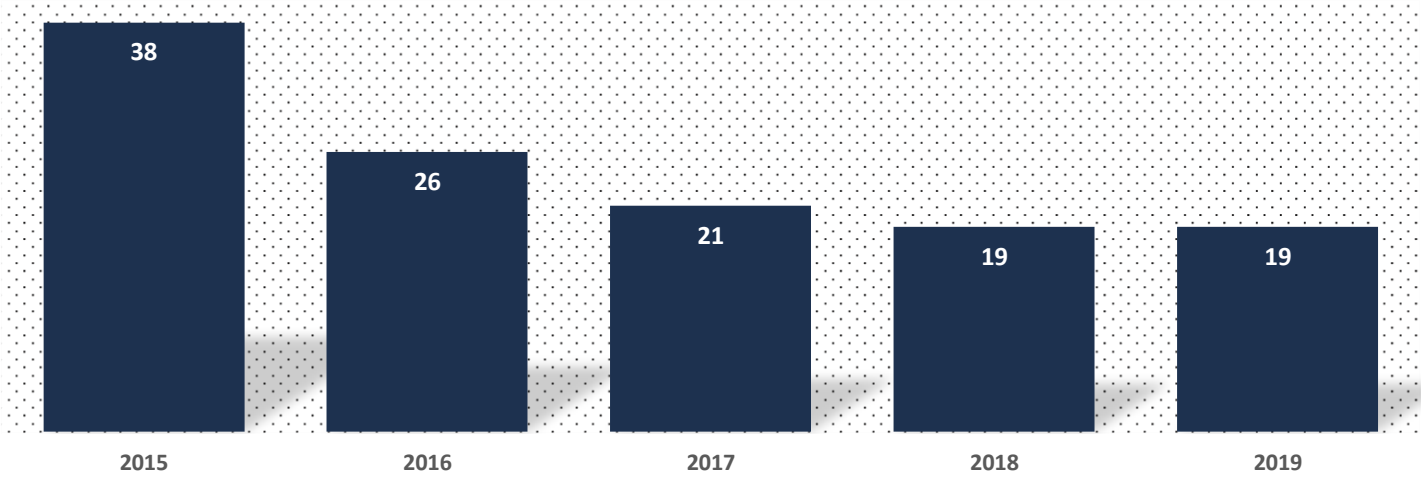
Breaches Affecting 500 or more Individuals
Reports Received Involving the Theft of PHI

Calendar Years 2015 - 2019



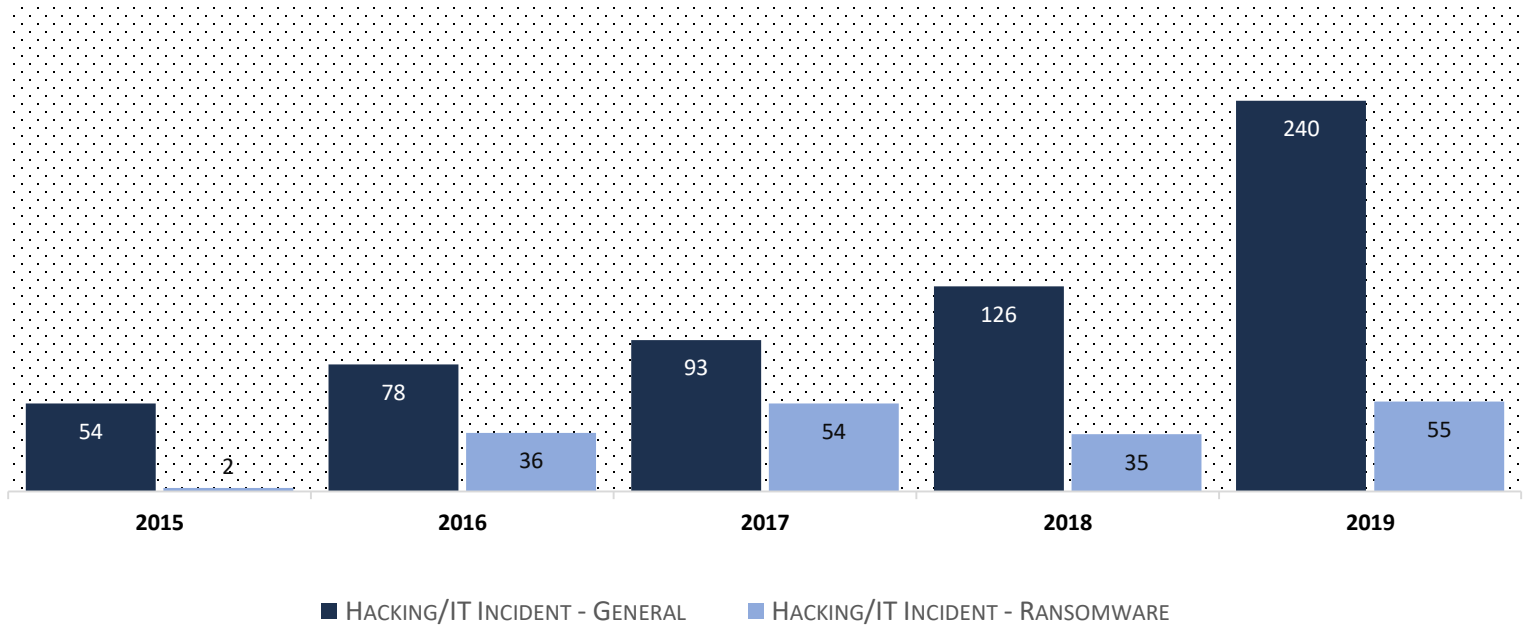
Breaches Affecting 500 or more Individuals
Reports Received of Breaches of Laptop Computers

Calendar Years 2015 - 2019



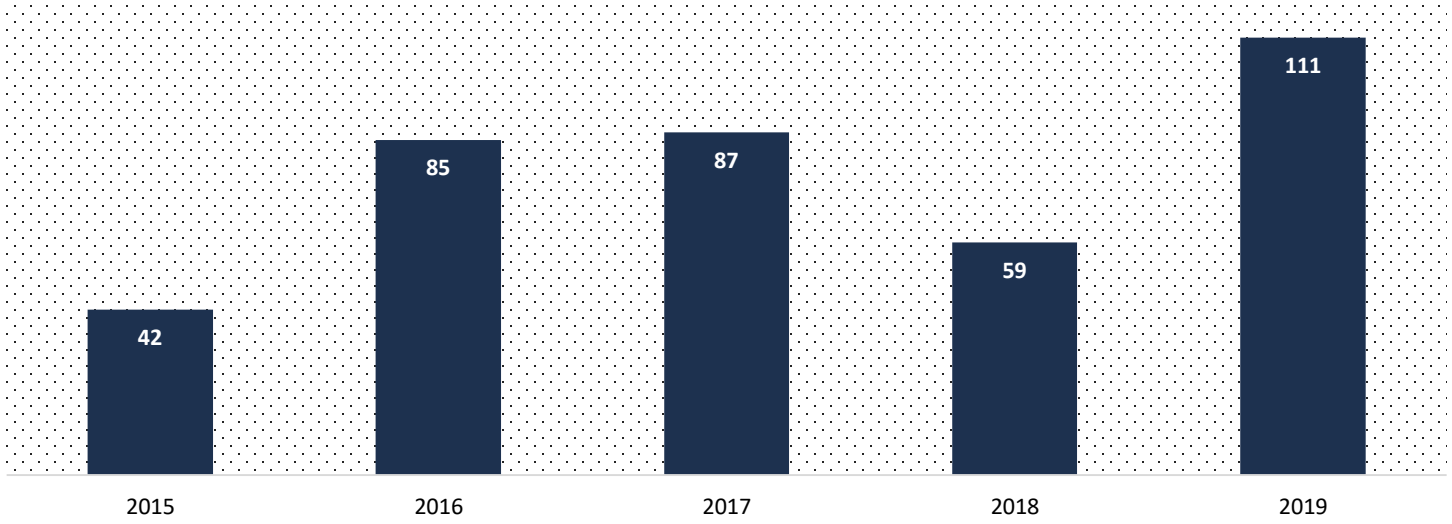
Breaches Affecting 500 or More Individuals
Reports Received Involving
Hacking/IT Incidents

Calendar Years 2015 - 2019



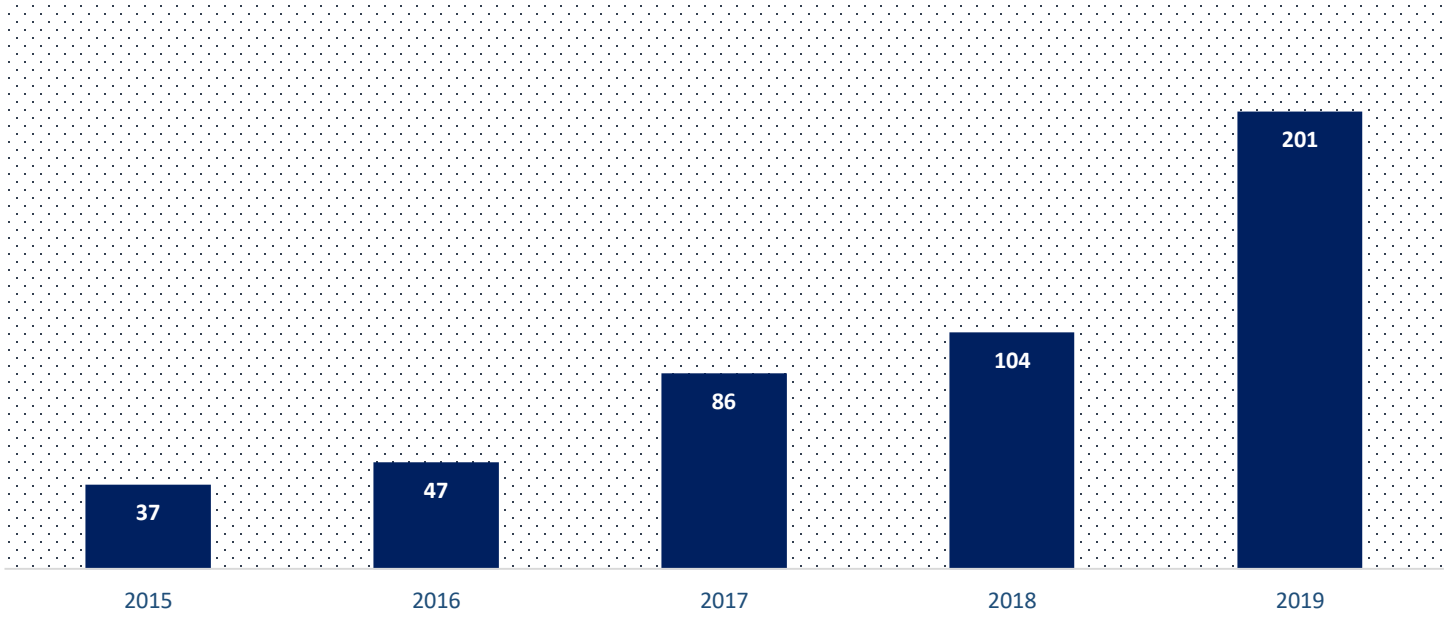
Breaches Affecting 500 or more Individuals
Reports Received of Breaches of Network Servers

Calendars Years 2015 - 2019



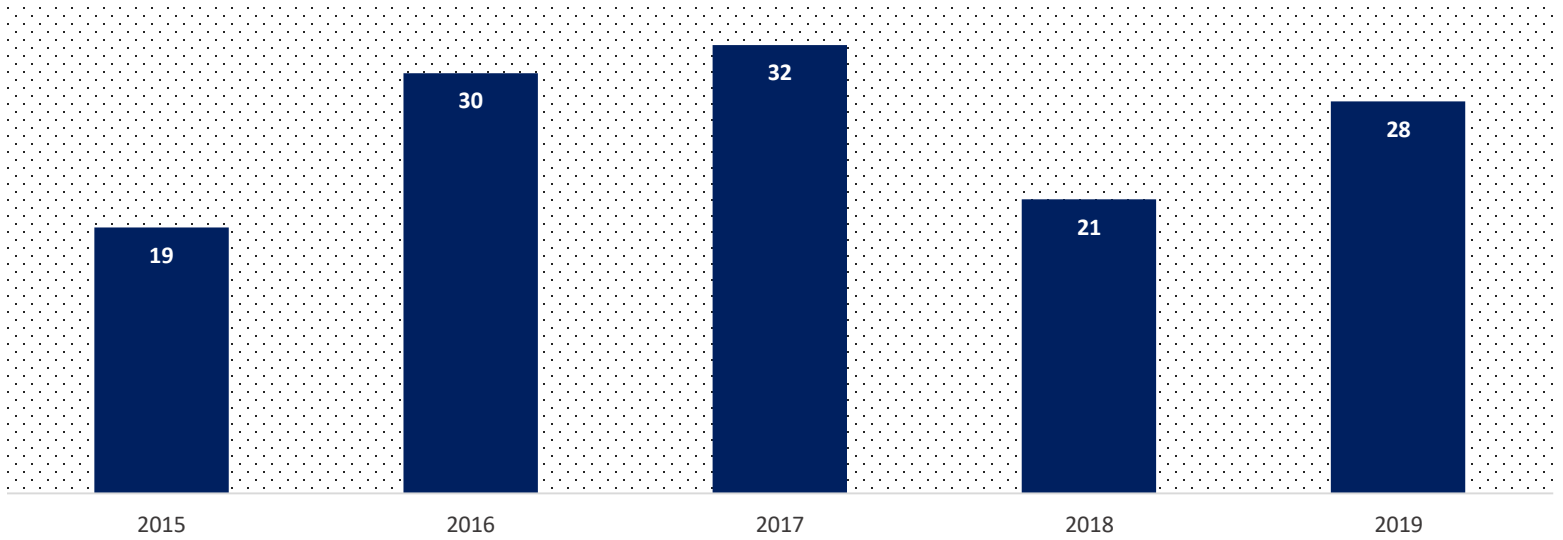
Breaches Affecting 500 or more Individuals
Reports Received of Breaches Involving Email Accounts

Calendar Years 2015 - 2019



Breaches Involving 500 or more Individuals
Reports Received involving Breaches of Electronic Medical Records

Calendar Years 2015 - 2019



Enforcement and Compliance Activities

- Complaint Investigations
- Compliance Reviews
  - Including all 500+ breach reports
- Letters of Finding
- Settlement Agreements
- Formal Enforcement

Recurring Compliance Issues

- Business Associate Agreements
- Risk Analysis
- Failure to Manage Identified Risk, e.g. Encryption
- Lack of Transmission Security
- Lack of Appropriate Auditing
- Patching of Software
- Insufficient Data Backup and Contingency Planning
- Individual Right to Access

2019 Enforcement Actions

4/2019	Touchstone Medical Imaging	$3,000,000	OCR Initiated
4/2019	Medical Informatics Engineering	$100,000	Breach Report
9/2019	Bayfront Health St. Petersburg	$85,000	Complaint
9/2019	Elite Dental Associates	$10,000	Complaint
10/2019	Jackson Health System (CMP)	$2,154,000	Breach Reports/ OCR Initiated
10/2019	Texas Health and Human Services Commission (CMP)	$1,600,000	Breach Report
10/2019	University of Rochester Medical Center	$3,000,000	Breach Reports
11/2019	Sentara Hospitals	$2,175,000	Complaint
12/2019	Korunda Medical	$85,000	Complaint
12/2019	West Georgia Ambulance	$65,000	Breach Report

Total: $12,274,000

2020 Enforcement

2/2020	Steven A. Porter, M.D.	$100,000	Breach Report*

Dr. Steven Porter

- Breach Report
- Gastroenterologist
- Solo practitioner
- Did not have risk analysis
- Multiple attempts at technical assistance regarding risk analysis and risk management plan
- $100,000 settlement
- 2 year corrective action plan
  - Security Management Process
  - Policies/Procedures
  - Business Associate Agreements

Civil Money Penalty Cases

Jackson Health System

- $2,154,000 civil money penalty
- 3 investigations
  - Paper records loss incidents
  - Media acquisition of PHI
  - Employee theft of PHI
- 3 violations
  - Breach Notification to the Secretary
  - Security Management Process
  - Information Access Management

TX Health and Human Services Commission

- $1,600,00 civil money penalty
- Breach investigation
  - ePHI viewable on the internet
    - Names, addresses, SSN, treatment info
- 4 violations
  - Impermissible disclosure
  - Access Controls
  - Audit Controls
  - Risk Analysis

Trends and Patterns

Impermissible Disclosure and Safeguards

- A covered entity, including a health care provider, may not use or disclose protected health information (PHI), except either: (1) as the HIPAA Privacy Rule permits or requires; or (2) as the individual who is the subject of the information (or the individual's personal representative) authorizes in writing. *See* 45 C.F.R. § 164.502(a).
- A covered entity must have in place appropriate administrative, technical, and physical safeguards that protect against uses and disclosures not permitted by the Privacy Rule, as well as that limit incidental uses or disclosures. *See* 45 C.F.R. § 164.530(c).

Trends and Patterns: Impermissible Disclosure

Elite Dental

- Originated as a complaint
- PHI discussed on Yelp Review page
  - Last name
  - Treatment plan
  - Insurance
  - Treatment cost
- Review found multiple patients' PHI discussed on Yelp Review page
- Failed to implement policies and procedures with respect to PHI
- Notice of Privacy Practices also deficient
- **$10,000** settlement
- 2 year corrective action plan

Trends and Patterns

Lackluster Responses to Security Incidents

- Security Training (45 C.F.R. § 164.308(a)(5))
- Security Incident - Response and Reporting (45 C.F.R. § 164.308(a)(6)(ii))
- Evaluation (45 C.F.R. § 164.308(8))
- Security Rule Policies and Procedures (45 C.F.R. § 164.316)
- Breach Reporting (45 C.F.R. § 164. 404-164.408)

Trends and Patterns: Lackluster Response

Touchstone Medical Imaging

- Originated as an OCR-initiated compliance review
- Provider of diagnostic medical imaging services
- Over 300,000 individuals ePHI exposed online through insecure server
- TMI informed by both FBI and OCR in May 2014
  - Said no patient info exposed
  - Ultimately, 300k+ patients' info deemed to have been on web
  - Including full names, SSNs, DOB, addresses
- Notification to individuals and media untimely
- Failed to have BAAs in place with vendors, including their IT support vendor and 3rd party data center provider
- Failed to conduct an accurate and thorough risk analysis
- Often overlooked Administrative Safeguard: Security incident procedures.
- Requires CEs/BAs to implement policies and procedures to address security incidents.
- **$3,000,000** settlement
- 2 year corrective action plan

Trends and Patterns: Lackluster Response

West Georgia Ambulance

- Breach Report regarding unencrypted laptop, PHI of 500 individuals
- Did not have a risk analysis
- Did not have Security Rule policies or procedures
- Failed to train staff
- $65,000 settlement
- 2 year corrective action plan

Trends and Patterns: Lackluster Response

Sentara Hospitals

- Originated as a complaint
- Complainant received bill with another individual's PHI
- PHI of 577 individuals sent to wrong address
- Sentara only notified HHS of 8
- Failed to obtain business associate agreement
- Failed to notify HHS of breach even after technical assistance
- $2,175,000 settlement
- 2 year corrective action plan

Trends and Patterns: Right of Access Initiative

Common Compliance Issues:

- Untimely Access;
- Unreasonable Fees;
- Form and Format;
- Validation Burdens; and
- Withholding Access for Non-Payment.

Privacy Rule Right of Access Requests

- [An] individual has a right of access to inspect and obtain a copy of protected health information about the individual in a designated record set, for as long as the protected health information is maintained in the designated record set.... See 45 C.F.R. §164.524(a)(1).
- [T]he covered entity must act on a request for access no later than 30 days after receipt of the request.... See 45 C.F.R. §164.524(b)(2).
- Includes the right to inspect records. 45 C.F.R. §164.524(b)(1).
- The provision of access must be provided in the form and format requested. 45 C.F.R. §164.524(c)(2).
- Can be directed to a person designated by the individual at the individual's signed written request. See 45 C.F.R. §164.524(c)(3).
- Only reasonable, cost-based fees may be assessed. See 45 C.F.R. §164.524(c)(4).

Trends and Patterns: Right of Access Initiative

Bayfront St. Petersburg

- 1st Right of Access Initiative case
- Originated as a Complaint
- Records requested related to child's birth
- October 2017- 2 requests due to confusion about which designated record set contained the requested information
- Immediately corrected by Complainant
- January and February 2018 – attorney requested records
- March 2018 – partial records delivered to attorney
- August 2018 – full records delivered to attorney
- February 2019 – full records delivered to Complainant
- $85,000 settlement
- 1 year corrective action plan

Trends and Patterns: Right of Access Initiative

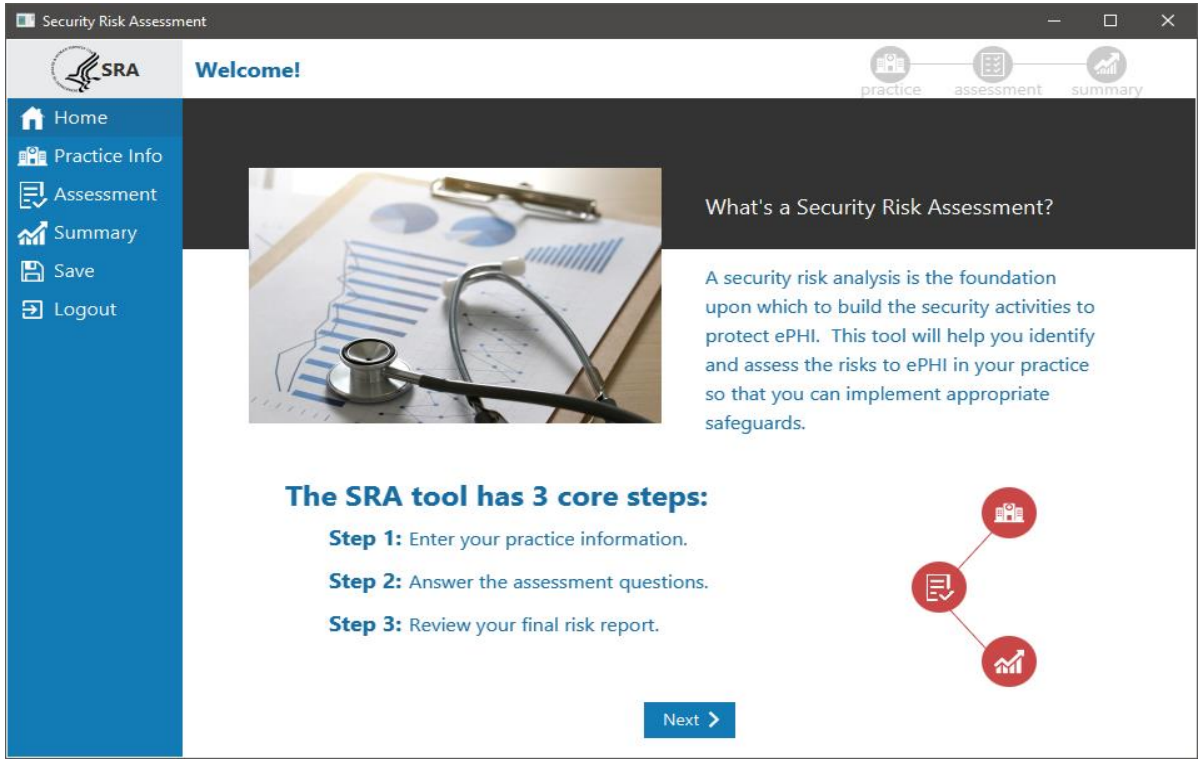
Korunda Medical

- Originated as Complaint
- October 2018 – Right of Access Request. 3rd party directive.
- March 2019 – Complaint filed with OCR
- March 2019 – Technical assistance to CE
- March 2019 – Second complaint filed
- May 2019 – OCR informed CE of 2nd complaint
- May 2019 – Records Provided
- **$85,000** settlement
- 1 year corrective action plan

Best Practices

- Risk analysis and risk management should be integrated into business processes; conducted regularly and when new technologies and business operations are planned
- Incorporate lessons learned from incidents into the overall security management process
- Review Records Access Policies, Procedures and Practices
- Train staff on the difference between Right of Access requests and authorizations
- Provide training specific to organization and job responsibilities and on regular basis; reinforce workforce members' critical role in protecting privacy and security
- Review all vendor and contractor relationships to ensure BAAs are in place as appropriate and address breach/security incident obligations

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.

Connect with Us

Office for Civil Rights

U.S. Department of Health and Human Services

www.hhs.gov/hipaa

Join our Privacy and Security listserves 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