Update on HIPAA Enforcement

Serena Mosley-Day

Senior Advisor for HIPAA Compliance & Enforcement
Office for Civil Rights (OCR)
U.S. Department of Health and Human Services

Updates

- Policy
- Breach
- Enforcement

Policy Update

Policy Update

Apps, APIs and the HIPAA Right of Access FAQs

- In April 2019, OCR issued new FAQs addressing the applicability of HIPAA to the use of software applications (apps) by individuals to receive health information from their providers.
- Provides guidance for covered entities, EHR developers and app developers.
- Reiterates the importance of HIPAA's right to access for individuals.
- https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access-right-health-apps-apis/index.html

Policy Update: Direct Liability of Business Associates

Business associates are directly liable for HIPAA violations as follows:

- Failure to provide the Secretary with records and compliance reports; cooperate with complaint investigations and compliance reviews; and permit access by the Secretary to information, including protected health information (PHI), pertinent to determining compliance.
- Taking any retaliatory action against any individual or other person for filing a HIPAA complaint, participating in an investigation or other enforcement process, or opposing an act or practice that is unlawful under the HIPAA Rules.
- Failure to comply with the requirements of the Security Rule.
- Failure to provide breach notification to a covered entity or another business associate.
- Impermissible uses and disclosures of PHI.

Policy Update: Direct Liability of Business Associates

Business associates are directly liable for HIPAA violations as follows:

- Failure to disclose a copy of electronic PHI (ePHI) to either the covered entity, the individual, or the individual's designee (whichever is specified in the business associate agreement) to satisfy a covered entity's obligations regarding the form and format, and the time and manner of access under 45 C.F.R. §§ 164.524(c)(2)(ii) and 3(ii), respectively.
- Failure to make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.
- Failure, in certain circumstances, to provide an accounting of disclosures.
- Failure to enter into business associate agreements with subcontractors that create or receive PHI on their behalf, and failure to comply with the implementation specifications for such agreements.
- Failure to take reasonable steps to address a material breach or violation of the subcontractor's business associate agreement.

Policy Update: Direct Liability of Business Associates

- Notably, OCR lacks the authority to enforce the "reasonable, cost-based fee" limitation in 45 C.F.R. § 164.524(c)(4) against business associates because the HITECH Act does not apply the fee limitation provision to business associates. A covered entity that engages the services of a business associate to fulfill an individual's request for access to their PHI is responsible for ensuring that, where applicable, no more than the reasonable, cost-based fee permitted under HIPAA is charged. If the fee charged is in excess of the fee limitation, OCR can take enforcement action against only the covered entity.
- https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/factsheet/index.html

Breach Update

Breach Update

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 Update

Breach Reporting – What Should be Reported?

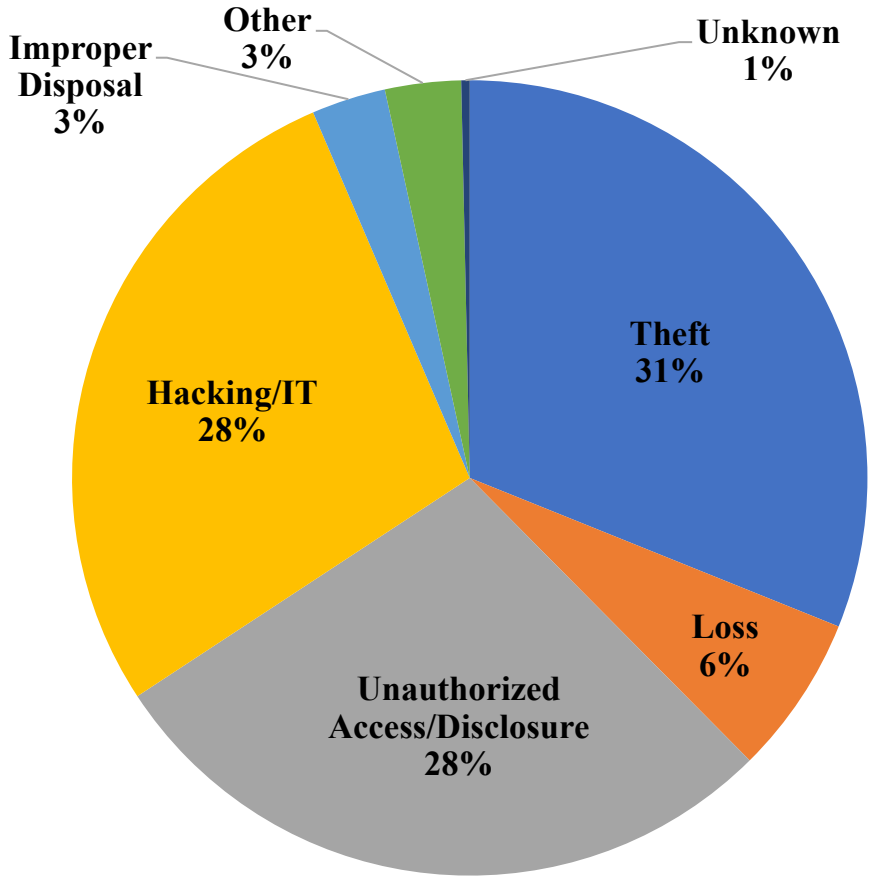
- "Acquisition, access, use, or disclosure of protected health information in a manner not permitted under [the Privacy Rule] which compromises the security or privacy of the protected health information."
- Presumption of breach unless a covered entity or business associate can demonstrate a low probability that PHI has been compromised based on at least the following factors:
    - Nature and extent of PHI
    - The person who used or received the PHI
    - Whether PHI was actually viewed or acquired
    - Extent risk has been mitigated
- Breach risk assessment
    - Must be documented

Breach Update

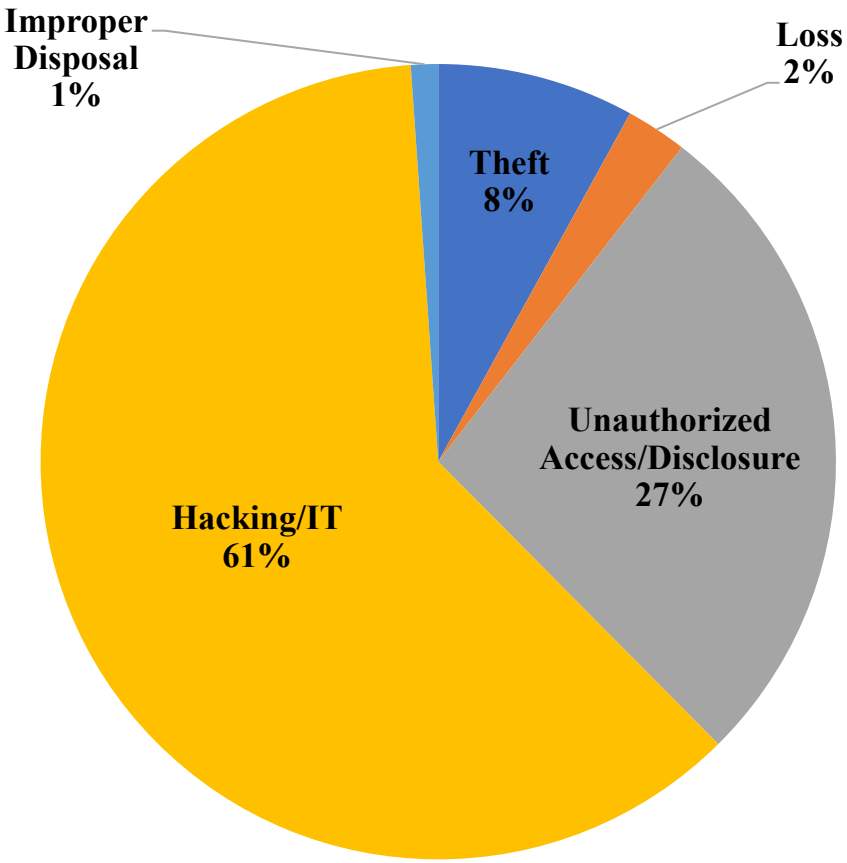
- OCR posts breaches affecting 500+ individuals on OCR website (after verification of report)
  - Public can search and sort posted breaches
  - Approx. 350 500+ breach reports per year
- OCR investigates every breach affecting 500+ individuals
- Investigations involve looking at:
  - Underlying cause of the breach
  - Actions taken to respond to the breach (including compliance with breach notification requirements) and prevent future incidents
  - Entity's compliance prior to breach

Breach Update

500+ Breaches by Type of Breach

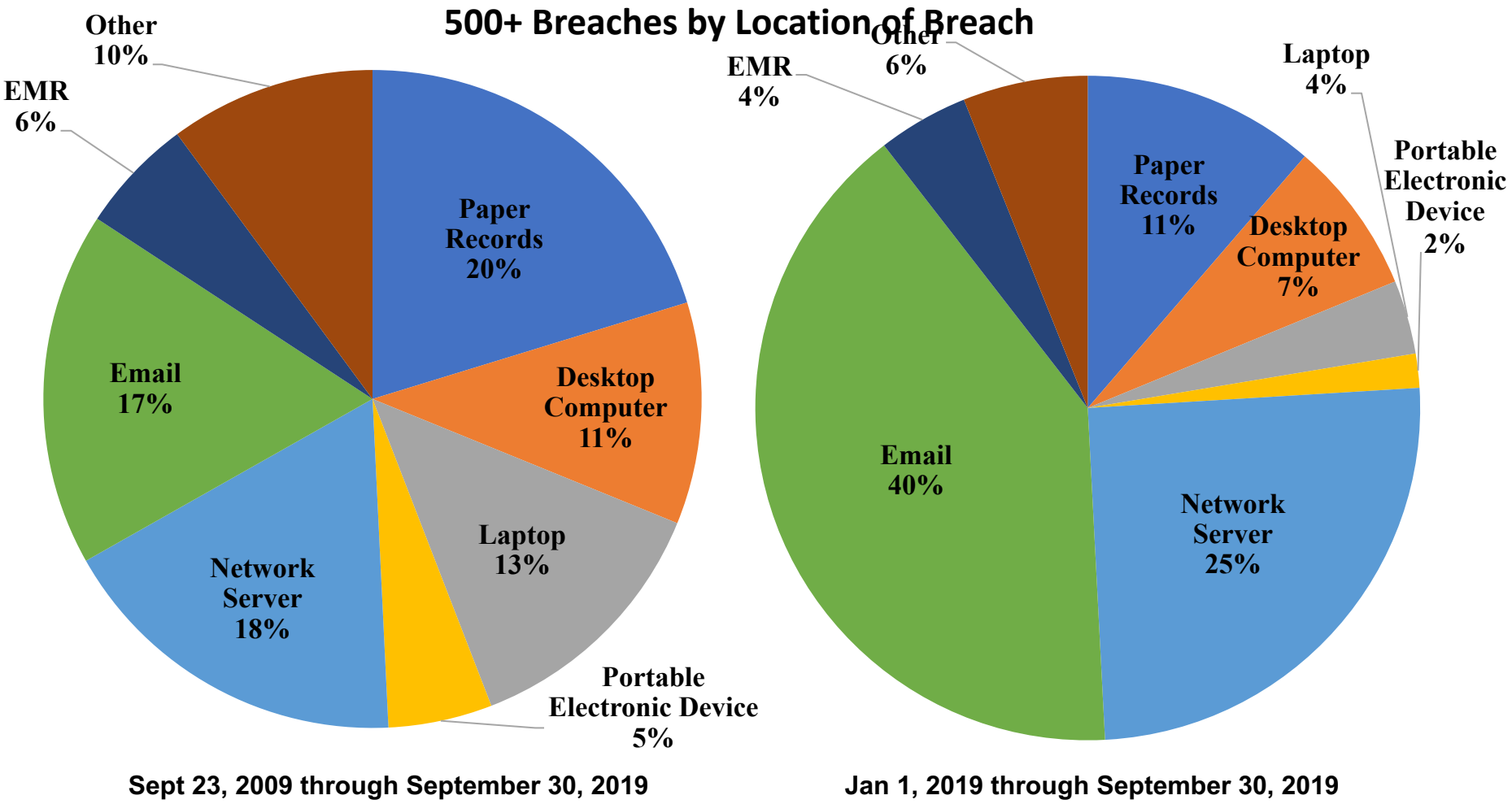


Sept 23, 2009 through September 30, 2019

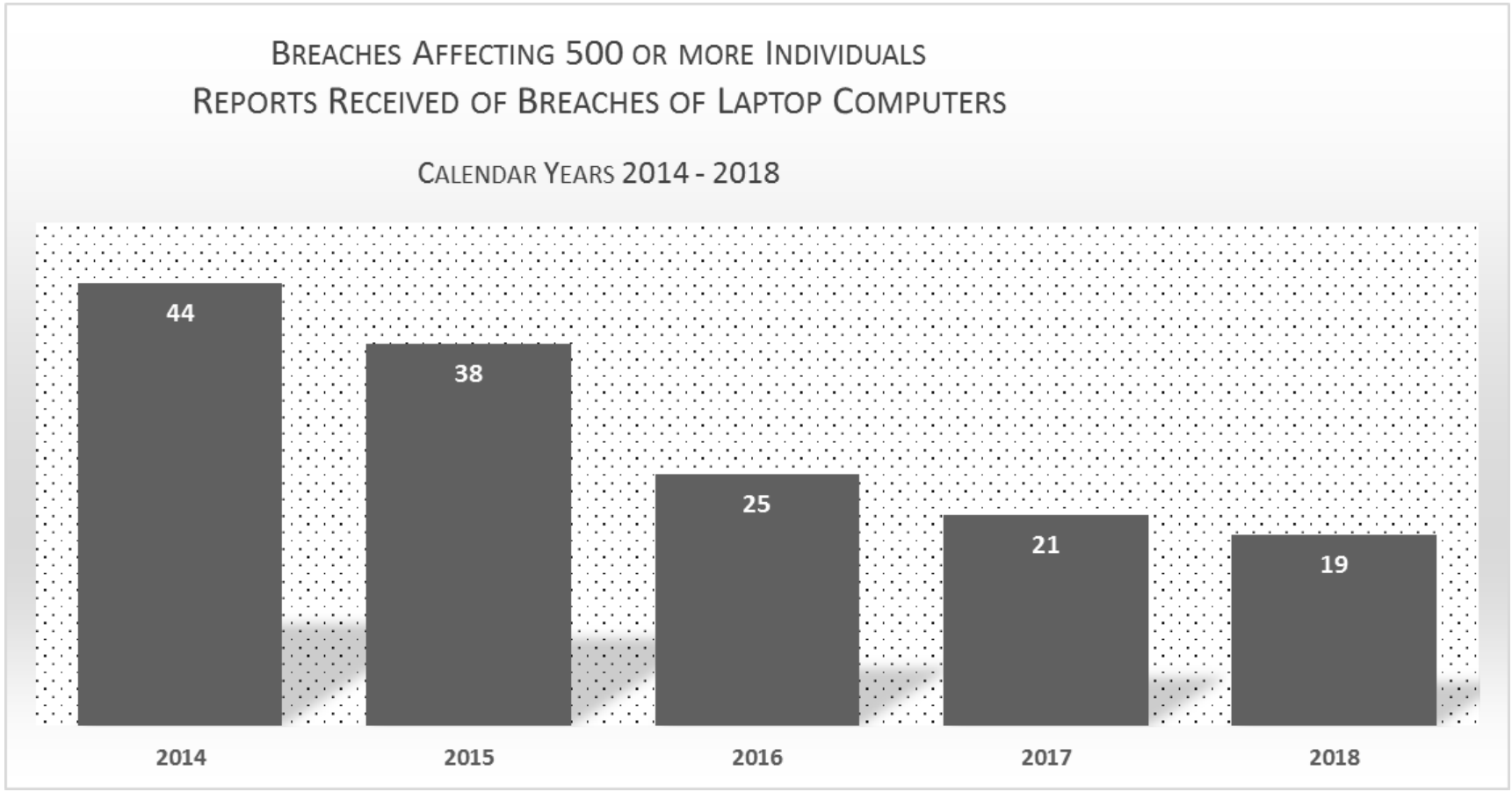


Jan 1, 2019 through September 30, 2019

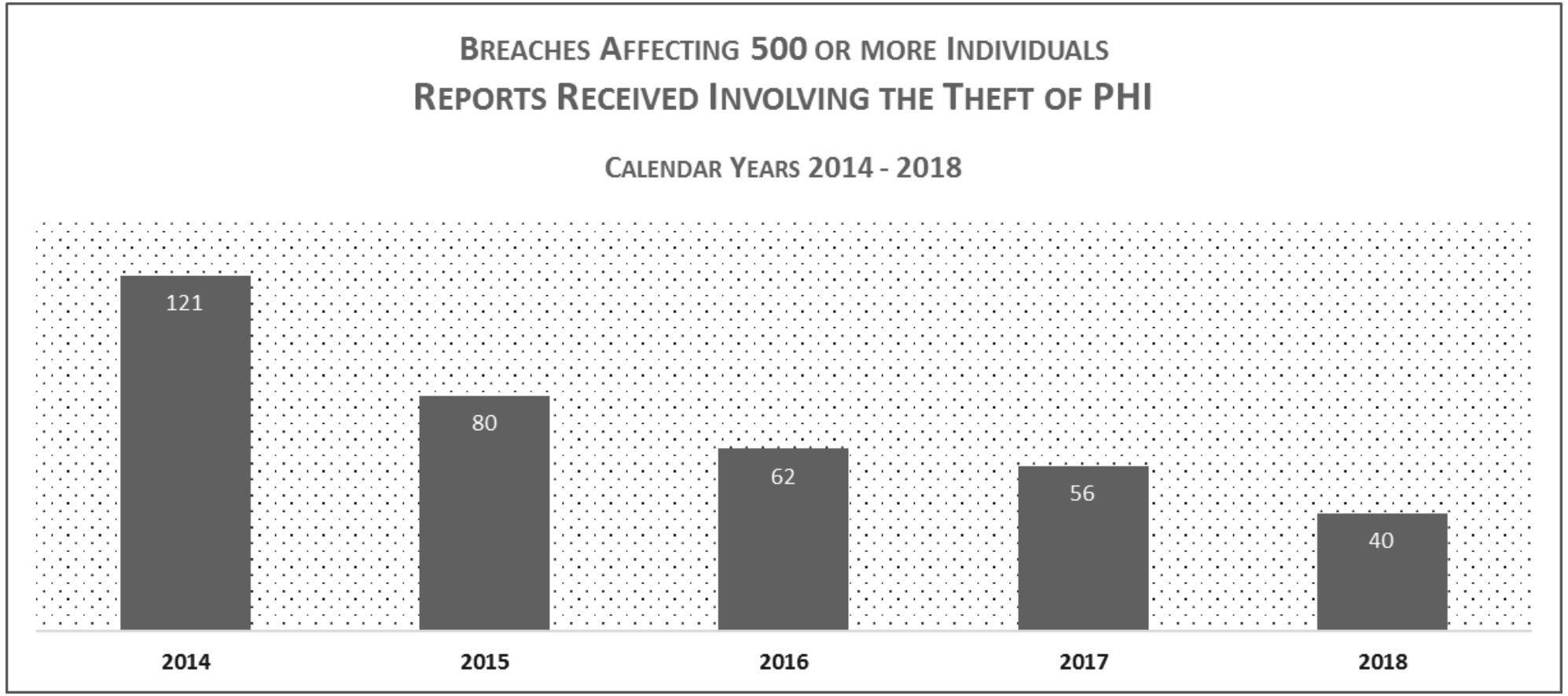
Breach Update



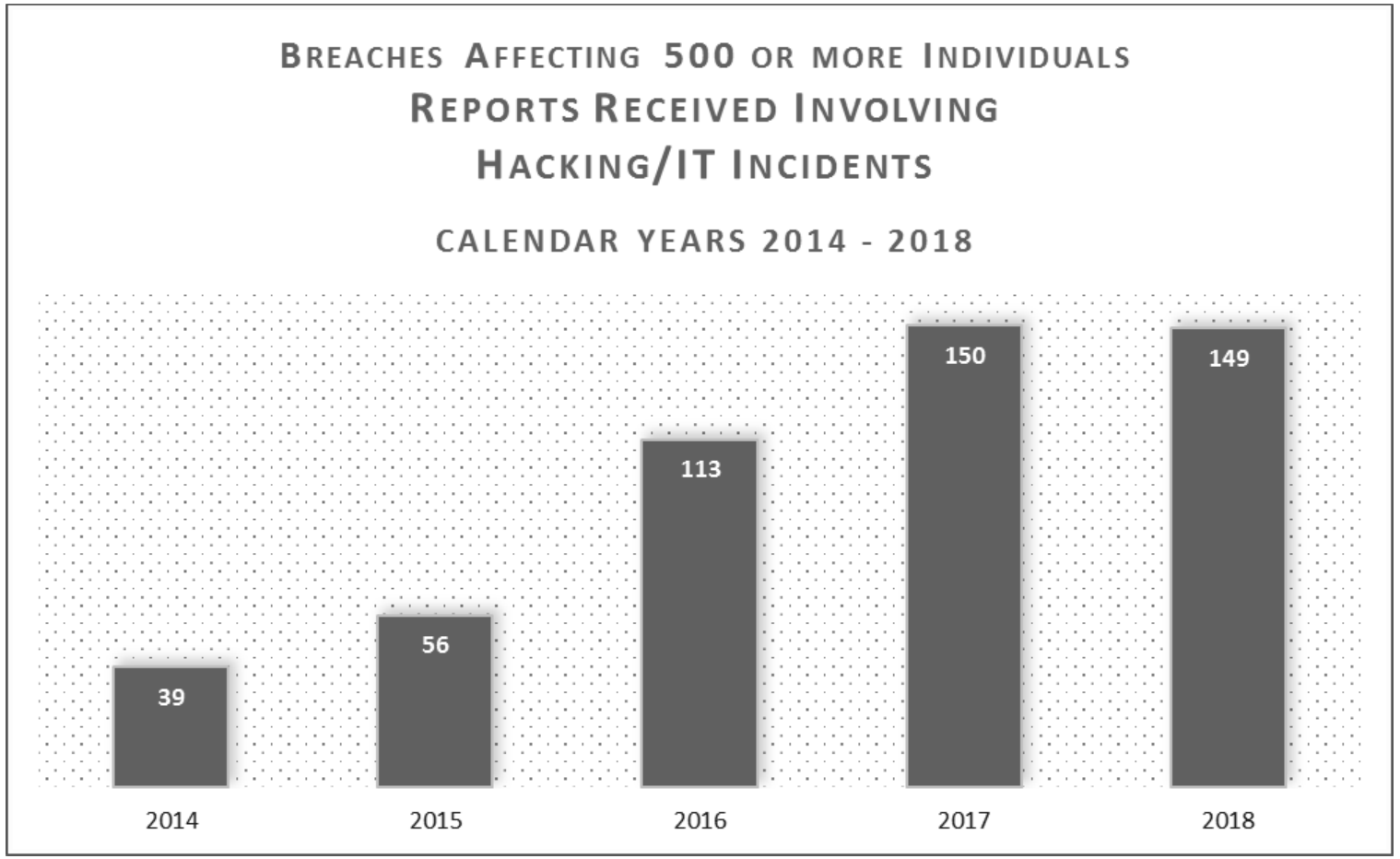
Breach Update



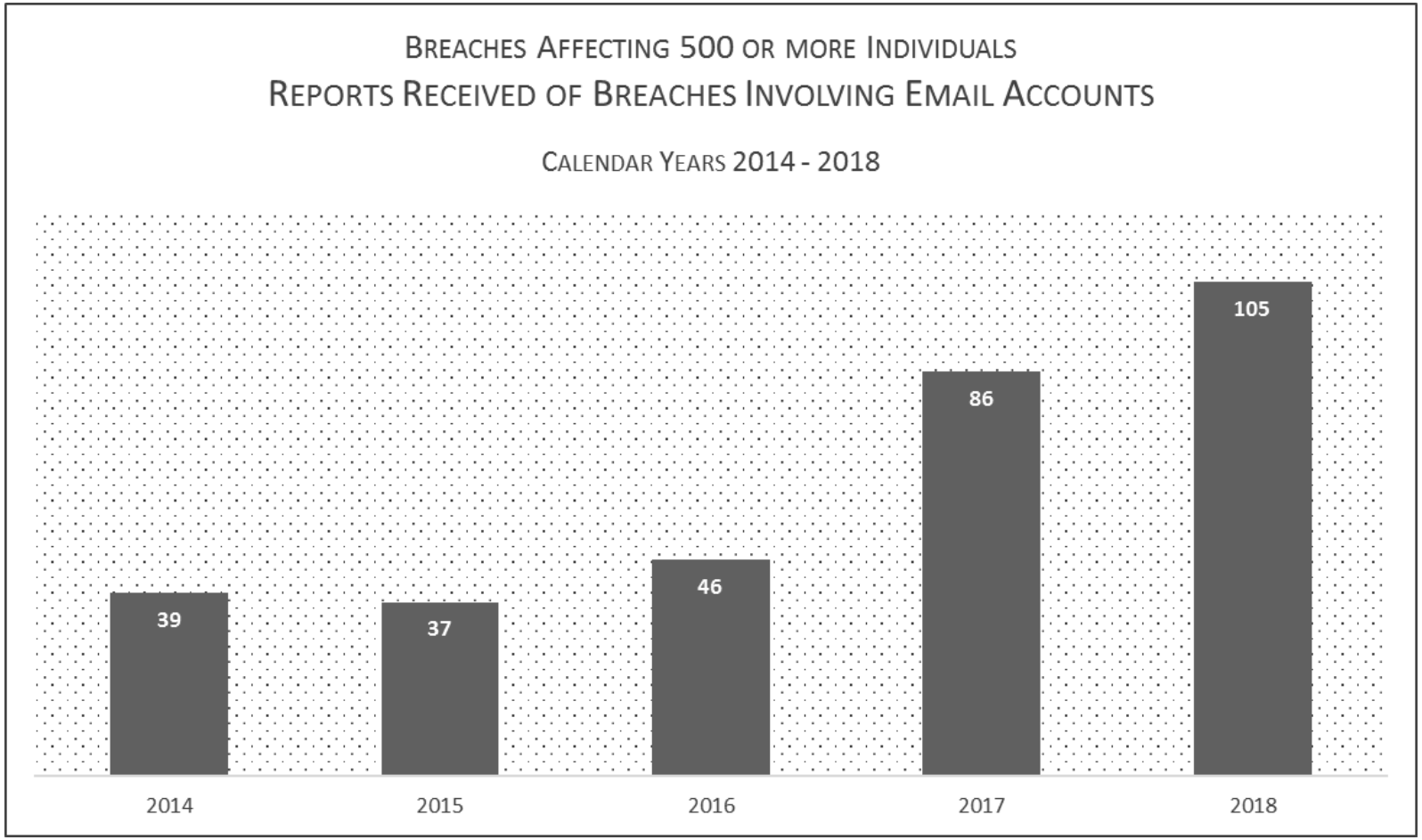
Breach Update



Breach Update



Breach Update



Cyber Security and Ransomware

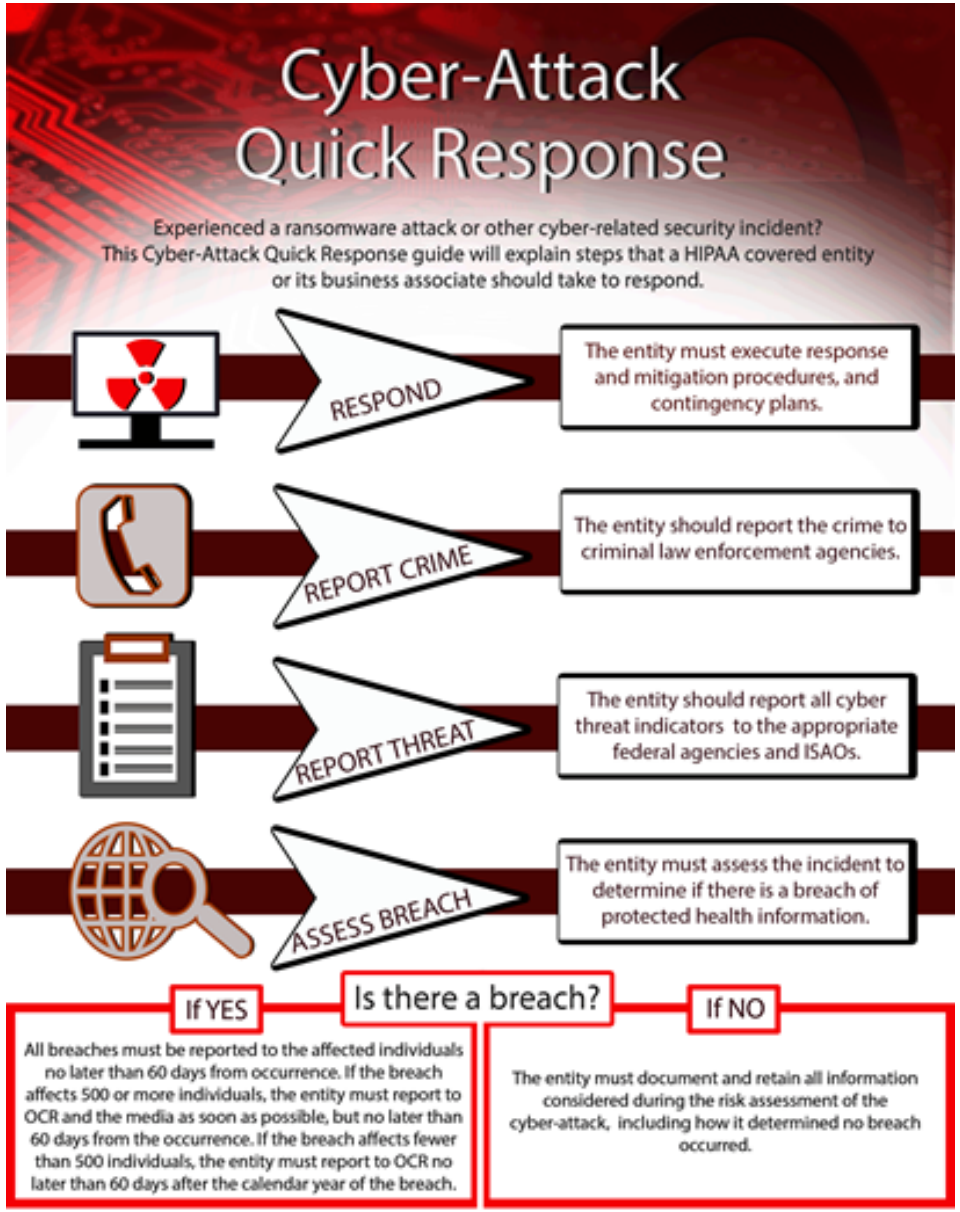
- Following the May 2017 WannaCry ransomware attack, HHS reminded organizations to adhere to the OCR ransomware guidance as part of strong cyber hygiene.
- <u>OCR presumes a breach in the case of a ransomware attack.</u>

"Maintaining frequent backups and ensuring the ability to recover data from backups is crucial to recovering from a ransomware attack."

Cyber Security

Fact Sheet: Ransomware and HIPAA

www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf



Enforcement Update

Enforcement Update

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.

Enforcement Update

General HIPAA Enforcement Highlights

- Expect to receive over 26,000 complaints this year
- In most cases, entities 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
  - 63 settlement agreements that include detailed corrective action plans and monetary settlement amounts
- 4 civil money penalties

As of September 30, 2019

Enforcement Update

Recent Enforcement Actions

9/2018	Brigham and Women's Hospital	$384,000
9/2018	Massachusetts General Hospital	$515,000
9/2018	Advanced Care Hospitalists	$500,000
10/2018	Allergy Associates of Hartford	$125,000
10/2018	Anthem	$16,000,000
11/2018	Pagosa Springs Medical Center	$111,400
12/2018	Cottage Health	$3,000,000
4/2019	Touchstone Medical Imaging	$3,000,000
4/2019	Medical Informatics Engineering	$100,000
9/2019	Bayfront Health St. Petersburg	$85,000
9/2019	Elite Dental	$10,000

Enforcement Update

Recurring Compliance Issues

- Right of Access
- Business Associate Agreements
- Risk Analysis
- Impermissible Disclosures
- Failure to Manage Identified Risk, e.g. Encrypt
- Lack of Transmission Security
- Lack of Appropriate Auditing
- Insider Threat

Enforcement Update

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).

- OCR Right of Access guidance - www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html

Enforcement Update

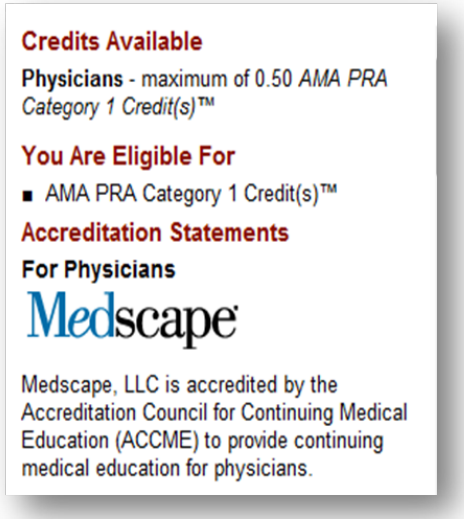
Bayfront Health - St. Petersburg:

- 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

Enforcement Update

Provider Education:

An Individual's Right to Access and Obtain their Health Information Under HIPAA



- Web-based Video Training for Free Continuing Medical Education and Continuing Education Credit for Health Care Professionals via Medscape
- 70,000+ health care providers and allied health professionals trained
  - http://www.medscape.org/viewarticle/876110

Enforcement Update

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 §§ 164.502(e), 164.504(e), and 164.308(b).

The HIPAA Omnibus Rule, issued in January 2013, changed the standards for BAAs

- Modified BAA requirements
- Must execute a BAA that includes the modified provisions
- Compliance date: September 23, 2013

Enforcement Update

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

Enforcement Update

Risk Analysis: Incomplete or Inaccurate

- Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the [organization]. See 45 C.F.R. § 164.308(a)(1)(ii)(A).

Enforcement Update

Medical Informatics Engineering

- Breach report received through breach portal
- Hackers used user ID and password to get ePHI of 3.5 million people
  - Including names, addresses, DOB, SSN, email addresses, clinical information and health insurance information
- Included information held by subsidiary-NoMoreClipboard
- Impermissible disclosure to hackers
- No comprehensive risk analysis
- $100,000 settlement
- 2 year corrective action plan

Enforcement Update

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 CFR 164.530(c).

Enforcement Update

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

Enforcement Update

Pagosa Springs Medical Center

- Originated as a complaint
- PSMC is a critical access hospital
- Former employee continued to have remote access to online scheduling calendar, which ePHI, after employment ended
  - Termination procedures insufficient – did not deactivate username and password
- No BAA with the online scheduling calendar (Google)
- $111,400 settlement
- 2 year corrective action plan

Enforcement Update

Corrective Actions May Include:

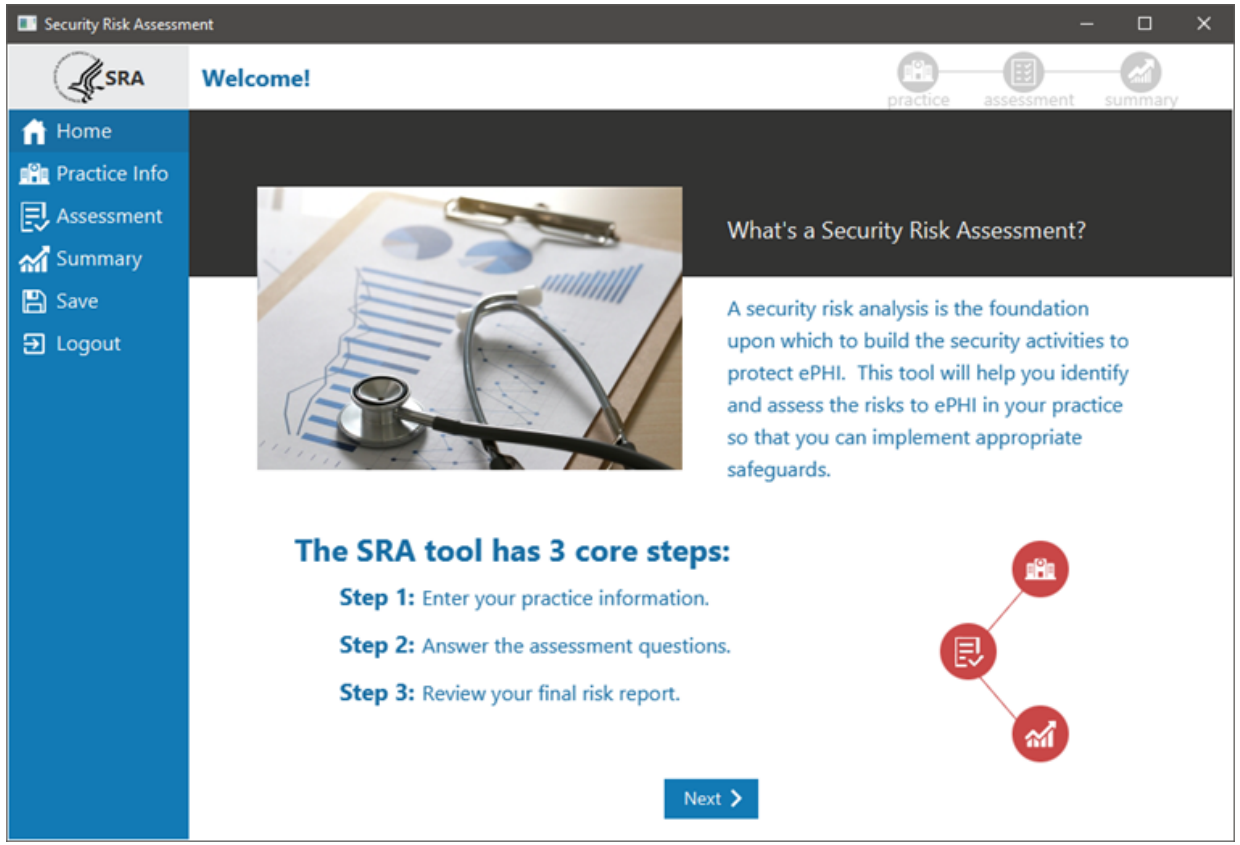
- Updating risk analysis and risk management plans
- Updating policies and procedures
- Evaluating vendor/contractor relationships and updating BAAs
- Training of workforce
- Implementing specific technical or other safeguards
- Monitoring

Enforcement Update

Best Practices to Consider

- 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
- Review access request policies, procedures and training. Ensure workforce members are aware of the difference between authorizations and right of access requests
- 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

Enforcement Update



SRA 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.

https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
Office for Civil Rights

Connect with Us

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