HIPAA

Common Compliance Issues and Recent Enforcement Activities

OFFICE FOR CIVIL RIGHTS (OCR)
U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

BARBARA STAMPUL
DEPUTY REGIONAL MANAGER
SOUTHEAST REGION

SEPTEMBER 25, 2019

What is the Office for Civil Rights (OCR)?

- U.S. Department of Health and Human Services
- As the Department's civil rights, conscience and religious freedom, and health privacy rights law enforcement agency, OCR investigates complaints, enforces rights, and promulgates regulations, develops policy and provides technical assistance and public education to ensure understanding of and compliance with non-discrimination and health information privacy laws.
- Enforces the HIPAA Privacy, Security, and Breach Notification Rules

OCR's Mission and Vision

- **Mission**

  The mission of the Office for Civil Rights is to improve the health and well-being of people across the nation; to ensure that people have equal access to and the opportunity to participate in and receive services from HHS programs without facing unlawful discrimination; and to protect the privacy and security of health information in accordance with applicable law.

- **Vision**

  Through investigations, voluntary dispute resolution, enforcement, technical assistance, policy development and information services, OCR will protect the civil rights of all individuals who are subject to discrimination in health and human services programs and protect the health information privacy rights of consumers.

Major Laws Enforced By OCR

- Title VI of the Civil Rights Act of 1964
- Section 504 of the Rehabilitation Act of 1973
- Title II of the Americans with Disabilities Act of 1990
- The Age Discrimination Act of 1975
- Section 1557 of the Affordable Care Act
- HIPAA Privacy, Security, and Breach Notification Rules

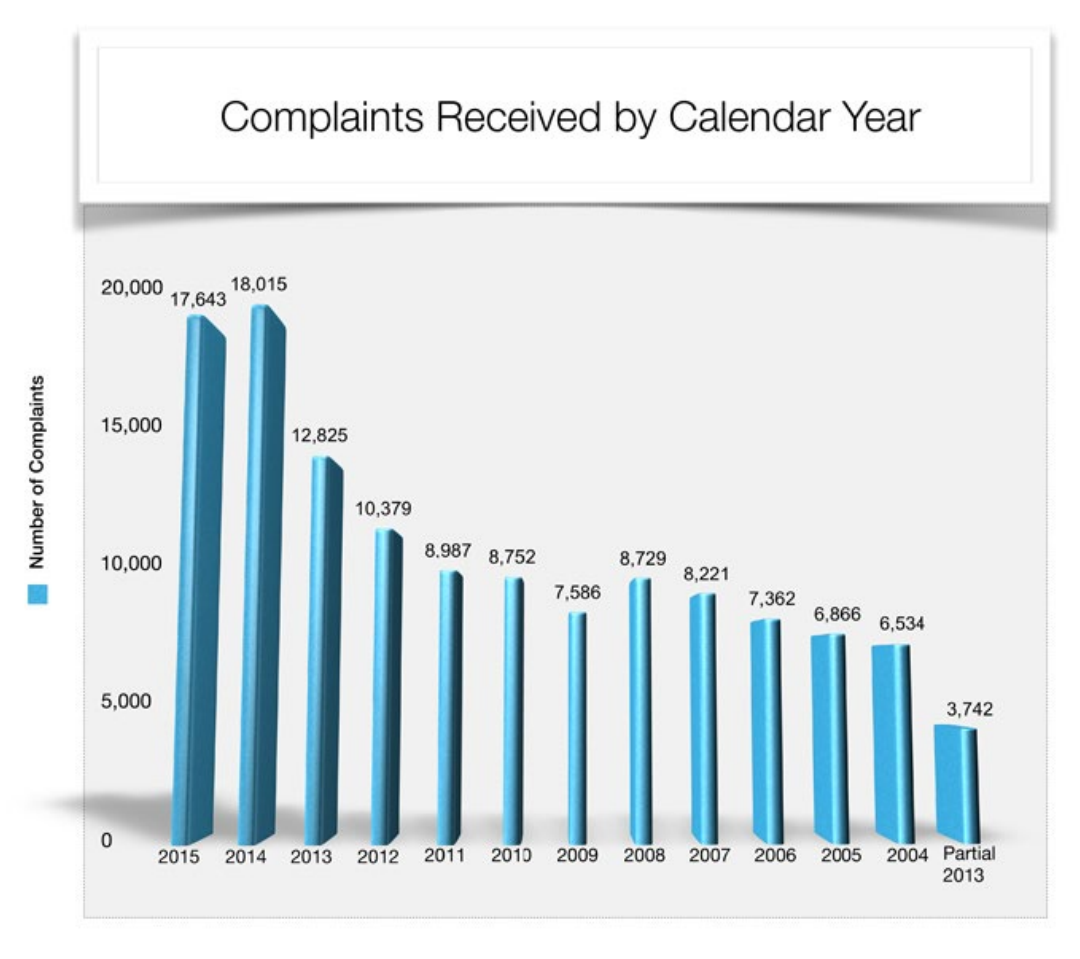
What do we do?

- Enforcement and Compliance Activities
  - Complaint Investigations
  - Compliance Reviews
  - Voluntary Resolution Agreements
  - Formal Enforcement
  - Audits
  - Outreach and Public Education
  - Policy Development

HIPAA: Who is Covered?

- Limited by law to:
  - "Covered Entities" (CEs):
  - Health care providers who transmit health information electronically in connection with a transaction for which there is a HIPAA standard
  - **Health plans**
  - Health care clearinghouses
  - Business Associates

HIPAA Complaints



Top Five Issues in Investigated Cases Closed with Corrective Action

Year	Issue 1	Issue 2	Issue 3	Issue 4	Issue 5
2015	Impermissible Uses & Disclosures	Safeguards	Administrative Safeguards	Access	Technical Safeguards
2014	Impermissible Uses & Disclosures	Safeguards	Administrative Safeguards	Access	Technical Safegards
2013	Impermissible Uses & Disclosures	Safeguards	Access	Administrative Safeguards	Minimum Necessary
2012	Impermissible Uses & Disclosures	Safeguards	Administrative Safeguards	Access	Minimum Necessary
2011	Impermissible Uses & Disclosures	Safeguards	Access	Notice to Individuals	Minimum Necessary
2010	Impermissible Uses & Disclosures	Safeguards	Access	Minimum Necessary	Complaints

OCR Updates

- Policy Development
- Breach Notification
- Enforcement

Recent Security Rule Guidance Material

- **Cloud Service Provider**
  - OCR released guidance clarifying that a CSP is a business associate – and therefore required to comply with applicable HIPAA regulations – when the CSP creates, receives, maintains or transmits identifiable health information (referred to in HIPAA as electronic protected health information or ePHI) on behalf of a covered entity or business associate.

    http://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html
- **Ransomware**

  https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html
  - OCR recently released guidance on ransomware. The new guidance reinforces activities required by HIPAA that can help organizations prevent, detect, contain, and respond to threats.
  - Includes guidance on security incident procedures, prevention techniques, and assessing whether a HIPAA breach has occurred

Ransomware

Prevention:

- Know your threats and vulnerabilities by conducting a thorough risk analysis
  - Mitigate and remediate identified risks
- Update antivirus and malware software—early detection and response is key!
- Train users to identify and report
  - Social engineering, increase in CPU activity, files missing, suspicious network activity, etc.
- Limit technical access—*including vendors*
- Frequent backups to ensure continuity
- Routinely test contingency plans

Response:

Activate Security Incident Procedures (NIST SP 800-61, Rev.2) to include:

- Identifying and analyzing scope of damage—what is affected, is it still going, etc.
- Containing impact and propagation
- Eradicating the malware and remediating cause of intrusion

Recovery:

- Restore lost data and continue operations
- Consider notifying local FBI or U.S. Secret Service field office
- Review any other required actions (under HIPAA, per contractual relationship, etc.)

Common Breaches & Compliance Issues

- Lack of Business Associate agreements
- Insufficient Risk Analysis and failure to manage identified risks
- Failure to Manage Identified Risk
- Lack of transmission security (i.e. Encryption)
- Lack of appropriate auditing and review of user activity
- Failure to patch/update software (antivirus, malware)
- Insider threat (bad actors)
- Improper disposal (paper and electronic PHI)
- Failure to regularly train workforce
- Failure to restrict access to minimum necessary
- Improper Disposal
- Insufficient Data Backup and Contingency Planning
- Compliance with Individual's Right to Access medical records

Risk Analyses

- CE/BA must 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 entity. See 45 C.F.R. § 164.308(a)(1)(ii)(A).
- Organizations frequently underestimate the proliferation of ePHI within their environments. Identify all ePHI created, maintained, received or transmitted. Be sure to consider:
  - Applications (EHR, PM, billing systems; documents and spreadsheets; database systems and web servers; fax servers, backup servers; etc.)
  - Computers (servers, workstations, laptops, virtual and cloud based systems, etc.)
  - Medical Devices (tomography, radiology, DXA, EKG, ultrasounds, spirometry, etc.)
  - Messaging Apps (email, texting, ftp, etc.)
  - Mobile and Other Devices (tablets, smartphones, copiers, digital cameras, etc.)
  - Media (tapes, CDs/DVDs, USB drives, memory cards, etc.)

Risk Analysis Guidance

- http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidance.html
- http://scap.nist.gov/hipaa/
- http://www.healthit.gov/providers-professionals/security-risk-assessment

Corrective Action after a Breach

- Update risk analysis and management plan
- Review and revise policies and procedures
- Re-training workforce
- Sanctions as appropriate
- Implementation of specific technical or other safeguards
- Mitigation
- CAPs may include monitoring

Enforcement

Investigations involve analyzing:

- Underlying cause of the breach
- Actions taken to respond to the breach, including compliance with notification requirements
- Actions taken to prevent future incidents
- Compliance prior to the breach

Enforcement action is warranted in cases where entities are unreceptive to OCR's technical assistance or systemic noncompliance is evident

BREACHES

BREACH HIGHLIGHTS AND RECENT ENFORCEMENT ACTIVITY

BREACHES

What is a Breach?

- **Definition of a Breach: *See* § 164.402**
  - A breach means the acquisition, access, use or disclosure of protected health information … which compromises the security or privacy of the protected health information.
- *OCR Discretion: A breach of PHI is **presumed a breach** unless a CE or BA demonstrates a low probability of compromise based on a **risk assessment**.*
- **Low probability of Compromise- 4 factor test**
  - Examples: Burglarized storage unit vs. Landlord-Tenant dispute

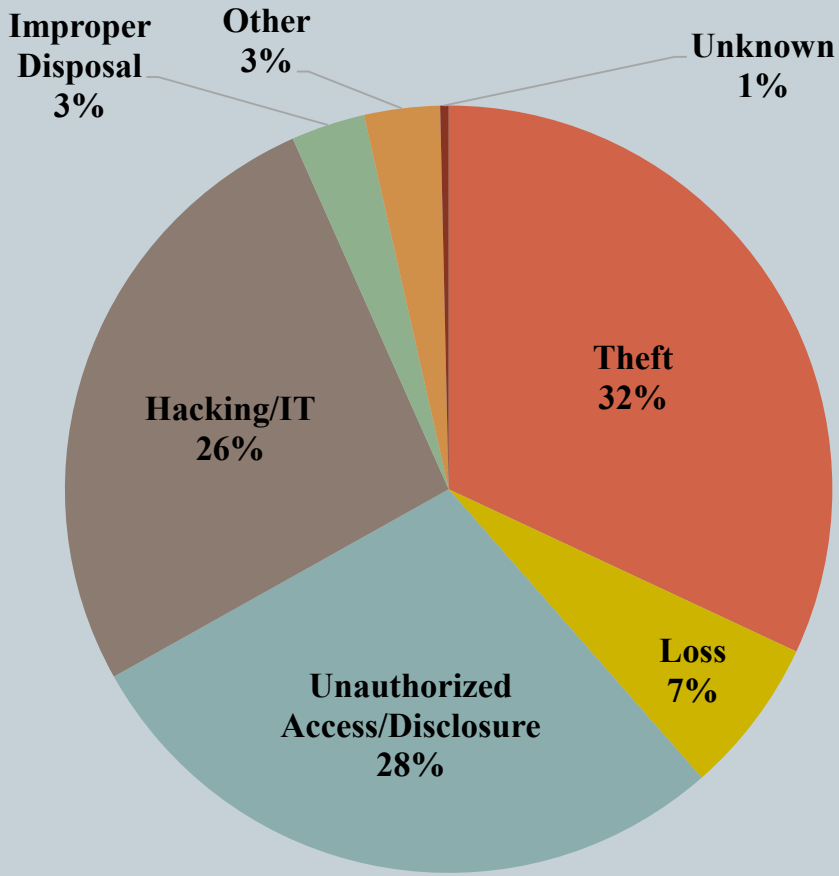
Breach Notification Requirements

- Covered entity must notify affected individuals, HHS, and in some cases, the media, of breach
- Business associate must notify covered entity of 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
- OCR posts breaches affecting 500+ individuals on OCR website

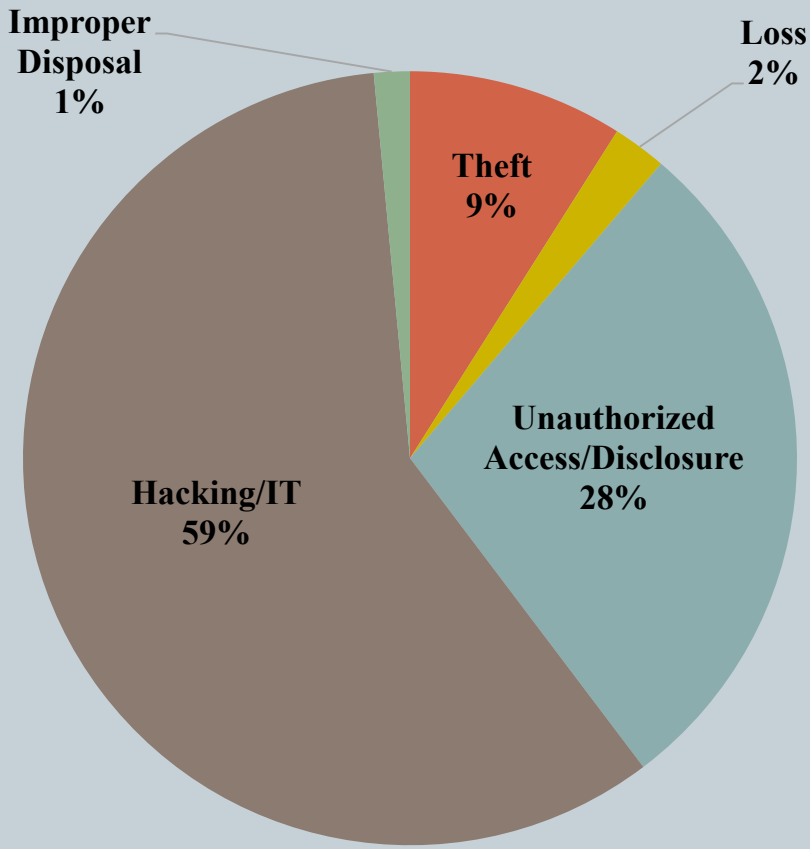
September 2009 through July 2019

BREACH PATTERNS OVER THE YEARS

500+ Breaches by Type of Breach

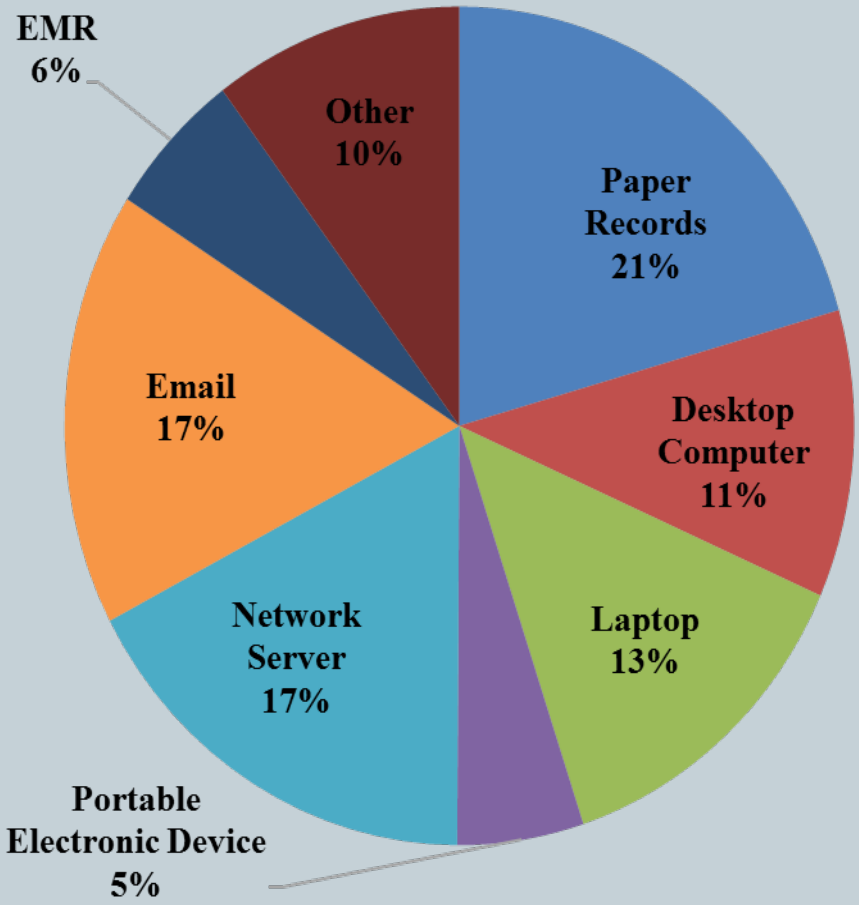


Sept 23, 2009 through July 31, 2019

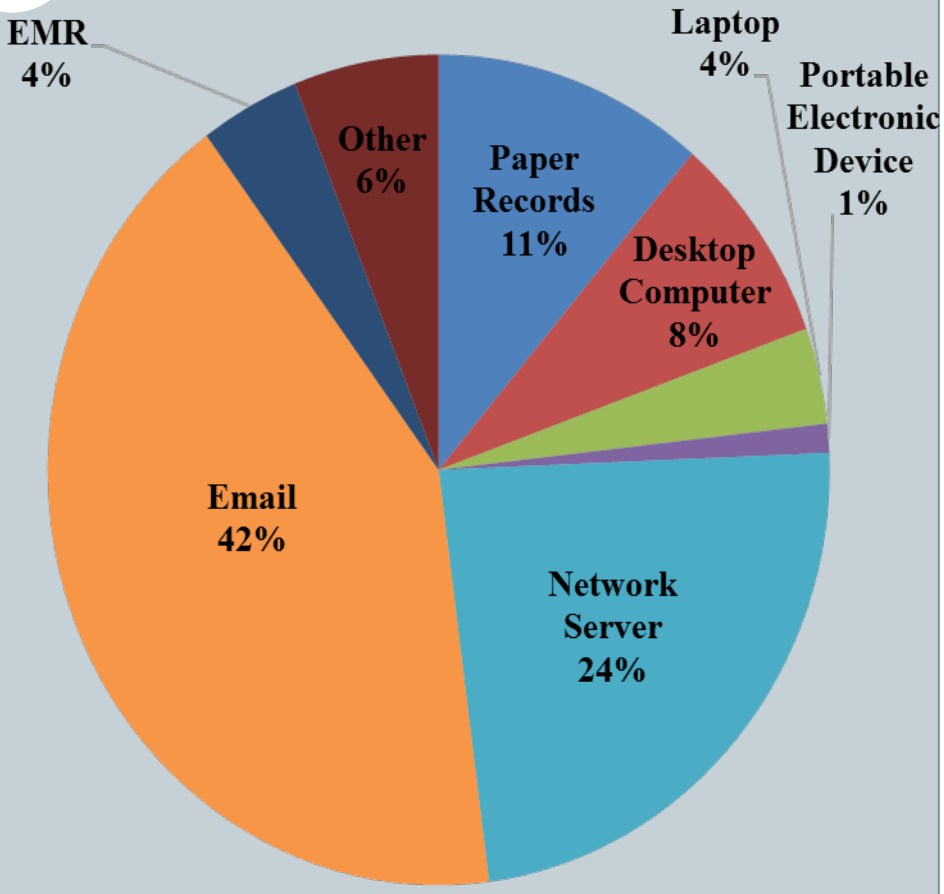


Jan 1, 2019 through July 31, 2019

500+ Breaches by Location as of Breach



Sept 23, 2019 through July 31, 2019

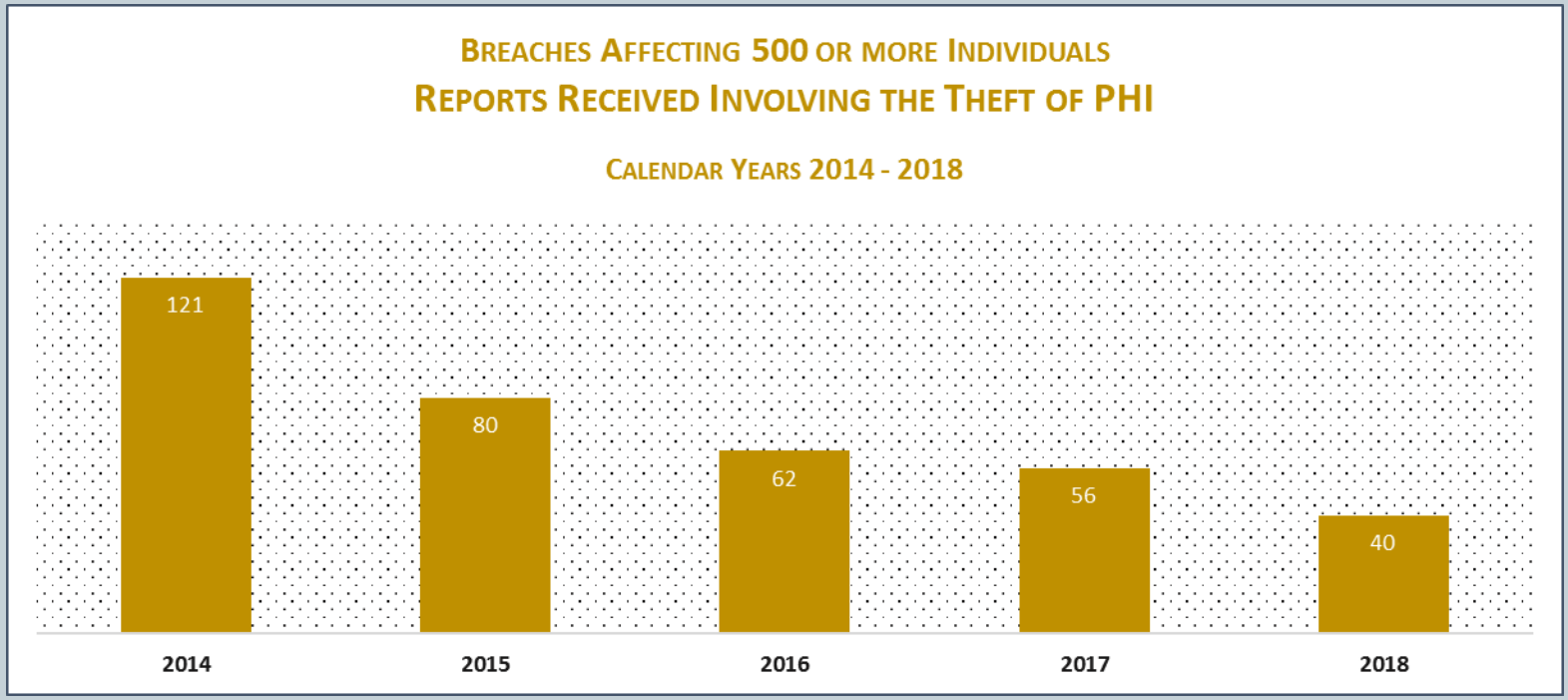


Jan 1, 2019 through July 31, 2019

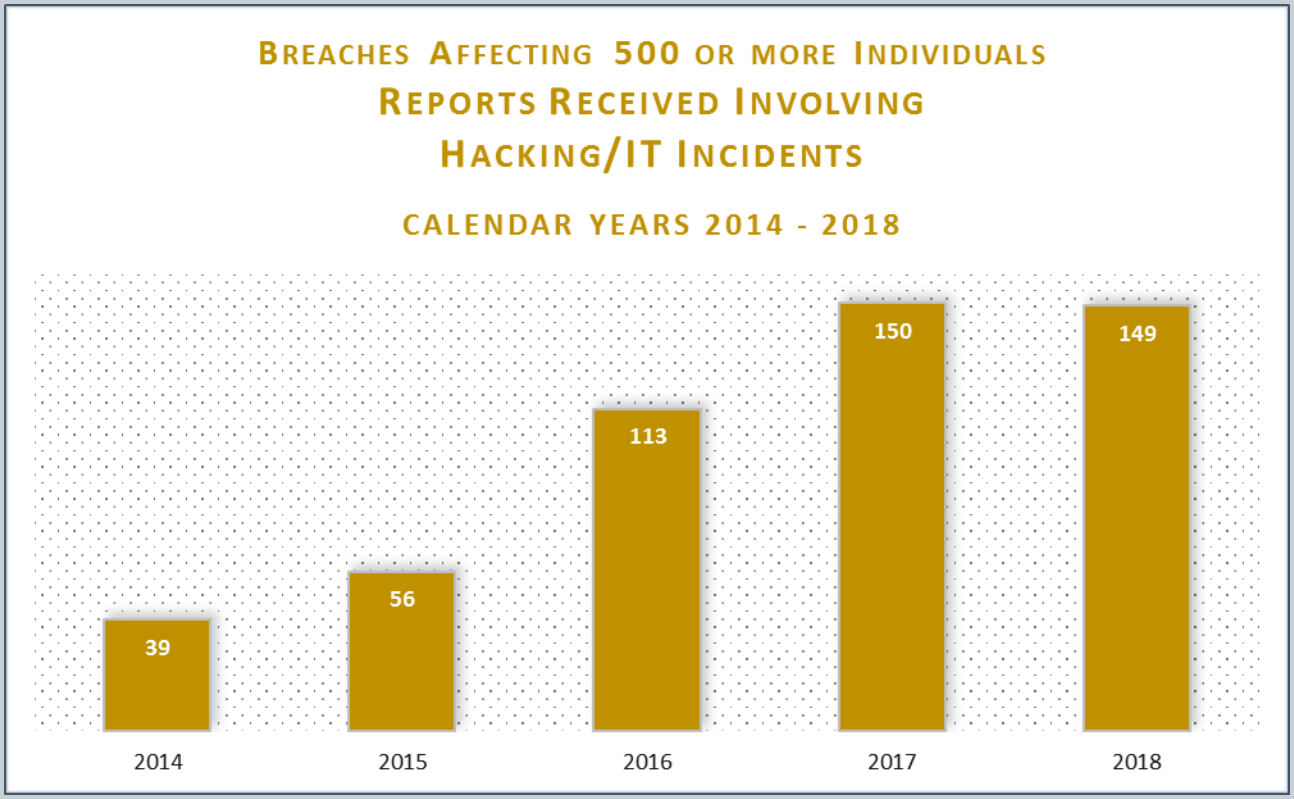
Breach Investigations

- OCR posts breaches affecting 500+ individuals on OCR website (after verification of report)
  - Public can search and sort posted breaches
- OCR opens investigations into breaches affecting 500+ individuals, and into number of smaller breaches
- 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

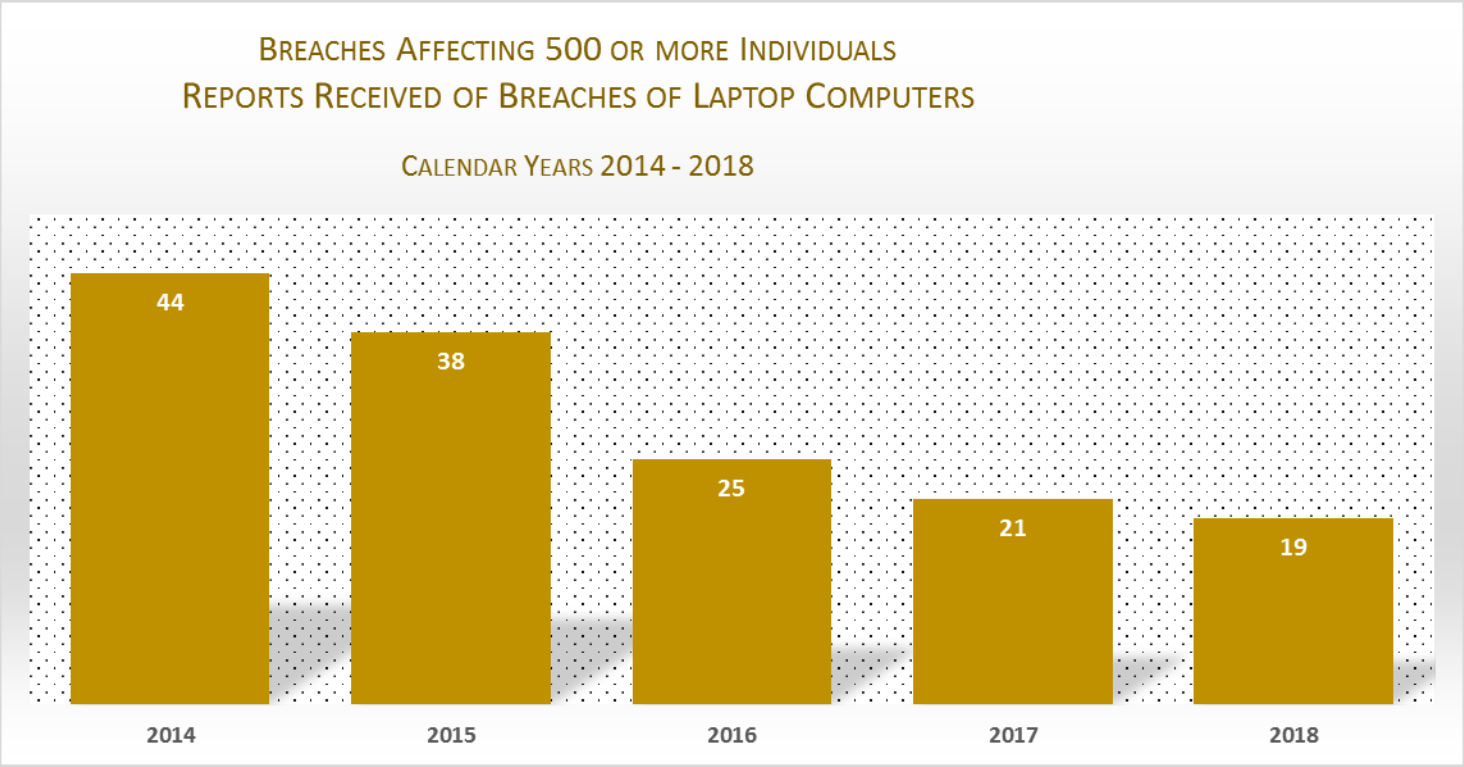
Breach Statistics



Breach Statistics



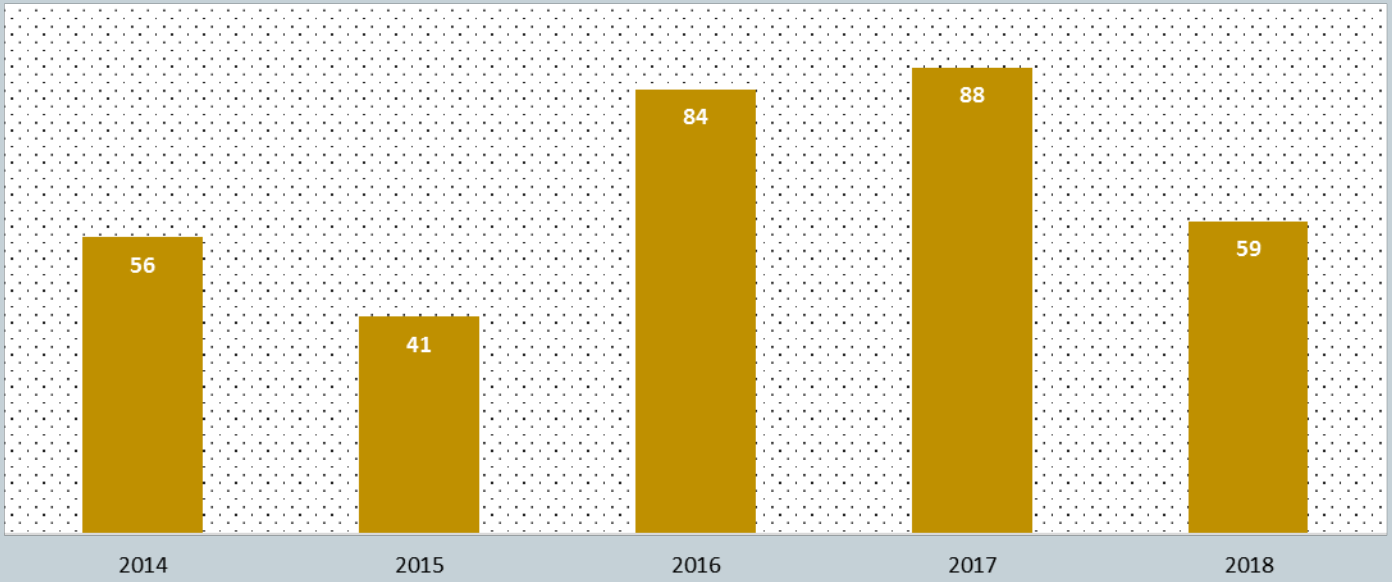
Breach Statistics



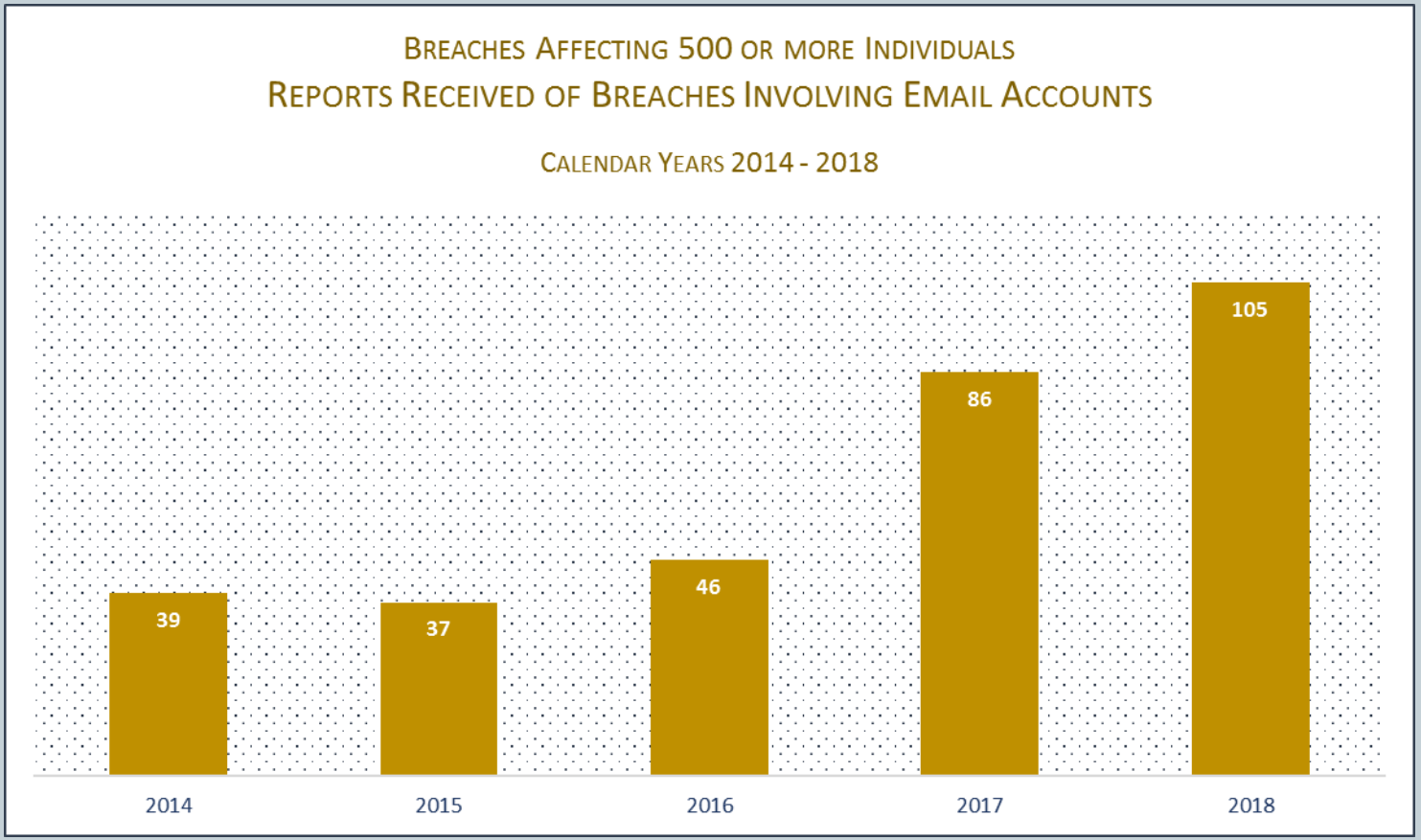
Breach Statistics

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

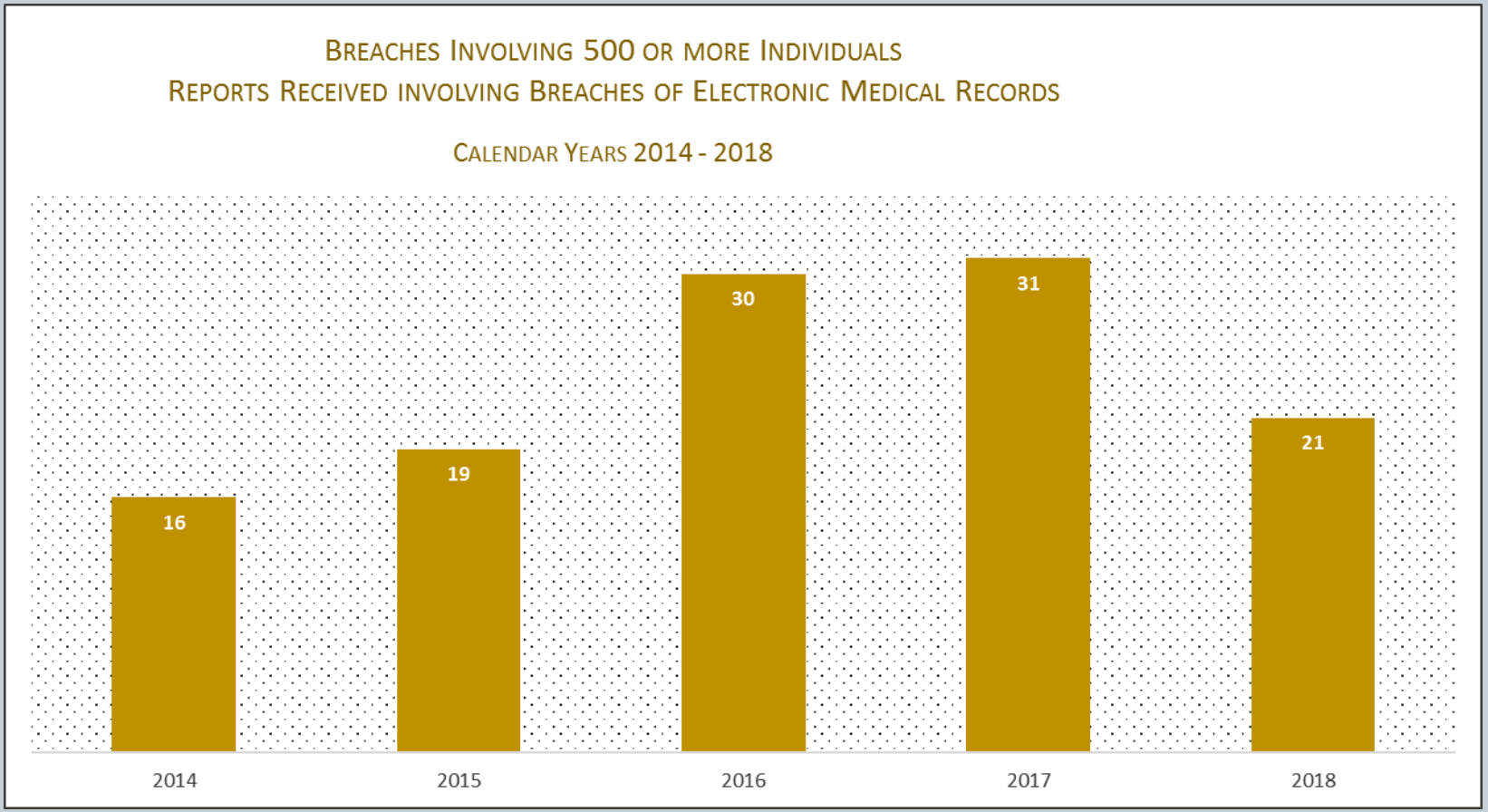
Calendars Years 2014 - 2018



Breach Statistics



Breach Statistics



Breach Review Observations

- In most cases, entities able to demonstrate satisfactory compliance through voluntary cooperation and corrective action
- In some cases though, nature or scope of indicated noncompliance warrants additional enforcement action
- Resolution Agreements/Corrective Action Plans
  - 62 settlement agreements that include detailed corrective action plans and monetary settlement amounts
- 4 civil money penalties

As of July 31, 2019

Recent Enforcement Activities

9/2018	Boston Medical Center	$100,000
9/2018	Brigham and Women's Hospital	$384,000
9/2018	Massachusetts General Hospital	$515,000
10/2018	Anthem	$16,000,000
11/2018	Allergy Associates of Hartford	$125,000
12/2018	Advanced Care Hospitalists	$500,000
12/2018	Pagosa Springs Medical Center	$111,400
12/2018	Cottage Health	$3,000,000
5/2019	Tennessee Medical Imaging	$3,000,000
5/2019	Medical Informatics Engineering	$100,000

Recent Enforcement Activities

Other recent cases involve ePHI viewable on the web, failure to manage identified risks, and malware attacks

Resolution Agreements:

https://www.hhs.gov/hipaa/

Some Good 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

UPDATES

UPDATES

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

UPDATES

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

UPDATES

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.

UPDATES

Direct Liability of Business Associates (Continued)

- 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.

https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/factsheet/index.html

UPDATES

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.

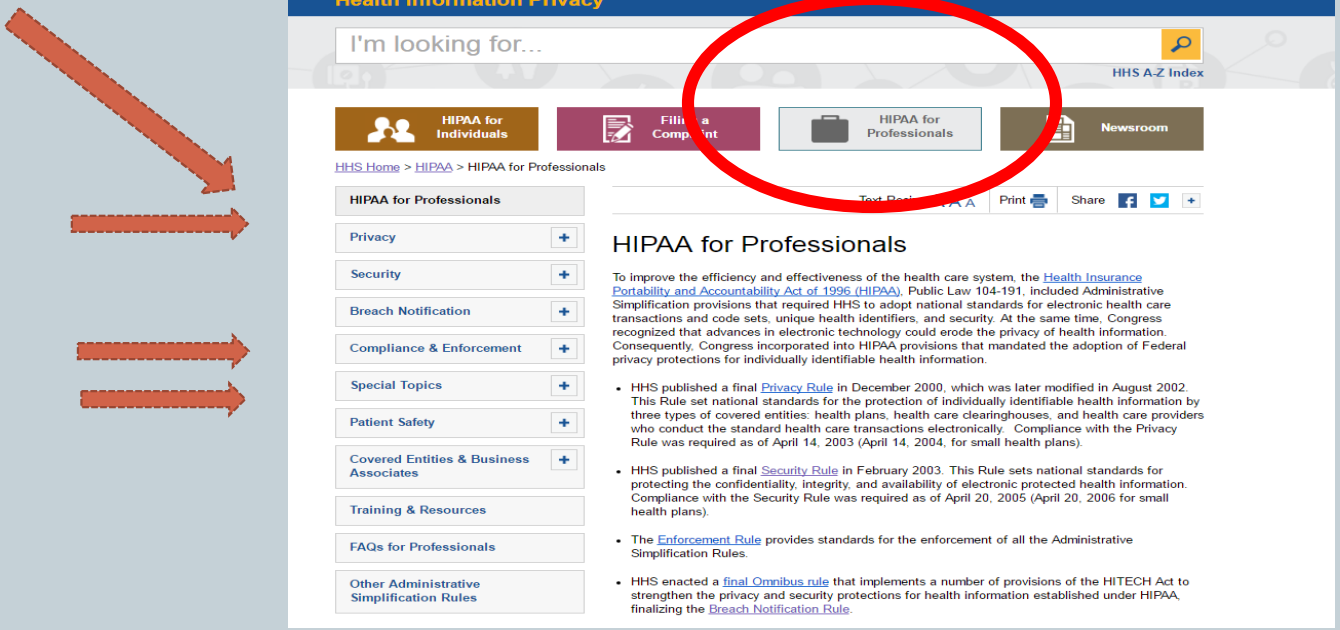
- https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/factsheet/index.html

RESOURCES

- **HIPAA Regulation**
- **Supplements to the HIPAA Regulation**
  - **HIPAA Security Information Series: (educational papers)**
    - **https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html?language=es**
    - **Administrative, Physical, and Technical Safeguards**
    - **Basics of Risk Analysis and Risk Management**
  - **Additional Security Guidance Material:**
    - **Remote use, mobile device, and ransomware**
  - **Cybersecurity Newsletters**
    - Risk Analyses v. Gap Analyses, workstation security, software vulnerability and patching, guidance on disposing of electronic devices and media, considerations for securing electronic media and devices
    - **Sign up for OCR Listserv: http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html**
- **Join us on Twitter @hhsocr**
- **OCR Hotline: (800) 368-1019 or (800) 537-7697 (TDD).**

Additional Resources

https://www.hhs.gov/hipaa



Privacy and Security Toolkit:

https://www.hhs.gov/hipaa/for-professionals/special-topics/health-information-technology/index.html

www.healthit.gov


Questions?