HIPAA Security Rule Breach Notification, and Cybersecurity

Nicholas Heesters, MEng, JD, CIPP
Advisory Council on Employee Welfare and Pension Benefit Plans
September 8, 2022

HHS Office for Civil Rights

Headquarters - Washington, DC

- Policy Development (e.g., regulations, guidance)
- Compliance & Enforcement National Coordination
- Outreach & Media

Regional Offices - Boston, New York City, Philadelphia, Atlanta, Denver, Dallas, Kansas City, San Francisco, Los Angeles, Chicago, Seattle

- Investigations
- Technical Assistance
- Outreach

Who We Are

As the Department's civil rights, conscience and religious freedom, and health information 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.

HIPAA Security Rule Overview

OCR Approach to HIPAA Security

- Standards to ensure the confidentiality, integrity, and availability of ePHI
- Through reasonable and appropriate safeguards
- Addresses risks and vulnerabilities identified through analysis and management of risk
- Appropriate to the size and complexity of the organization and its information systems
- Technology neutral

Standards and Implementation Specifications

Standards

- Required - A covered entity (and business associate) must comply with the standards

Implementation Specifications

- Required - a covered entity must implement the specification
- Addressable - a covered entity must assess whether the specification is reasonable and appropriate in its environment and document its decision to either implement the specification or implement an equivalent alternative

Administrative Safeguards

Administrative Safeguards

- "…are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information." (*Definitions - 45 CFR §164.304)*

Physical & Technical Safeguards

Physical Safeguards

- "…are physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion." (*Definitions - 45 CFR §164.304)*

Technical Safeguards

- "…means the technology and the policy and procedures for its use that protect electronic protected health information and control access to it." (*Definitions - 45 CFR §164.304)*

Organizational Requirements

Organizational Requirements

- Contains the standards for business associate contracts and other arrangements
- Contains the requirements for group health plans

Policies and Procedures and Documentation Requirements

- Requires the implementation of reasonable and appropriate policies and procedures
- Requires the maintenance of documentation (written or electronic)
- Establishes the retention, availability, and update conditions for documentation

Compliance Challenges

Incomplete or Inaccurate Risk Analysis

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

- Organizations frequently underestimate the proliferation of ePHI within their environments. When conducting a risk analysis, an organization must identify all of the ePHI created, maintained, received or transmitted by the organization.

- Examples: Applications like EHR, billing systems; documents and spreadsheets; database systems and web servers; fax servers, backup servers; etc.); Cloud based servers; Medical Devices Messaging Apps (email, texting, ftp); Media

The Risk Analysis Process: Key Activities Required by the Security Rule

- **Inventory** to determine where ePHI is stored
- **Evaluate** probability and criticality of potential risks
- **Adopt** reasonable and appropriate security safeguards based on results of risk analysis
- **Implement/Modify** security safeguards to reduce risk to a reasonable and appropriate level
- **Document** safeguards and rationale
- **Evaluate** effectiveness of measures in place
- **Maintain** continuous security protections
- **Repeat**

Failure to Manage Identified Risk

- The Risk Management Standard requires the "[implementation of] security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with [the Security Rule]." *See 45 CFR § 164.308(a)(1)(ii)(B).*
- Investigations conducted by OCR regarding several instances of breaches uncovered that risks attributable to a reported breach had been previously identified as part of a risk analysis, but that the organization failed to act on its risk analysis and implement appropriate security measures.
- In some instances, encryption was included as part of a remediation plan; however, activities to implement encryption were not carried out or were not implemented within a reasonable timeframe as established in a remediation plan.

Lack of Transmission Security

- When electronically transmitting ePHI, a mechanism to encrypt the ePHI must be implemented unless not reasonable and appropriate. *See 45 CFR § 164.312(e)(2)(ii).*
- Applications for which encryption should be considered when transmitting ePHI may include:
  - Email
  - Texting
  - Application sessions
  - File transmissions (e.g., ftp)
  - Remote backups
  - Remote access and support sessions (e.g., VPN)

Lack of Appropriate Auditing

- The HIPAA Rules require the "[implementation] of hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information." *See 45 CFR § 164.312(b).*

- Once audit mechanisms are put into place on appropriate information systems, procedures must be implemented to "regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports." *See 45 CFR § 164.308(a)(1)(ii)(D).*

- Activities that could warrant additional investigation:
  - Access to PHI during non-business hours or during time off
  - Access to an abnormally high number of records containing PHI
  - Access to PHI of persons for which media interest exists
  - Access to PHI of employees
  - Failed log-in attempts

No Patching of Software

- The use of unpatched or unsupported software on systems that access ePHI could introduce additional risk into an environment.
- Continued use of such systems must be included within an organization's risk analysis and appropriate mitigation strategies implemented to reduce risk to a reasonable and appropriate level.
- In addition to operating systems, EMR/PM systems, and office productivity software, software that should be monitored for patches and vendor end-of-life for support include:
  - Router and firewall firmware
  - Anti-virus and anti-malware software
  - Multimedia and runtime environments (e.g., Adobe Flash, Java, etc.)

Insider Threat

- Organizations must "[i]mplement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information … and to prevent those workforce members who do not have access … from obtaining access to electronic protected health information," as part of its Workforce Security plan. *See 45 CFR § 164.308(a)(3).*
- Appropriate workforce screening procedures could be included as part of an organization's Workforce Clearance process (e.g., background and OIG LEIE checks). *See 45 CFR § 164.308(a)(3)(ii)(B).*
- Termination Procedures should be in place to ensure that access to PHI is revoked as part of an organization's workforce exit or separation process. *See 45 CFR § 164.308(a)(3)(ii)(C).*

Disposal

- When an organization disposes of electronic media which may contain ePHI, it must implement policies and procedures to ensure that proper and secure disposal processes are used. *See 45 CFR § 164.310(d)(2)(i).*
- The implemented disposal procedures must ensure that "[e]lectronic media have been cleared, purged, or destroyed consistent with *NIST Special Publication 800–88: Guidelines for Media Sanitization*, such that the PHI cannot be retrieved."
- Electronic media and devices identified for disposal should be disposed of in a timely manner to avoid accidental improper disposal.
- Organizations must ensure that all electronic devices and media containing PHI are disposed of securely; including non-computer devices such as copier systems and medical devices.

Insufficient Backup and Contingency Planning

- Organizations must ensure that adequate contingency plans (including data backup and disaster recovery plans) are in place and would be effective when implemented in the event of an actual disaster or emergency situation. *See 45 CFR § 164.308(a)(7).*
- Leveraging the resources of cloud vendors may aid an organization with its contingency planning regarding certain applications or computer systems, but may not encompass all that is required for an effective contingency plan.
- As reasonable and appropriate, organizations must periodically test their contingency plans and revise such plans as necessary when the results of the contingency exercise identify deficiencies. *See 45 CFR § 164.308(a)(7)(ii)(D).*

Security Rule Resources

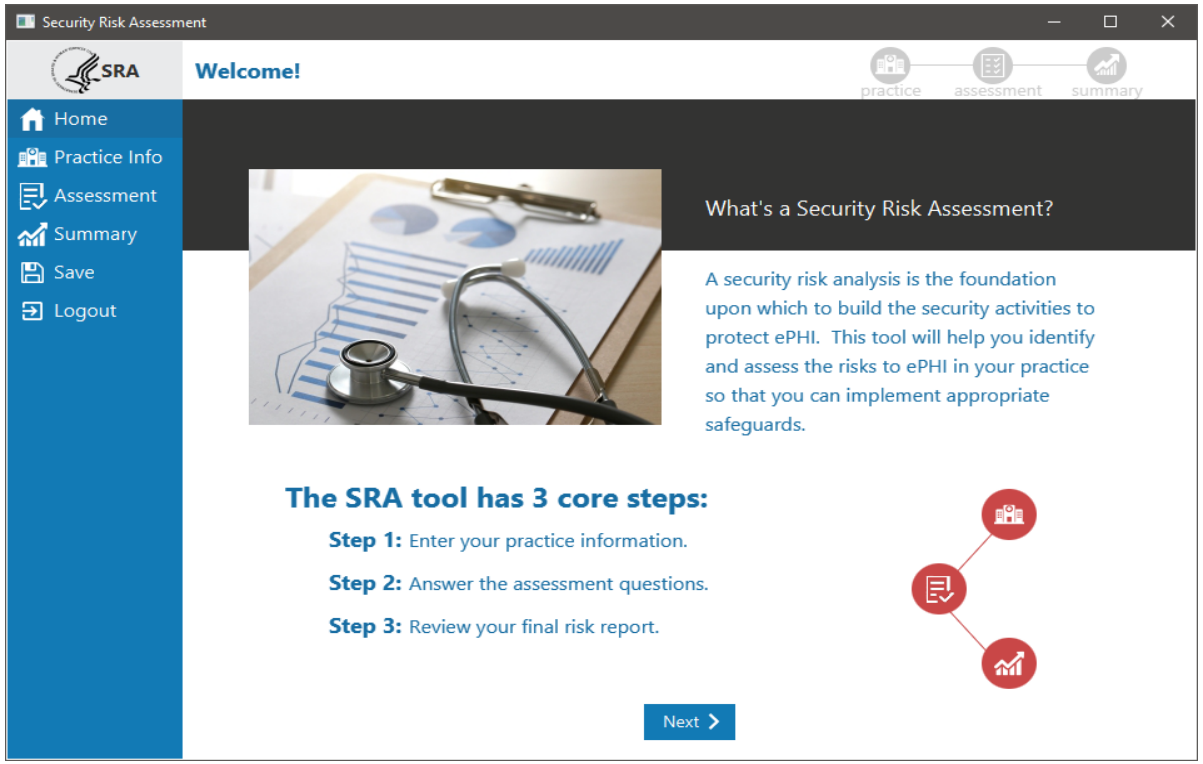
http://www.hhs.gov/hipaa/for-professionals/security/index.html

- The Security Rule
- Security Rule History
- Security Rule Guidance and Notices
- NIST Toolkit
- FAQs

Cloud Guidance

- OCR released guidance clarifying that a Cloud Service Provider (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.
- When a CSP stores and/or processes ePHI for a covered entity or business associate, that CSP is a business associate under HIPAA, even if the CSP stores the ePHI in encrypted form and does not have the key.
- CSPs are not likely to be considered "conduits," because their services typically involve storage of ePHI on more than a temporary basis.
- http://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html
- http://www.hhs.gov/hipaa/for-professionals/faq/2074/may-a-business-associate-of-a-hipaa-covered-entity-block-or-terminate-access/index.html

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.

Ransomware Resources

HHS Health Sector Cybersecurity Coordination Center Threat Briefs:

- https://www.hhs.gov/about/agencies/asa/ocio/hc3/products/index.html#sector-alerts

HHS Resources on Section 405(d) of the Cybersecurity Act of 2015:

- Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients https://www.phe.gov/Preparedness/planning/405d/Pages/hic-practices.aspx
- Cybersecurity Reports and Tools https://www.phe.gov/Preparedness/planning/405d/Pages/reportandtools.aspx

OCR Guidance:

- Ransomware https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf
- Cybersecurity https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html
- Risk Analysis https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf

HHS Security Risk Assessment Tool: https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool

CISA Resources:

- https://www.cisa.gov/stopransomware
- https://www.cisa.gov/sites/default/files/publications/CISA_Fact_Sheet-Protecting_Sensitive_and_Personal_Information_from_Ransomware-Caused_Data_Breaches-508C.pdf
- https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C_.pdf

FBI Resources:

- https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware
- https://www.ic3.gov/Media/Y2019/PSA191002

Cybersecurity Guidance Material

OCR has a Cybersecurity Guidance Material webpage, including a Cybersecurity Checklist and Infographic, which explain the steps for a HIPAA covered entity or its business associate to take in response to a cyber-related security incident.

- Cybersecurity Checklist - PDF
- Cybersecurity Infographic [GIF 802 KB]

https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html

Cybersecurity Newsletters

- Recent Topics Include:
  - Defending Against Common Cyber-Attacks
  - Securing Your Legacy [System Security]
  - Controlling Access to ePHI
  - 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
- Sign up for the OCR Listserv:

  http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html

Breach Notification Rule

Definition of Breach

- The acquisition, access, use, or disclosure of PHI in a manner not permitted by the HIPAA Rules which compromises the security or privacy of the PHI

- Impermissible use/disclosure of (unsecured) PHI *presumed* to require notification, unless CE/BA can demonstrate low probability that PHI has been compromised based on a risk assessment

Exceptions to the definition of breach

1. Unintentional acquisition, access, or use of PHI by workforce member or person acting under the authority of a CE or BA if done in good faith and in the scope of authority and there is no further impermissible use or disclosure of the PHI.
2. Inadvertent disclosure by a person authorized to access PHI to another person authorized to access PHI at the same CE or BA or OHCA and the information received is not further impermissibly used or disclosed by the recipient.
3. CE or BA have a good faith reason to believe the unauthorized recipient could not reasonably have been able to retain the information.

Breach Checklist for Covered Entities

1. Has there been an impermissible acquisition, access, use, or disclosure of PHI?
2. Determine whether the incident falls under any of the exceptions to the definition of breach. If no exception, breach is presumed.
3. Provide breach notification, or first conduct risk assessment (see below) to determine whether low probability of compromise. If more than a low probability of compromise, provide breach notification.

Breach risk assessment - determine and document at least:

- Nature & extent of PHI involved
- Who received/accessed the information
- Potential that PHI was actually acquired or viewed
- Extent to which risk to the data has been mitigated

Notification obligation only applies to "Unsecured PHI"

- Unsecured PHI is PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals
- Acceptable methods of securing PHI are encryption and destruction
- Loss or compromise of PHI that has been encrypted or properly destroyed does not trigger the duty to notify or report

Notification to Individuals

- A covered entity must notify each affected individual following the discovery of a breach of unsecured PHI
- The obligation to notify applies to those breaches that the covered entity knows about or s*hould have known* about if exercising reasonable diligence

"Known or should have known" Standard

- Means that covered entities can be liable for failing to provide notice to individuals in situations where they did not know of a breach but would have known if they exercised reasonable diligence
- Employees of a covered entity are considered agents of the organization and any knowledge an employee has will be attributed to the covered entity (except where the employee is the person committing the breach)
- Because of this standard, covered entities need to have reasonable systems in place to discover breaches, including training of staff on prompt reporting of any known breaches

Breach Notification

- 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

Timeliness of Notification

- Notice must be provided to the individual without unreasonable delay and in no case later than **60 calendar days** after discovery of the breach
- 60 days is an outer limit; the covered entity should send the notifications sooner if it is ready

Content of Notification

The notification must contain, to the extent possible:

- Description of what happened and dates, if known
- Description of the types of unsecured PHI involved in the breach
- Any steps individuals should take to protect themselves
- Description of what the covered entity is doing to investigate and mitigate harm
- Contact information for individuals to learn more which must include a toll-free telephone number, e-mail address, website, or postal address

Business Associates

- Business associates must notify covered entities of breaches without unreasonable delay and in no case later than 60 days
- Breaches are treated as discovered on the first day that the breach is known or by exercising reasonable diligence would have been known to the BA
- The content of the notification from the BA to the CE must include, to the extent possible, the identification of the affected individuals and as much information that is known to the BA which the CE would be required to include in its notice to the individual

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.

Direct Liability of Business Associate, cont.

- 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 CFR §§ 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

Law Enforcement Delay

- If law enforcement makes a written statement to a covered entity or business associate that notification or posting of a breach would impede a criminal investigation, the covered entity must delay notification until the time specified by law enforcement
- If the requested delay by law enforcement is oral, the covered entity must document the oral request and delay notification for no longer than 30 days from the date of the request

What happens when 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
- Received over 700 breach reports affecting 500+ individuals in 2021

OCR opens investigations into breaches affecting 500+ individuals, and into number of smaller breaches

Investigations involve looking at

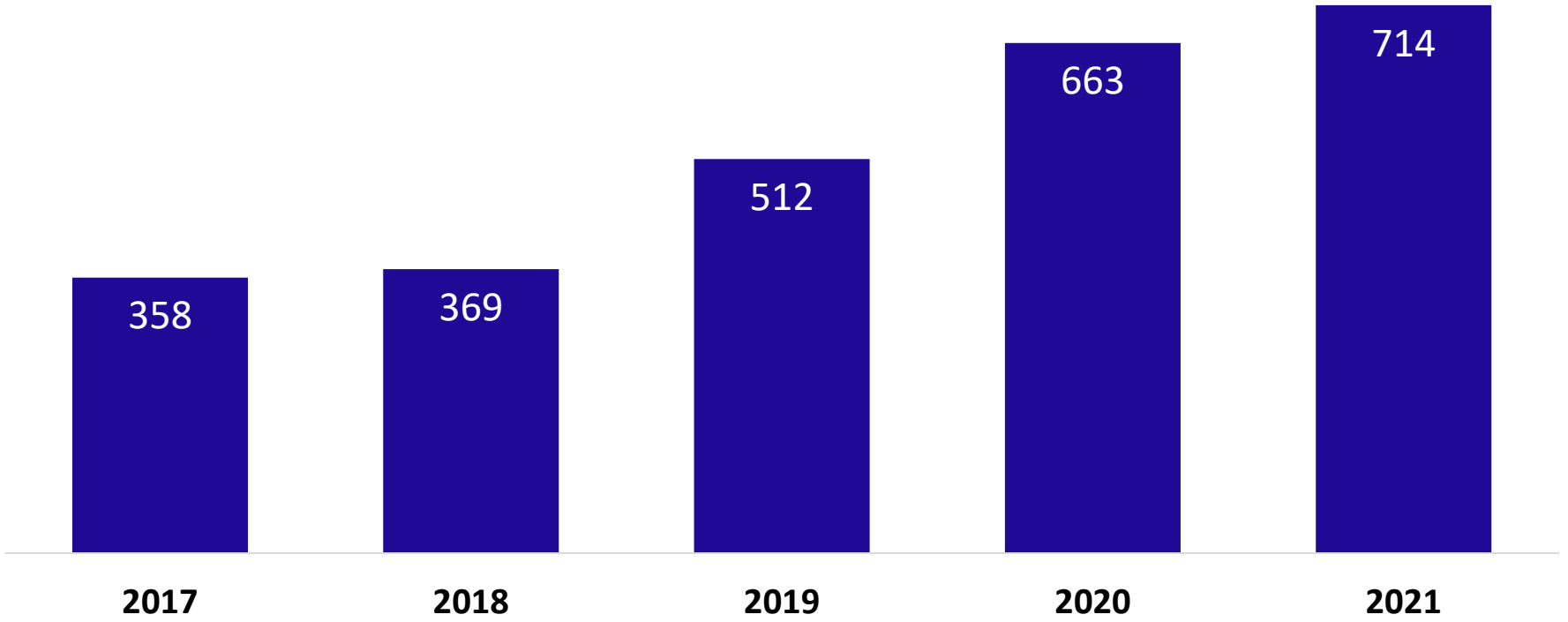
- Underlying cause of the breach
- Actions taken to respond to the breach (breach notification) and prevent future incidents
- Entity's compliance prior to breach

Breach reporting - https://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html

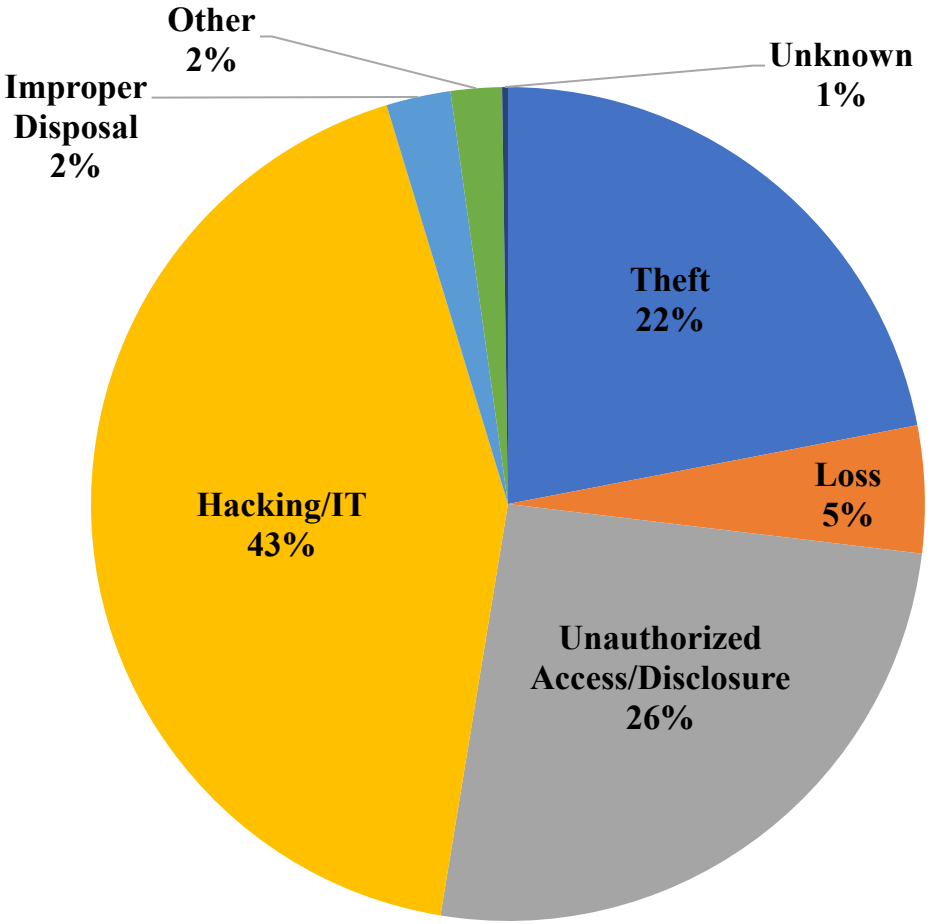
Enforcement

Breaches Affecting 500 or More Individuals
Reports Received by Year

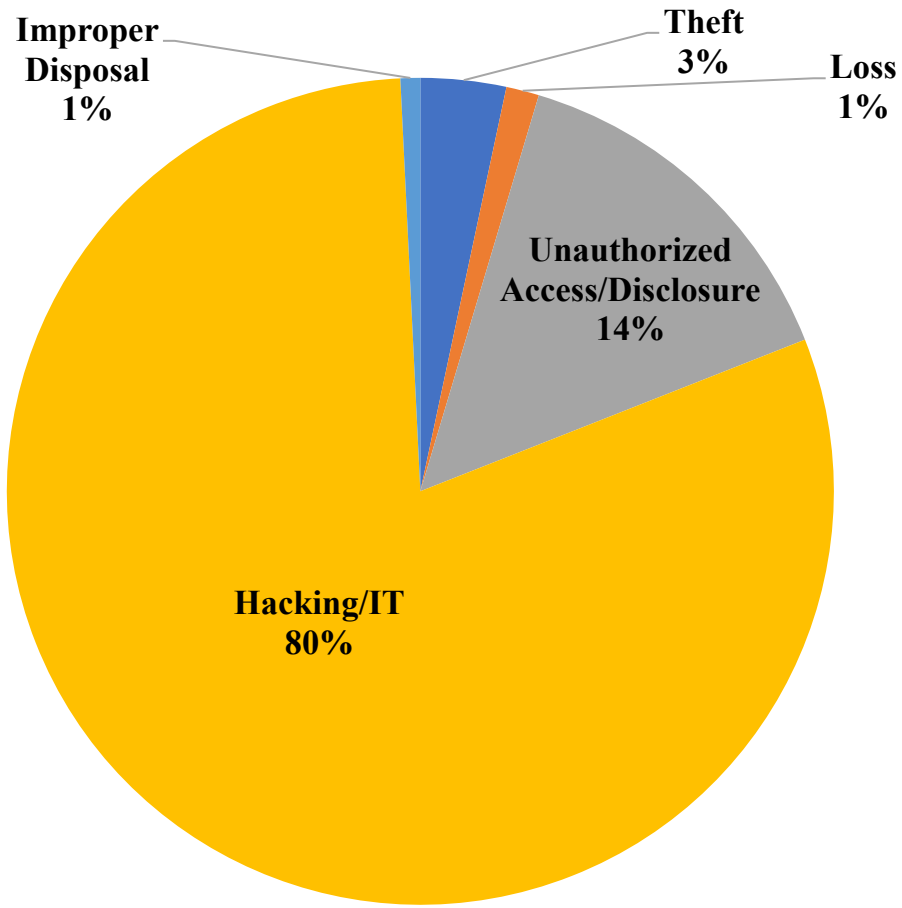
Calendar Years 2017 - 2021



500+ Breaches by Type of Breach

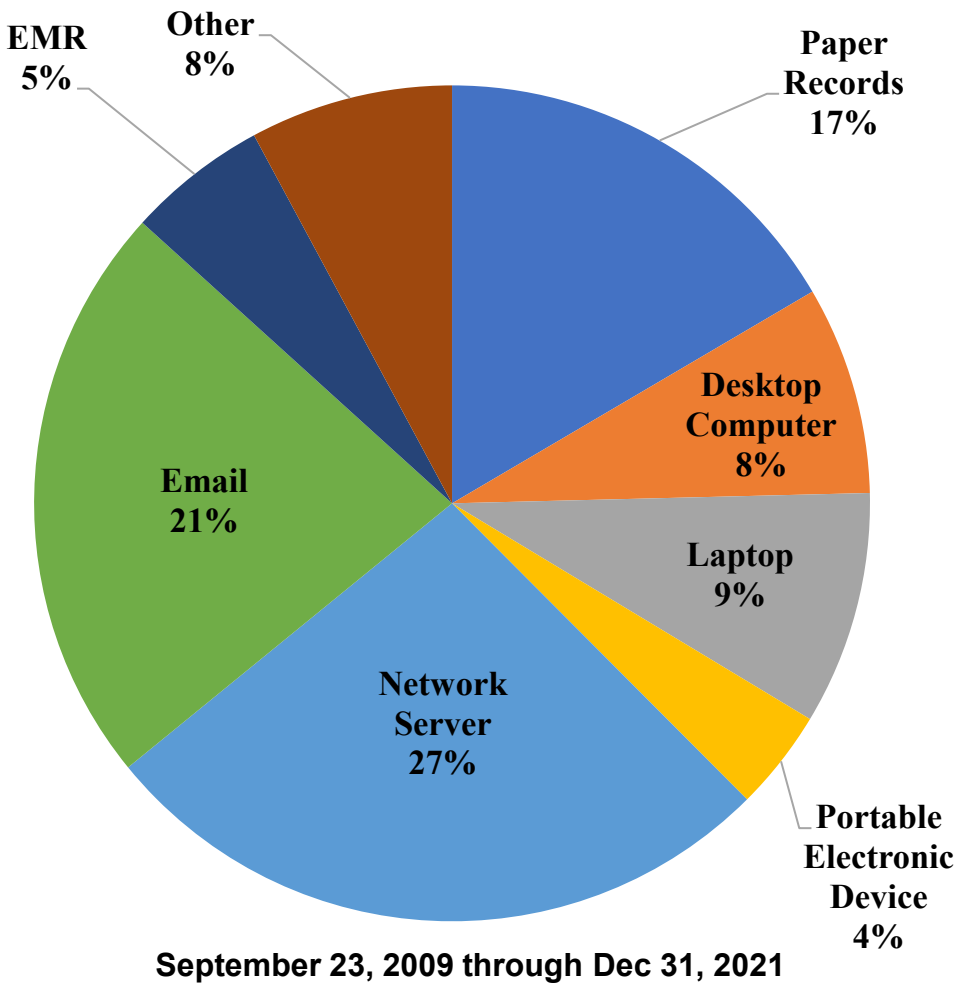


September 23, 2009 through Dec 31, 2021

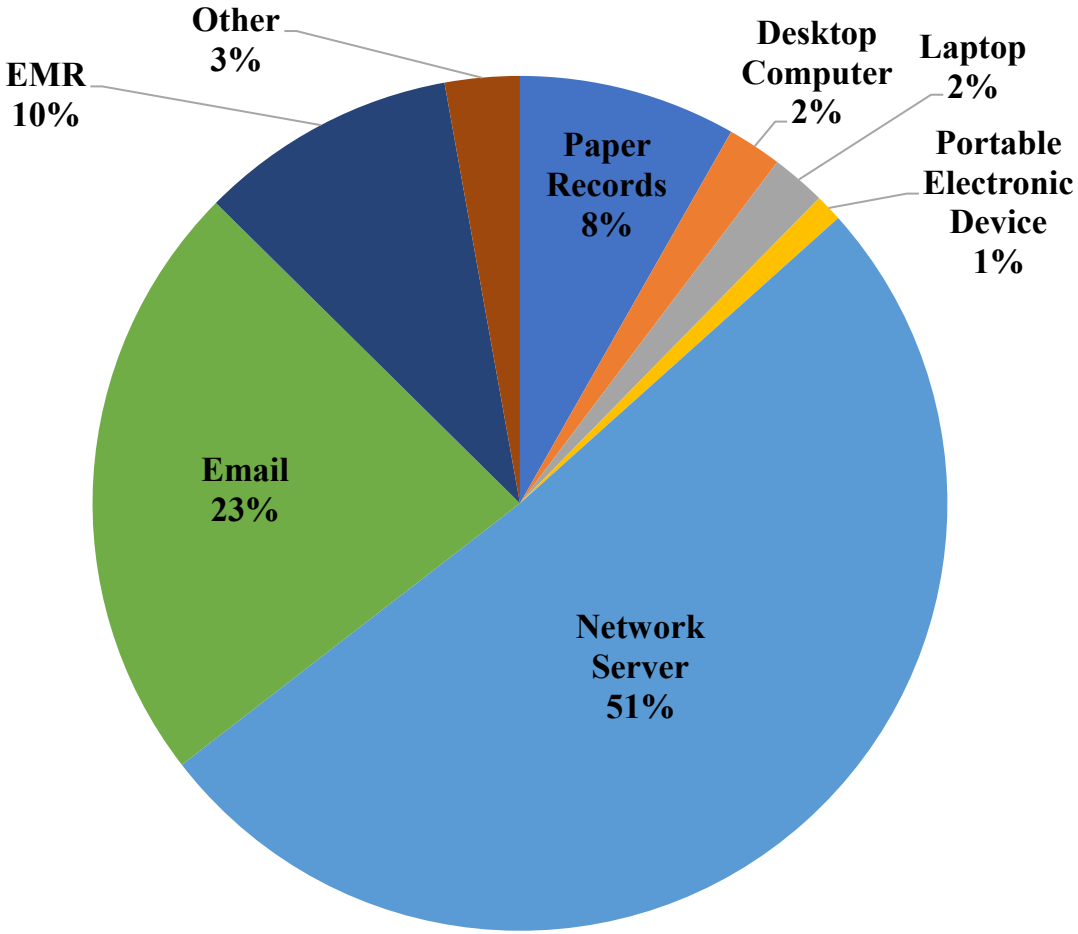


January 1, 2022 through July 31, 2022

500+ Breaches by Location of Breach



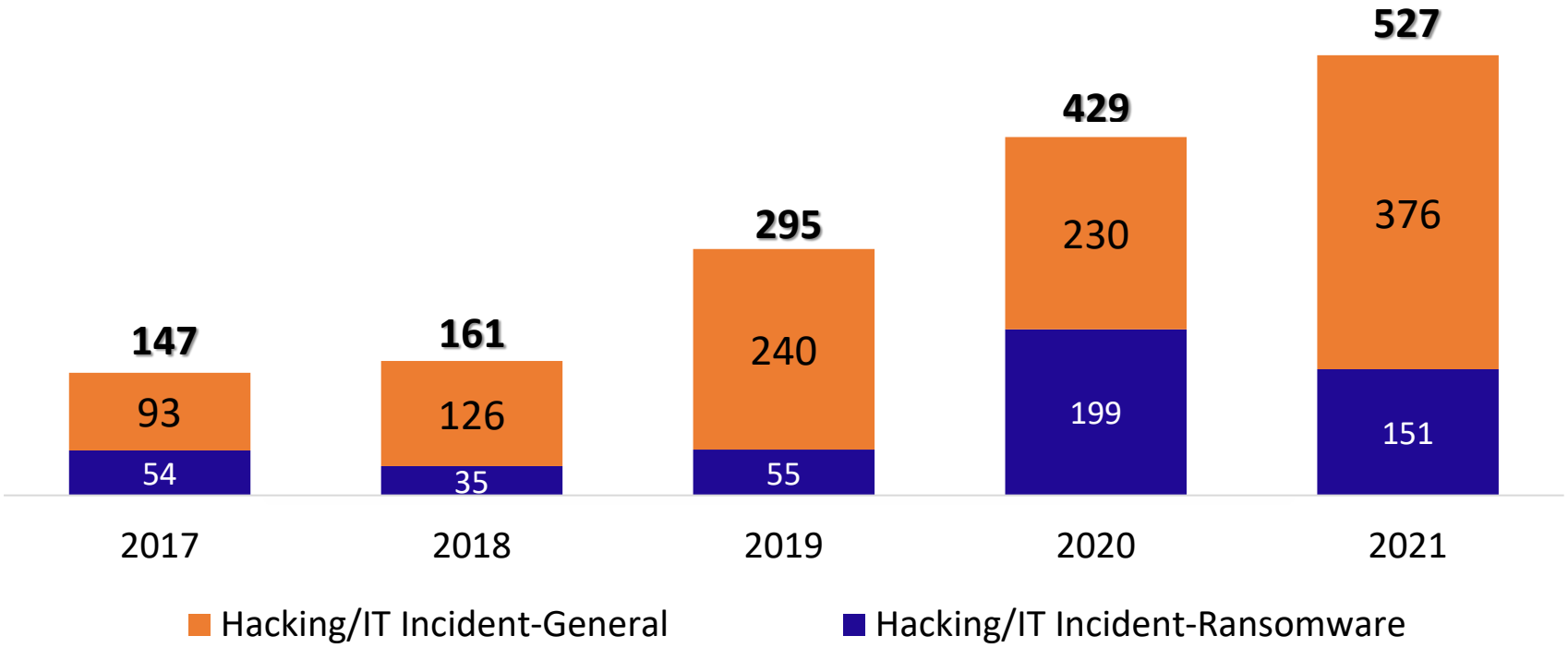
September 23, 2009 through Dec 31, 2021



January 1, 2022 through July 31, 2022

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

Calendar Years 2017 - 2021



General HIPAA Enforcement Highlights

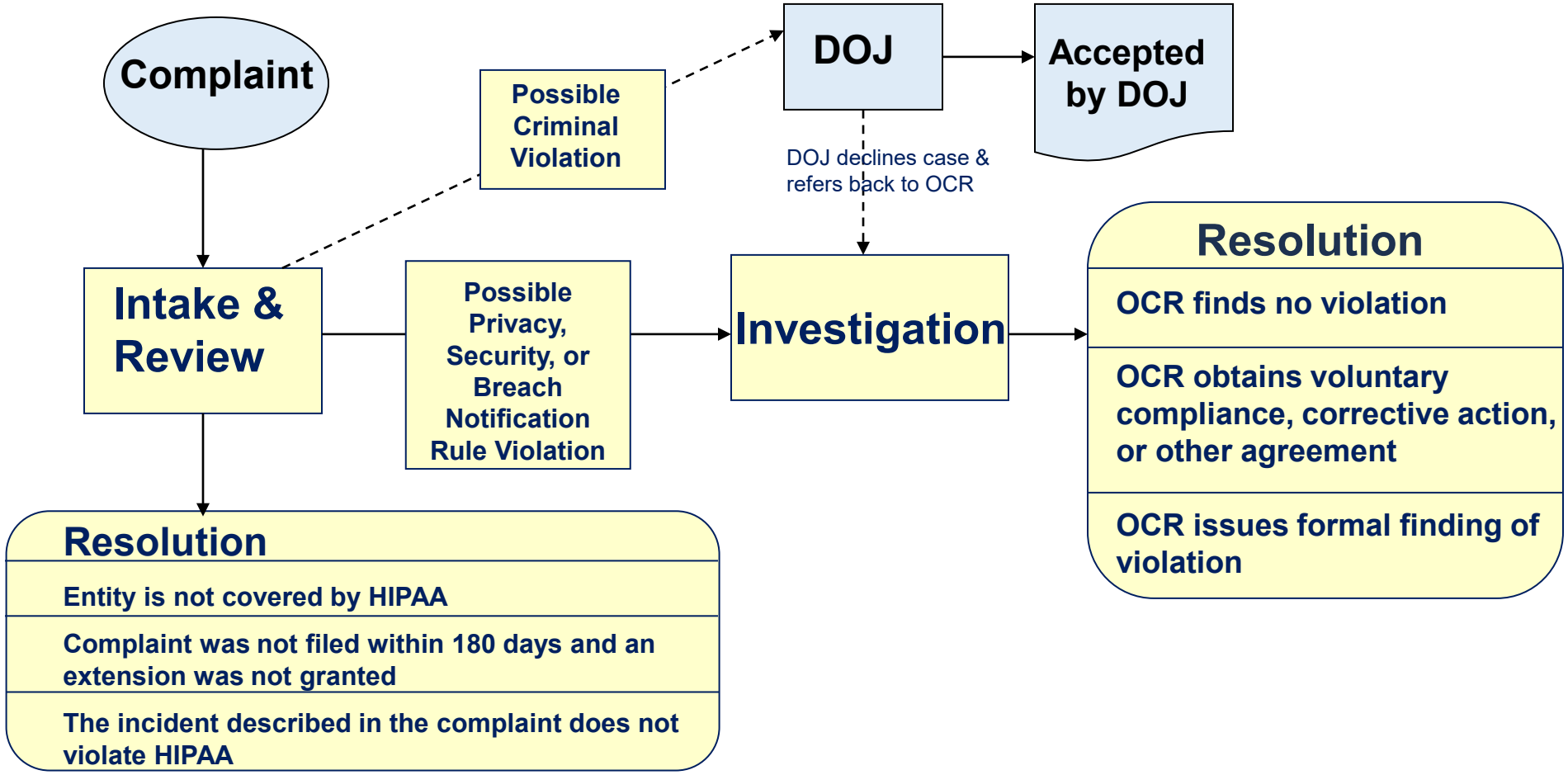
- OCR expects to receive over 33,000 complaints this year.
- In most cases, entities are able to demonstrate satisfactory compliance through voluntary cooperation and corrective action.
- In some cases, the nature or scope of indicated noncompliance warrants additional enforcement action.
- Resolution Agreements/Corrective Action Plans
  - 114 settlement agreements that include detailed corrective action plans and monetary settlement amounts
- 8 civil money penalties

As of July 31, 2022

Recent OCR HIPAA Enforcement Action Announcements

Mar-22	Dr. Donald Brockley, D.D.M.	$30,000
Mar-22	Dr. U. Phillip Igbinadolor, D.M.D. & Associates, P.A.	$50,000 **(CMP)**
Mar-22	Jacob and Associates	$28,000
Mar-22	Northcutt Dental – Fairhope, LLC	$62,500
July-22	ACPM Podiatry	$100,000 **(CMP)**
July-22	Associated Retina Specialists	$22,500
July-22	Lawrence Bell Jr., D.D.S	$5,000
July-22	Coastal Ear, Nose, and Throat	$20,000
July-22	Danbury Psychiatric Consultants	$3,500
July-22	Erie County Medical Center Corporation	$50,000
July-22	Fallbrook Family Health Center	$30,000
July-22	Hillcrest Commons Nursing and Rehabilitation	$55,000
July-22	Melrose Wakefield Healthcare	$55,000
July-22	Memorial Hermann Health System	$240,000
July-22	Southwest Surgical Associates	$65,000
July-22	Oklahoma State University	$875,000

Complaint Process



Enforcement Process

OCR reviews the information, or evidence, that it gathers in each case. If the evidence indicates that the covered entity was not in compliance, OCR will attempt to resolve the case with the covered entity by obtaining:

- Voluntary compliance;
- Corrective action; and/or
- Resolution agreement.

https://www.hhs.gov/hipaa/for-professionals/special-topics/enforcement-rule/index.html

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.

Recognized Security Practices

- HITECH Amendment, signed into law and effective January 5, 2021
- Standards, guidelines, best practices, methodologies, procedures, and processes developed under:
  - Section 2(c)(15) of NIST Act
  - Section 405(d) of Cybersecurity Act of 2015
  - “Other” programs that address cybersecurity recognized by statute or regulation
- Must be adequately demonstrated to be in place for previous 12 months
- Mitigates civil money penalties, other remedies in an agreement, or early, favorable termination of an audit
- No liability for electing not to engage in recognized security practices

https://www.govinfo.gov/content/pkg/PLAW-116publ321/pdf/PLAW-116publ321.pdf

Corrective Action

Corrective Actions May Include:

- Updating risk analysis and risk management plans
- Updating policies and procedures
- Training of workforce
- CAPs may include 3rd party monitoring

Recurring Compliance Issues

- Business Associate Agreements
- Risk Analysis
- Failure to Manage Identified Risk, e.g. Encrypt
- Lack of Transmission Security
- Lack of Appropriate Auditing
- No Patching of Software
- Insider Threat
- Improper Disposal
- Insufficient Data Backup and Contingency Planning
- Individual Right to Access

Best 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

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