ACHC U®
EDUCATIONAL RESOURCES

DMEPOS

What Constitutes a HIPAA Breach and How to Respond to the Breach

Denise M. Leard, Esq.
Brown & Fortunato

What's the Likelihood?

- OCR 2017 Desk Audits
  - 94% of organizations had inadequate risk management plans
  - 83% of organizations had performed inadequate risk analyses
  - 89% of organizations were inadequate on patient's right to access
- 90% of healthcare organizations experience at least one data breach within a 2-year period.
- Half of those organizations experience more than five data breaches within a 2-year period.

Common Causes of Breaches

- Third Parties
  - 41% of breaches experienced by covered entities
- Unintentional Employee Actions
  - 36% of breaches experienced by covered entities
  - 55% of breaches experienced by business associates

Is Breach a Four Letter Word?

- Not necessarily—A breach is NOT equivalent to a HIPAA violation that can result in significant fines and penalties.
- Failing to report a breach and/or failing to take steps to prevent breaches will likely in serious consequences for covered entities and business associates.

Is Breach a Four Letter Word?

- Case in Point: Presence Health
  - January 9, 2017
  - OCR alleged that Presence Health failed to timely notify affected individuals and the media following a breach
  - $475,000 settlement

Civil Penalties for HIPAA Violations

Tier 1
- Did not know and could not have reasonably known of violation
- $100 - $50,000 per violation; maximum of $25,000 per year

Tier 2
- Reasonable cause to believe knew/should have known of violation
- $1,000 - $50,000 per violation; maximum of $100,000 per year

Tier 3
- Violation due to willful neglect but corrected within 30 days
- $10,000 - $50,000 per violation; maximum of $250,000 per year

Tier 4
- Violation due to willful neglect and not corrected within 30 days
- $50,000 per violation; maximum of $1.5 million per year

ACHC U®
EDUCATIONAL RESOURCES

Identify a Breach

Identify a Breach

- What is a breach?
  - The unauthorized “acquisition, access, use, or disclosure of protected health information in a manner not permitted under [the HIPAA Privacy Rule] which compromises the security or privacy of the protected health information.”

- Four Key Questions:
  1. Was there an unauthorized acquisition of, access to, or use or disclosure of PHI?
  2. Was the PHI unsecure?
  3. Does an exception to the definition of breach apply?
  4. Can the entity demonstrate a low probability that the PHI has been compromised?

Identify a Breach

- Question 1: Was there an unauthorized acquisition of, access to, or use or disclosure of PHI?
  - To answer this question, it is necessary to understand a few terms:
    - Protected Health Information
    - Unauthorized
    - Acquisition / Access / Use / Disclosure
  - Case Study: Why is it important to understand the breadth of “PHI”
    - In 2017, Memorial Hermann Health System paid $2.4 million to settle claims of a HIPAA Breach.

Identify a Breach

- Question 2: Was the PHI unsecure when it was acquired/accessed/used/disclosed?
  - PHI is secure if it is either:
    - Appropriately encrypted (i.e. converted into encoded or unreadable text that requires a confidential process or key to assign meaning), or
    - Properly destroyed
  - OCR has cautioned about the limits of full disk encryption
    - Laptop with full disk encryption – security of PHI depends on if the laptop was powered on and in use or was powered off

Identify a Breach

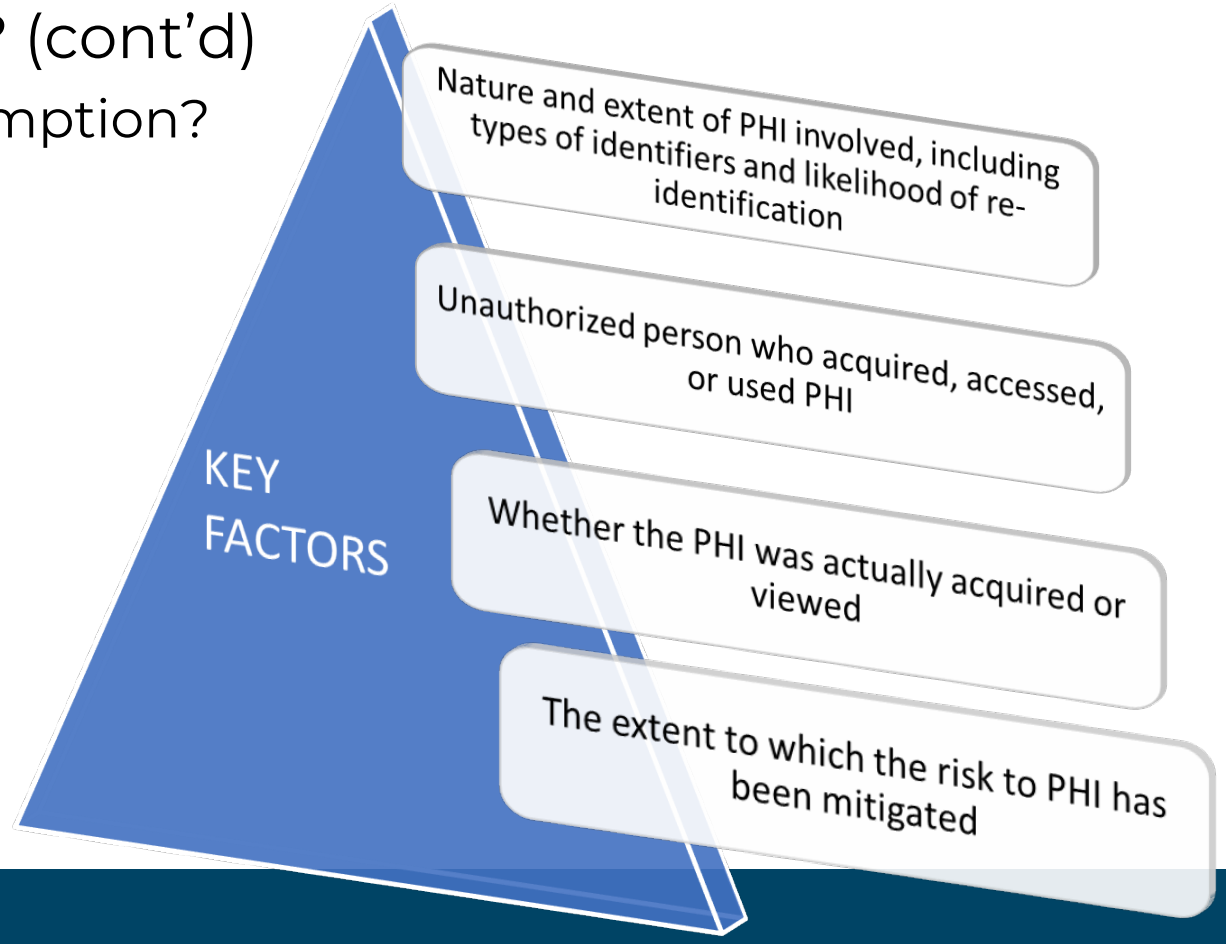
- Question 3: Does an exception to the definition of breach apply?
  - There are three exceptions under the Breach Notification Rule:
    1. Unintentional acquisition, access, or use of PHI by a workforce member made in good faith, was within the scope of authority, and does not result in further inappropriate use or disclosure
    2. Inadvertent disclosure of PHI by an authorized person to another person authorized to access PHI at the same covered entity or organized health care organization and does not result in further inappropriate use or disclosure
    3. Disclosure of PHI where the entity has a good faith belief that the unauthorized person to whom the disclosure was made would not reasonably have been able to retain the information

Identify a Breach

- Question 4: Can the entity demonstrate a low probability that the PHI has been compromised?
  - Presumption
    - If there was an unauthorized acquisition, access, use, or disclosure of PHI and no exception applies, then the incident is presumed to be a breach unless the entity can demonstrate that there is a low probability that the PHI has been compromised.

Identify a Breach

- Question 4: Can the entity demonstrate a low probability that the PHI has been compromised? (cont'd)
  - How to rebut the presumption?



ACHC U®
EDUCATIONAL RESOURCES

DMEPOS

Reporting A Breach

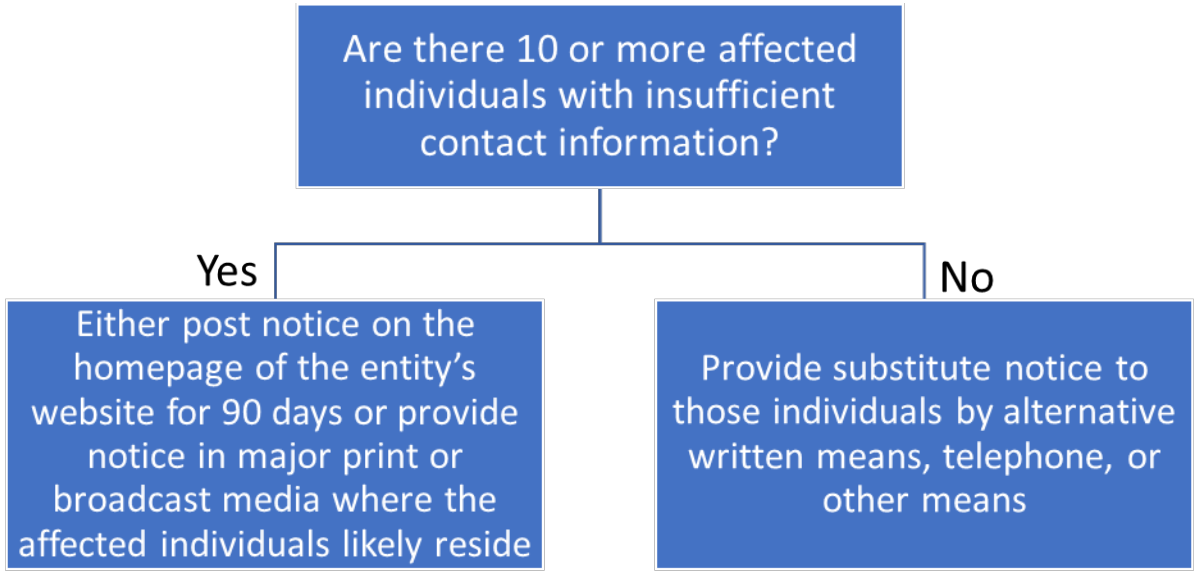
Reporting a Breach

- Federal Requirements for Reporting a Breach
  - Individual notice
  - Notice to OCR
  - Notice to media

- State Law Requirements

Reporting a Breach

- Individual Notice
  - General Notice Requirement
    - Written notice sent by first-class mail or by email if the affected individual has agreed to electronic notice
    - Without unreasonable delay but in no case more than 60 days after discovery of the breach
  - Substitute Notice

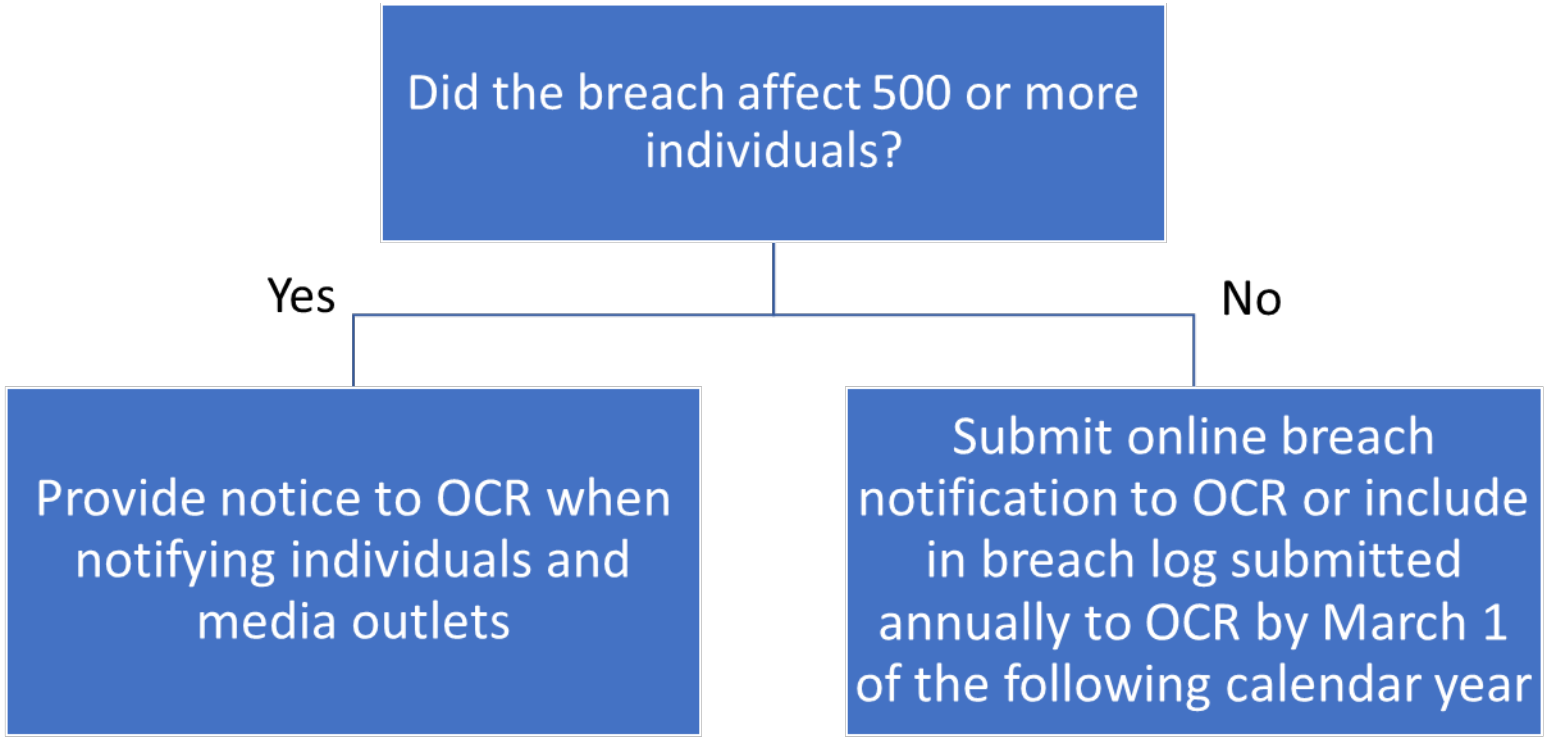


Reporting a Breach

- Content of Individual Notice
  - Description of incident
  - Description of PHI involved
  - Steps that can be taken to protect against potential harm
  - Description of investigation undertaken
  - Steps taken to mitigate harm and protect against future breaches
  - Contact information

Reporting a Breach

- Notice to OCR and Others



Reporting a Breach

- State Law Breach Reporting
  - All states have laws governing patient privacy and require reporting of certain breaches.
  - Such laws may be stricter than HIPAA and should be reviewed in the event of a breach to ensure compliance.

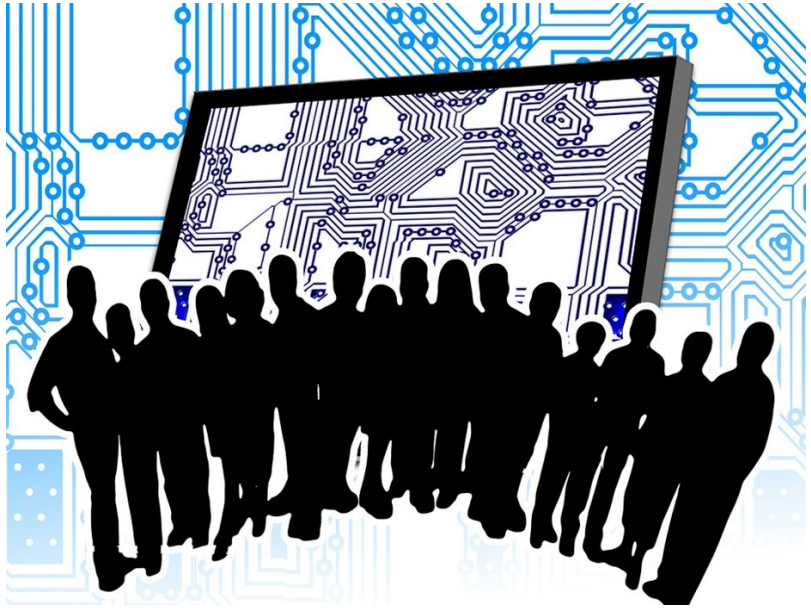
ACHC U®
EDUCATIONAL RESOURCES

DMEPOS

Responding to/Preventing a Breach

Responding to a Security Incident or Potential Breach

- Assemble a Team
  - Include high-level personnel with authority to take action
  - Assess need for outside consultants
    - Attorney
    - Computer forensic consultant
    - Public relations firm



Responding to a Security Incident or Potential Breach

- Investigate, Analyze, and Take Action
  - Gather information and interview employees
  - Take steps to maintain confidentiality and preserve evidence
  - Mitigate harm
  - Develop and implement a corrective action plan (including an update to the entity's risk analysis and management plan)
  - Involve law enforcement?
  - Notify insurance carriers?
  - Determine what kind of breach reporting will be required
  - Document the company's investigations and actions

Prevent and Prepare for a Breach

- Conduct and update security risk assessments.
- Prepare and implement risk management plans.
- Invest in (and use) encryption technology.
- Train employees.
- Investigate business associates and strengthen rights with business associates.

ACHC U®
EDUCATIONAL RESOURCES

DMEPOS

HIPAA Restrictions on Marketing

HIPAA Restrictions on Marketing

- The Health Insurance Portability and Accountability Act (“HIPAA”) requires “covered entities” to obtain a valid authorization from individuals before using or disclosing protected health information (“PHI”) to market a product or service to them.
- HIPAA broadly defines “use” of PHI to include the sharing, employment, application, utilization, examination, or analysis of such information. 42 CFR § 160.103.

HIPAA Restrictions on Marketing

- The new HIPAA definition of marketing list exceptions to what is considered marketing:
  - communications made to describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communications, including communications about:
    - the entities participating in a healthcare provider network or health plan network; replacement of, or enhancements to, a health plan; and
    - health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefit
  - communications made for the treatment of the individual; and
  - communications for case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual

HIPAA Restrictions on Marketing

- the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits

HIPAA Restrictions on Marketing

- Marketing communications require prior valid authorization from the customer.
- Therefore, to avoid HIPAA's requirement that the DME supplier obtain a valid authorization from the customer before making a marketing communication, the marketing communication must concern a health-related product or service:
  - provided by the supplier; and
  - the supplier cannot receive financial remuneration in exchange for making the communication

HIPAA Restrictions on Marketing

- When the Department of Health and Human Services revised the definition of marketing communication, it issued the following comments to the final rule:
  - We believe Congress intended that these provisions curtail a covered entity's ability to use the exceptions to the definition of "marketing" in the Privacy Rule to send communications to the individual that are motivated more by commercial gain or other commercial purpose rather than for the purpose of the individual's health care, despite the communication being about a health-related product or service.

HIPAA Restrictions on Marketing

- HIPAA applies to any patient—no matter how old or how young—and whether the patient is covered by Medicare or commercial insurance.
- In other words, HIPAA is not limited to Medicare patients.

ACHC U®
EDUCATIONAL RESOURCES

DMEPOS

HIPAA Enforcement

Enforcing the HIPAA Privacy and Security Rules

- The Office of Civil Rights (OCR) is responsible for enforcing the HIPAA Privacy and Security Rules (45 C.F.R. Parts 160 and 164, Subparts A, C, and E).
- OCR investigate complaints filed with it alleging a violation of the Privacy or Security Rules
  - An individual may file a health information privacy and security complaint with the OCR if they feel a covered entity or business associate violated their (or someone else's) health information privacy rights or committed another violation of the Privacy, Security or Breach Notification Rules.

Enforcing the HIPAA Privacy and Security Rules

- What happens when a complaint is filed?
  - OCR carefully reviews all health information privacy and security complaints. Under the law, OCR only may act on complaints if:
    - An individual's rights were violated by a covered entity or business associate
    - The complaint is filed within 180 days of the violation

Enforcing the HIPAA Privacy and Security Rules

- What Happens After the Investigation
  - At the end of the investigation, OCR issues a letter describing the resolution of the investigation.
  - If OCR determines that a covered entity or business associate may not have complied with the HIPAA Rules, that entity or business associate must:
    - Voluntarily comply with the HIPAA Rules
    - Take corrective action
    - Agree to a settlement
    - If the covered entity or business associate does not take satisfactory action to resolve the matter, OCR may decide to impose civil money penalties (CMPs) on the covered entity.
    - If CMPs are imposed, the covered entity may request a hearing in which an HHS administrative law judge decides if the penalties are supported by the evidence in the case.

Enforcing the HIPAA Privacy and Security Rules

- OCR may act only on complaints that meet the following conditions:
  - The alleged action must have occurred in the past 6 years.
  - The complaint must be filed against an entity that is required by law to comply with the HIPAA Rules.
  - A complaint must allege an activity that, if proven true, would violate the HIPAA Rules.
    - For example, OCR generally could not investigate a complaint that alleged that a physician sent an individual's health information to another health care provider for consultation relating to a patient, because the Privacy Rule permits covered health care providers to use and disclose such information for such treatment purposes.
  - Complaints must be filed within 180 days of when the person submitting the complaint knew or should have known about the alleged violation of the HIPAA Rules.
    - OCR may waive this time limit if it determines that the person submitting the complaint shows good cause for not submitting the complaint within the 180-day time frame (e.g., such as circumstances that made submitting the complaint within 180 days impossible).

Enforcing the HIPAA Privacy and Security Rules

- If OCR accepts a complaint for investigation:
  - OCR will notify the person who filed the complaint, and the covered entity named in it.
  - Then the complainant and the covered entity are asked to present information about the incident or problem described in the complaint.
  - OCR may request specific information from each to get an understanding of the facts.
  - Covered entities are required by law to cooperate with complaint investigations.

Enforcing the HIPAA Privacy and Security Rules

- If OCR accepts a complaint for investigation (cont'd):
  - If a complaint describes an action that could be a violation of the criminal provision of HIPAA (42 U.S.C. 1320d-6), OCR may refer the complaint to the Department of Justice for investigation.
  - OCR reviews the information, or evidence, that it gathers in each case.
    - In some cases, it may determine that the covered entity did not violate the requirements of the Privacy or Security Rule.
  - 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.
  - Most Privacy and Security Rule investigations are concluded to the satisfaction of OCR through these types of resolutions

Enforcing the HIPAA Privacy and Security Rules

- If OCR accepts a complaint for investigation (cont'd):
  - OCR notifies the person who filed the complaint and the covered entity in writing of the resolution result.
  - If the covered entity does not take action to resolve the matter in a way that is satisfactory, OCR may decide to impose civil money penalties (CMPs) on the covered entity.
  - If CMPs are imposed, the covered entity may request a hearing in which an HHS administrative law judge decides if the penalties are supported by the evidence in the case.
  - Complainants do not receive a portion of CMPs collected from covered entities; the penalties are deposited in the U.S. Treasury.

Enforcing the HIPAA Privacy and Security Rules

- OCR may also conduct compliance reviews to determine if covered entities are in compliance, and OCR performs education and outreach to foster compliance with requirements of the Privacy and Security Rules.

ACHC U®
EDUCATIONAL RESOURCES

DMEPOS

Recent HIPAA Cases

Recent HIPAA Cases

- On December 10, 2024 (OCR) announced a settlement with Inmediata Health Group, LLC (Inmediata), a health care clearinghouse, concerning potential violations of the privacy and security rule following OCR's receipt of a complaint that HIPAA protected health information was accessible to search engines like Google, on the internet.

Recent HIPAA Cases: Inmediata Health Group, LLC (Inmediata)

- Facts:
  - In 2018, OCR received a complaint concerning PHI left unsecured on the internet.
  - Following the initiation of OCR's investigation, Inmediata provided breach notification to HHS, and affected individuals.
  - OCR's investigation determined that from May 2016 through January 2019, the PHI of 1,565,338 individuals was made publicly available online.

Recent HIPAA Cases: Inmediata Health Group, LLC (Inmediata)

- Facts (cont'd):
  - The PHI disclosed included
    - patient names,
    - dates of birth,
    - home addresses,
    - Social Security numbers,
    - claims information,
    - diagnosis/conditions and
    - other treatment information.
  - These impermissible disclosures of PHI were potential violations of the HIPAA Privacy Rule.

Recent HIPAA Cases: Inmediata Health Group, LLC (Inmediata)

- Facts (cont'd):
  - OCR's investigation also identified multiple potential HIPAA Security Rule violations including:
    - failures by Inmediata to conduct a compliant risk analysis to determine the potential risks and vulnerabilities to ePHI in its systems; and
    - to monitor and review its health information systems' activity.
  - The settlement resolves OCR's investigation concerning this HIPAA breach.

Recent HIPAA Cases: Inmediata Health Group, LLC (Inmediata)

- Fines:
  - Under the terms of the settlement, Inmediata paid OCR $250,000.
  - OCR determined that a corrective action plan was not necessary in this resolution as Inmediata had previously agreed to a settlement with 33 states that includes corrective actions that address OCR's findings in this matter.

OCR Recommendations

- OCR recommends Covered Entities and business associates that are covered by HIPAA take the following steps to protect ePHI:
  - Review all vendor and contractor relationships to ensure business associate agreements are in place as appropriate and address breach/security incident obligations.
  - Integrate risk analysis and risk management into business processes; conducted regularly and when new technologies and business operations are planned.
  - Ensure audit controls are in place to record and examine information system activity.
  - Implement regular review of information system activity.
  - Utilize multi-factor authentication to ensure only authorized users are accessing ePHI.
  - Encrypt ePHI to guard against unauthorized access to ePHI.
  - 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.

Recent HIPAA Cases

- November 19th, 2024, OCR, announced a $100,000 civil monetary penalty against Rio Hondo Community Mental Health Center (“Rio Hondo”) in California.

Recent HIPAA Cases: Rio Hondo Community Mental Health Center ("Rio Hondo")

- OCR launched an investigation after receiving a complaint from a patient that they were not given timely access to their medical records, despite multiple requests in writing and by telephone.
- OCR's investigation found that it took nearly 7 months from the time the patient first requested the records until Rio Hondo provided them.
- The patient made multiple telephone calls in July and August 2020, regarding the status of her request, but still did not receive the requested records.
- Based on the facts, OCR found that Rio Hondo failed to take timely action in response to the patient's right of access in accordance with the HIPAA Privacy Rule.
- In July 2024, OCR issued a Notice of Proposed Determination to impose a $100,000 civil monetary penalty. Rio Hondo waived its right to a hearing and did not contest the findings of OCR's Notice of Proposed Determination.

Recent HIPAA Cases

- July 1, 2024, OCR announced a settlement with Heritage Valley Health System (Heritage Valley), which provides care in Pennsylvania, Ohio and West Virginia, concerning potential violations of the HIPAA Security Rule, following a ransomware attack.

Recent HIPAA Cases: Heritage Valley Health System (Heritage Valley)

- Ransomware and hacking are the primary cyber-threats in health care.
- Since 2018, there has been a 264% increase in large breaches reported to OCR involving ransomware attacks.

Recent HIPAA Cases: Heritage Valley Health System (Heritage Valley)

- Resolution Agreement
  - Heritage Valley agreed to pay $950,000; and
  - Implement a corrective action plan that will be monitored by OCR for three years.

Recent HIPAA Cases: Heritage Valley Health System (Heritage Valley)

- Under the plan Heritage Valley will take a number of steps to resolve potential violations of the HIPAA Security Rule and protect the security of electronic protected health information, including:
  - Conduct an accurate and thorough risk analysis to determine the potential risks and vulnerabilities to the confidentiality, integrity, and availability of its electronic protected health information;
  - Implement a risk management plan to address and mitigate security risks and vulnerabilities identified in their risk analysis;
  - Review and develop, maintain, and revise, as necessary its written policies and procedures to comply with the HIPAA Rules; and
  - Train their workforce on their HIPAA policies and procedures.

OCR Recommendations

- OCR recommends Covered Entities and business associates that are covered by HIPAA take the following steps to mitigate or prevent cyber-threats:
  - Review all vendor and contractor relationships to ensure business associate agreements are in place as appropriate and address breach/security incident obligations.
  - Integrate risk analysis and risk management into business processes; conducted regularly and when new technologies and business operations are planned.
  - Ensure audit controls are in place to record and examine information system activity.
  - Implement regular review of information system activity.
  - Utilize multi-factor authentication to ensure only authorized users are accessing electronic protected health information (ePHI).
  - Encrypt ePHI to guard against unauthorized access to ePHI.
  - 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.

ACHC U®
EDUCATIONAL RESOURCES

Questions?

ACHC U
EDUCATIONAL RESOURCES

Thank you

Denise M. Leard, Esq.
dleard@bf-law.com | 806-345-6318

Brown & Fortunato
Amarillo · Dallas