HIPAA SUMMIT 41, February 27th, 2024

Recap of the Key Points

I'll strive to maintain brevity in this document, ensuring I cover all essential information from the summit. Where applicable, I'll include links for further reading. Enjoy!

Michael Cullen
Certified Ethical Hacker
HIPAA Certified IT Professional
Microsoft Certified Systems Administrator

2024 HIPAA Priorities for OCR – Office of Civil Rights

- Completing the review and finalization of the proposed changes to the HIPAA Privacy Rule introduced in 2023, aimed at enhancing privacy protections for reproductive health care, alongside adjustments to the Part 2 Rule.

- Giving precedence to investigations that align with current trends in HIPAA complaints and security breaches, including:

  - Cyber-attacks and hacking incidents

  - Ransomware attacks

  - Initiatives to enforce the right of individuals to access their health information

  - Efforts to enforce comprehensive risk analysis protocols

- Collaborating with the healthcare industry to bolster cybersecurity measures.

- Expanding our outreach and support across the country through:

  - Educational videos, guidance documents, and newsletters

  - Webinars and technical support sessions

- Conducting a thorough review of the HIPAA Security Rule to ensure it remains effective and up-to-date.

“Part 2” Final Rule

Issued on February 8, 2024, the Final Rule introduces modifications to Part 2 aimed at improving the coordination of care for patients with substance use disorders. It enhances confidentiality protections via civil enforcement mechanisms and integrates behavioral health information with other medical records, thereby aiming to elevate patient health outcomes. Key changes incorporated in the final rule are as follows:

- Now allows the use and disclosure of Part 2 records with a one-time consent from the patient that covers all future uses and disclosures for treatment, payment, and health care operations.

- Enables the redisclosure of Part 2 records by entities covered under HIPAA and their business associates, aligning with the HIPAA Privacy Rule, subject to specific exceptions.

- Introduces new rights for patients to receive an accounting of disclosures of their information and to place restrictions on certain types of disclosures.

- Grants the Department of Health and Human Services (HHS) the authority for civil enforcement, including the ability to impose civil money penalties for breaches of Part 2 rules.

- Mandates notification for any breaches involving Part 2 records, ensuring transparency and accountability.

Read about the final rule here:
https://www.federalregister.gov/documents/2024/02/16/2024-02544/confidentiality-of-substance-use-disorder-sud-patient-records

Suggested Changes to the HIPAA Privacy Rule to Support Reproductive Health Care Privacy

The proposal aims to enhance privacy measures by preventing the use or sharing of Protected Health Information (PHI) by regulated entities for the purposes of:

- Any criminal, civil, or administrative investigation or legal action against an individual related to seeking, obtaining, providing, or facilitating reproductive health care in cases where such care is legal in the context it's provided.

- Identifying any individual with the intent to initiate such investigations or proceedings.

This prohibition is specifically targeted in situations where:

- The reproductive health care involved is pursued, received, provided, or facilitated within a state where it is legal, but the investigation or proceeding originates from another state.

- The reproductive health care is protected, mandated, or explicitly allowed by federal law, irrespective of the state where the care is provided.

- The reproductive health care is delivered in a state authorizing the investigation or proceeding and complies with that state's laws.

The Office for Civil Rights (OCR) is currently reviewing public feedback and is in the process of developing a Final Rule on these matters.

NIST is offiering a guide for implementing the HIPAA Security Rule

This updated publication offers tools and insights designed to deepen understanding of the HIPAA Security Rule, promote adherence to its mandates, and enhance cybersecurity defenses. It includes:

- A comprehensive guide to the HIPAA Security Rule, including methods for evaluating and mitigating risks to electronic protected health information (ePHI).

- Recommendations for cybersecurity strategies and solutions that HIPAA-regulated entities and their business associates might incorporate into their information security protocols.

- A wealth of resources aimed at facilitating the effective implementation of the Security Rule. Specific areas of focus cover:

  - Detailed breakdowns of the requirements for Risk Analysis and Risk Management as stipulated by the HIPAA Security Rule.

  - Essential considerations for executing the provisions of the Security Rule.

  - Practical guidance on establishing security controls.

- Example inquiries to assess the sufficiency of cybersecurity practices in safeguarding ePHI.

Read the guide here: https://csrc.nist.gov/pubs/sp/800/66/r2/final

Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates

Outlines the responsibilities of HIPAA-regulated entities regarding the use of tracking technologies, such as Google Analytics and Meta Pixel, to gather and analyze data on user interactions with their websites or applications. It emphasizes that regulated entities must not employ tracking technologies in ways that could lead to unauthorized disclosure of Protected Health Information (PHI) or breach any HIPAA regulations.

Furthermore, it provides a clear explanation of what tracking technologies are, their applications, and the necessary measures regulated entities need to adopt to safeguard ePHI while utilizing these technologies in accordance with HIPAA standards. In detail, the bulletin offers insights and examples on:

- Tracking activities on websites

- Tracking within mobile applications

- The compliance duties of regulated entities in the context of using tracking technologies

The Office for Civil Rights (OCR) and the Federal Trade Commission (FTC) have also jointly issued a letter cautioning hospital systems and telehealth providers about the privacy and security risks associated with these technologies.

Read more here: https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html

Breach Activity

Statistics highlighting the most significant breaches since 2018 were presented, revealing concerning trends. Let's examine the data year by year.

Year	Number of “large” breaches	# of individuals affected
2018	369	15,210.437
2019	512	44,917,698
2020	663	34,800,838
2021	715	59,364,053
2022	719	55,962,895
2023	733	**134,787,438**

One silver lining in the breach statistics is the noticeable decrease in ransomware attacks from 2020 onwards, indicating an enhancement in cybersecurity awareness. On the flip side, the frequency of hacking incidents saw a twofold increase from 2020 to 2023. Alarmingly, the impact was extensive in 2023, affecting over 134 million individuals.

- In 2023, the Office for Civil Rights (OCR) handled 31,731 cases related to HIPAA.

- The majority of these cases were resolved as entities showed compliance through willing cooperation and the implementation of corrective measures.

- However, certain situations, due to the severity or extent of non-compliance, necessitated further enforcement measures.

- As part of resolving these issues, 136 settlement agreements were reached, comprising comprehensive corrective action plans and financial settlements.

- Additionally, there were 8 instances of civil money penalties being imposed.

Some of the Settlements Imposed:

$4.75 Million – Montefiore Medical Center

- An OCR investigation was initiated after a report of a breach disclosed that an employee had improperly accessed the electronic protected health information (ePHI) of 12,517 patients and had sold this information to a group engaged in identity theft.

- The investigation by OCR uncovered several potential infractions of the HIPAA Security Rule, including failures in:

  - Conducting a thorough risk analysis to pinpoint potential risks and vulnerabilities to ePHI,

  - Effectively monitoring and securing the activity within its health information systems, and

  - Implementing necessary hardware, software, and procedural safeguards to audit activities in systems handling or utilizing ePHI.

- As a result, Montefiore agreed to a settlement involving a payment of $4,750,000 to OCR and consented to execute a corrective action plan. This plan includes two years of OCR supervision aimed at enhancing the security of ePHI.

$480k – LaFourche Medical Group

- Following a report of a breach in which a hacker accessed an email account holding ePHI (impacting around 34,862 individuals), OCR initiated an investigation.

- The investigation uncovered several likely breaches of the HIPAA Security Rule, particularly in failing to:

  - Conduct thorough risk assessments to detect potential risks and vulnerabilities to PHI, and

  - Adequately monitor and protect the activity within its health information systems.

- In response, Lafourche agreed to a settlement that includes a payment of $480,000 to OCR and the implementation of a corrective action plan. This plan, overseen by OCR for two years, is aimed at bolstering the security of ePHI.

$40k – Green Ridge Behavioral Health

- An OCR inquiry was initiated after a breach report showed that a network server was compromised by ransomware, impacting over 14,000 patients.

- The investigation identified several potential violations of the HIPAA Security Rule, including the absence of:

  - A risk analysis to identify potential risks and vulnerabilities to electronic protected health information (ePHI),

  - Adequate security measures to mitigate these risks and vulnerabilities, and

  - Comprehensive monitoring of health information system activities to prevent cyber-attacks.

- To resolve these issues, Green Ridge has agreed to pay $40,000 to OCR and undertake a corrective action plan. This plan includes three years of OCR supervision aimed at enhancing the protection of ePHI.

I wrote about Green Ridge before: https://www.linkedin.com/posts/michael-cullen-250904113_green-ridge-behavioral-health-llc-resolution-activity-7166808228645818368-we47?utm_source=share&utm_medium=member_desktop

Risk Analysis Initiatives

OCR intends to intensify enforcement actions against Covered Entities (CEs) that neglect to conduct the mandatory risk analysis, a fundamental requirement outlined in the HIPAA Security Rule, as detailed in my HIPAA Guide: https://blackbearmssp.com/hipaa

Their goals are:

- Launch of a New Enforcement Effort

- Concentration on adherence to a required component of the HIPAA Security Rule

- Numerous significant breach inquiries by OCR have uncovered a common shortfall in conducting compliant risk analyses

- Aim to encourage improved measures for safeguarding electronic protected health information (ePHI)

- Enhance the overall security of data

Common HIPAA Complince Issues

OCR identified the most frequent compliance challenges they face in relation to HIPAA.

• Individual Right of Access

• Risk Analysis

• Business Associate Agreements

• Access Controls

• Audit Controls

• Information System Activity Review

Right of Access Explained

Although HIPAA is often associated with its emphasis on security and privacy, the law equally prioritizes the availability of data, specifically the "right of access," as a fundamental principle.

- The HIPAA Privacy Rule grants individuals the right to access their health records promptly—within 30 days, with an option for a one-time 30-day extension, and at a reasonable, cost-based fee.

- OCR frequently receives complaints about denied or unfulfilled requests for access to health records.

- An Enforcement Initiative was announced in February 2019, marking it as a priority for OCR.

- Nationwide investigations have been initiated.

- To date, there have been forty-four settlements and two Civil Money Penalties (CMPs) related to these enforcement efforts.

The OCR discussed best practices to implement. These best practices include:

- Ensure all vendor and contractor interactions are covered by Business Associate Agreements (BAAs) where necessary, including provisions for handling breaches and security incidents.

- Make risk analysis and management a core part of business operations; perform these activities routinely and ahead of introducing new technologies or business practices.

- Promptly dispose of any PHI (Protected Health Information) designated for disposal, whether it's stored on digital media or paper.

- Integrate insights gained from past security incidents into the overarching security management strategy.

- Conduct training tailored to the specific needs of the organization and the roles of employees, emphasizing the vital part each member plays in safeguarding privacy and security, and ensure this training is refreshed regularly.

Common Cyber Attacks Video creatd by OCR:

- A video detailing how adherence to the HIPAA Security Rule aids regulated entities in protecting against typical cyber-attacks, featuring a thorough breakdown of a cyber-attack's structure, including:

  - Entry through breached accounts

  - Reconnaissance efforts

  - Privilege escalation

  - Data theft or malware/ransomware deployment

- Discussion topics include:

  - Analysis of trends in OCR breaches and investigations

  - Prevalent methods of attack like phishing, exploiting vulnerabilities, and account compromises

  - OCR probes into vulnerabilities that precipitated or contributed to security breaches

- How compliance with the Security Rule can bolster regulated entities' defenses against cyber threats.

You can watch the video here: https://www.youtube.com/watch?v=VnbBxxyZLc8

HIPAA Risk Analysis Webinar:

We often encounter resistance from Covered Entities (CEs) who believe that conducting a risk analysis isn't mandated by HIPAA. However, this video clearly illustrates that such a belief is incorrect.

The video covers a lot including:

• How to prepare for a risk analysis

• How should ePHI be assessed

• What does it mean to be accurate and thorough

• What purpose does a risk analysis serve once completed

• Examples from OCR investigations

• Resources

You can watch the video here: https://www.youtube.com/watch?v=hxfxhokzKEU

OCR Releases Cybersecurity Performance Goals:

- In 2023, the Department of Health and Human Services (HHS) introduced Cybersecurity Performance Goals (CPGs) tailored for the healthcare sector. These guidelines are voluntary and aim to assist healthcare organizations in adopting effective cybersecurity measures.

- The objectives are crafted to enhance the healthcare industry's defenses against cyber threats, streamline responses to security incidents, and reduce the lingering risks.

- These efforts complement the HIPAA Security Rule, working together to bolster the security framework within healthcare.

View the specific goals in full detail here: https://hphcyber.hhs.gov/performance-goals.html

I hope this recap of the event provided you with valuable insights. I make it a point to stay updated with the latest in HIPAA developments, so you don't have to. Should you have any questions, please don't hesitate to reach out to me. To keep receiving my content, there's no need for any action on your part. However, should you decide to unsubscribe, please know that I fully respect and honor such requests.