PROGRAM MATERIALS
Program #35210
November 21, 2025

Ode to the Joy of HIPAA - A Focus on Emerging Obligations, Considerations and Trends

Celesq® AttorneysEd Center
www.celesq.com

5301 North Federal Highway, Suite 150, Boca Raton, FL 33487
Phone 561-241-1919

Ode to the Joy of HIPAA - A Focus on Emerging Obligations, Considerations and Trends.

Rachel V. Rose, JD, MBA

Celesq

Disclaimer

The information is current as of the date of the initial presentation and is not meant to constitute legal advice.

Agenda

- Learn 12 material items related to HIPAA compliance and mitigating risk.
- Appreciate current attacks that cybercriminals are deploying in the healthcare sector.
- Incorporate risk mitigation suggestions to decrease liability.
- Conclusion

Ode to HIPAA – 12 items

Days 1-3

- **Day 1:** Mark your calendar for February 16, 2026, to update Notice of Privacy Practices to integrate 42 CFR Part 2 items.
- **Day 2:** Consider, how legitimate is my third-party HIPAA risk analysis auditor? For example, are they asking if the truncated HHS-OCR 50 questions as part of its own audit program is sufficient or are they relying on the actual Security Rule and Privacy Rule CFR requirements for a comprehensive audit? Having represented companies before government agencies, the truncated version is not sufficient for covered entities and business associates.
- **Day 3:** Are state law requirements, including data breach reporting and the timeframes for providing medical records to patients included? Many state requirements differ from Federal HIPAA.

Days 4-6

- **Day 4:** Is training up to date?
- **Day 5:** Is data encrypted both at rest and in transit?
- **Day 6:** What is in your asset document and how does this differ from your access control document, which should list everyone who has access to a particular software, whether it is an electronic health record system or email.

Days 7-9

- **Day 7:** Are you addressing reproductive healthcare in light of the *Purl* case (Northern District of Texas) and *Skrmetti* (U.S. Supreme Court) and adjusting policies and procedures accordingly?
- **Day 8:** Is AI software being evaluated for HIPAA compliance and to ensure that it is safe, legal and effective?
- **Day 9:** Are state laws, including Texas S.B. 1188 being evaluated and incorporated into AI and HIPAA policies and procedures?

Days 10-12

- **Day 10:** Are you monitoring the latest bulletins from the FBI, CISA and DHS?
- **Day 11:** Have you scheduled your 2026 risk analysis and done adequate background checks on workforce members?
- **Day 12:** Are policies and procedures, as well as Business Associate Agreements up to date and do they consider potential updates set forth in the January 2025 Notice of Proposed Rule Making for the HIPAA Security Rule? Actual changes and announcements in 2026 by HHS-OCR should be monitored.

Current Attack Landscape

External and Internal Threat Actors

Internal Threat Actors

- 2021 Example – Gwinnett Medical Center CISO indicted for perpetrating an attack.
- 2025 Example – 3 former employees of 2 cybersecurity firms deploy Blackcat/AlphaV ransomware against its employers own clients.
  - 2 indicted
  - 3rd person – a co-conspirator – not named.

External Threat Actors

- **Healthcare ransomware attacks surge 30% in 2025, as cybercriminals shift focus to vendors and service partners**
  - In the first nine months of 2025, 293 ransomware attackswere recorded on hospitals, clinics, and other direct care providers.
  - An additional 130 attacks targeted businesses within the healthcare sector, including pharmaceutical manufacturers, medical billing providers, and healthcare tech companies.
  - Attacks on healthcare providers mirrored the figures from 2024 during the same period, while attacks on healthcare businesses rose by 30%.
- As of Oct. 3, 2025, 364 hacking incidents had been reported to the U.S. Department of Health and Human Services Office for Civil Rights, affecting over 33 million Americans.

AI

- According to the FBI – “Broadly speaking, AI systems are used to replicate or emulate certain aspects of cognition. We interact with AI almost every day in modern life, from the use of online search engines to video games, digital assistants commonly accessed through smart phones and smart devices, and automated cruise control functions in vehicles.”
- In the alert, the FBI warned of increased data theft and extortion intrusions from two specific groups.
- One of those groups is behind the recent Salesloft attack that opened a backdoor into Salesforce.
- Hackers exploited compromised OAuth tokens for the Salesloft Drift application, an AI chatbot that can be integrated with Salesforce via API.

Incorporate Risk Mitigation to Decrease Liability

2025 HHS OCR Resolution Agreements

- HHS' Office for Civil Rights Settles HIPAA Ransomware Security Rule Investigation with BST & Co. CPAs, LLP [PDF, 146 KB] - August 18, 2025
- HHS' Office for Civil Rights Settles HIPAA Ransomware Investigation with Syracuse ASC [PDF, 175 KB] - July 23, 2025
- HHS' Office for Civil Rights Settles HIPAA Privacy and Security Rule Investigation with a Behavioral Health Provider [PDF, 183 KB] - July 7, 2025

Blueprint for an AI Bill of Rights

- Five Principles

  (1)Safety and effectiveness

  (2)Algorithmic discrimination protections

  (3)Data privacy

  (4)Notice and explanation

  (5)Human alternatives, consideration and feedback

  https://bidenwhitehouse.archives.gov/ostp/ai-bill-of-rights/#:~:text=To%20advance%20President%20Biden's%20vision,or%20access%20to%20critical%20needs. (last visited November 9, 2025)

Risk Mitigation

- Adequate Training and Updates
- Providing medical records in the statutory-prescribed times – always look at state law first because it may be a shorter timeframe than the 30-day rule for federal HIPAA, which may be extended to 60 days.
- Conduct an annual risk analysis by a reputable third party that meets all of the Privacy Rule, Security Rule, Breach Notification Rule and Information Blocking, as well as state criteria.
- Review and revise comprehensive policies and procedures at least annually.
- Use 42 CFR § 483.85 as a framework to assess compliance programs generally.

Conclusion

Parting Thoughts

- Be proactive – cyber criminals are particular pernicious during the Holidays.
- Calendar January 31, 2026 as the date to have the revised NPP done before the February 16, 2026 due date.
- Schedule Annual HIPAA training, risk analysis and update P&Ps.
- Consider pros and cons, as well as potential downstream issues associated with the adoption of ethical, legal and safe AI.

Thank You and Questions

Rachel V. Rose – Attorney at Law, PLLC

Houston, Texas

(713) 907-7442 * www.rvrose.com