COSMOS
Navigate the Compliance Universe

Compliance Today - August 2022
The carrot, the stick, and the donkey: A HIPAA safe harbor?

By Ty Greenhalgh

Ty Greenhalgh (Ty.G@Claroty.com), Regional Director, Virginia Beach, VA.

- linkedin.com/in/tygreenhalgh/


Ty Greenhalgh

The carrot and the stick are a metaphor depicting the combination of both reward and punishment attempting to induce a desired behavioral response. We have all seen memes or cartoons of two riders racing donkeys. The losing rider is beating his donkey with a thorned switch and spurring it to move faster. The winner smugly sits in his saddle, casually holding out a baited pole in front of his donkey. Is one strategy better than the other? Are they more effective when used together? A new bill was recently signed into law that is passing out carrots to the healthcare industry.

The stick

In 2016 and 2017, the Office for Civil Rights (OCR) conducted HIPAA compliance audits of 166 covered entities (CEs) and 41 business associates (BAs).[1] The compliance effort ratings demonstrated 86% and 78% of the organizations documented inadequate effort and misunderstood HIPAA requirements related to risk analysis and risk management.

In 2018, during the Health Information and Management Systems Society convention in Las Vegas, I was shocked to hear then-Director of OCR Roger Severino announce, "The big juicy egregious breach is my priority… People need to come into compliance." Clearly OCR was signaling the healthcare industry to improve its cybersecurity posture, or else—the stick. While healthcare organizations made sincere attempts to improve their security and compliance with HIPAA, these efforts did not translate into cybersecurity breach reductions.

Cybersecurity breaches of 500 records or more steadily increased from 2018 to 2021: 369, 512, 663, and 714 incidents respectively.[2] During this time, OCR settled 53 cases with resolution agreements or corrective action plans (CAPs), with settlements exceeding $63 million dollars.[3] This figure does not reflect the costs to CEs and BAs for continued audits, impact to operations, legal fees, and CAPs. In September of 2021, OCR appointed a new director, Lisa J. Pino, who was formerly senior counselor at the U.S. Department of Homeland Security responsible for US cyber breach mitigation and developing new cybersecurity regulatory protections.[4]

Despite the CAPs and fines from OCR, organizations continue to misunderstand the requirements of HIPAA's Security and Privacy rules. The majority of investigations still find inadequate risk analysis and risk management practices. CEs and BAs consistently confuse the required gap analysis, risk analysis, and technical analysis, ultimately leaving the organization noncompliant and vulnerable. In 2018, OCR published an extremely helpful comparison between a risk analysis and gap analysis in an effort to help reduce confusion.[5]

While there have been no further audits since 2016, it is rumored OCR may hire a third party to handle HIPAA compliance and create a permanent audit program. If OCR is considering an increase in usage of the stick, it

would make sense to offset that behavioral conditioning with an incentive like this new law.

The carrot

The Health Information Technology for Economic and Clinical Health (HITECH) Act was created to promote the adoption of electronic health records within the healthcare system. On January 5, the president signed HR Bill 7898, amending the HITECH Act.[6] This law will allow the U.S. Department of Health & Human Services (HHS) to determine whether cybersecurity best practices were adopted by CEs or BAs. This would be applicable during an investigation of a breach, where financial and operational remedies are to be determined.

For organizations that can produce security best practice documentation for 12 months, consideration will be provided in an effort to reduce fines, audits, and remedies. Some in the industry are questioning whether this law is a "HIPAA safe harbor." While it technically seems to meet the definition by providing provisions to reduce legal or regulatory liability, HHS has used the term "safe harbor" specifically with encryption and the deidentification method of protected health information. We should be cautious using this term, as it may be easily misinterpreted and confuse organizations already struggling to understand OCR's guidance. A more relevant question might be, "What are recognized security practices?"

The donkey

Ultimately, both the carrot and the stick are designed to move the organization in the direction of improved compliance, security, and risk reduction. While the carrot and the stick are focal points of the story, the donkey's importance is frequently overlooked—yet it is the donkey that won the race. In an effort to improve outcomes, OCR has recommended particular steeds that it feels are capable of winning. The carrot is simply another technique to bring out the donkey's best performance. The health industry's success, in the race with hackers, rides upon choosing the best policies, procedures, and processes and driving them forward.

HR 7898 has identified recognized security practices as "standards, guidelines, best practices, methodologies, procedures, and processes developed under section 2(c)(15) of the National Institute of Standards and Technology Act, the approaches promulgated under section 405(d) of the Cybersecurity Information Sharing Act of 2015 (Cybersecurity Act), and other programs and processes that address cybersecurity and that are developed, recognized, or promulgated through regulations under other statutory authorities."

Most healthcare compliance, information technology, and information security departments are familiar with the National Institute of Standards and Technology (NIST) and its publications, Cybersecurity Framework (CSF), Privacy Framework, Risk Management Framework, etc. They provide a structure for effectively managing risk and applying technical and operational controls within the organization to improve HIPAA compliance and reduce risk. OCR has even created a crosswalk between the NIST CSF and the HIPAA Security Rule,[7] believing together they were more effective at improving security and compliance. Approaches under Section 405(d) of the Cybersecurity Act are less understood.

Cybersecurity Act, Section 405

Section 405(b) of the Cybersecurity Act required the HHS secretary to submit to the House of Representatives an assessment "on the preparedness of the health care industry in responding to cybersecurity threats."[8] Section 405(c) outlined requirements for the report. Section 405(d) required the HHS secretary to convene stakeholders and industry experts, establishing a task force to analyze how other industries implemented cybersecurity strategies and the challenges in securing the electronic health records and connected medical devices. The report concluded the healthcare industry's cybersecurity was in critical condition and provided recommendations,

imperatives, and action items.[9] Just prior to this assessment report being finalized and delivered to Congress in June 2017, the world was introduced to the WannaCry ransomware. A self-propagating worm, it replicated across the web, immediately shutting down the United Kingdom's healthcare infrastructure and threatening America's next. One of our nation's 16 critical infrastructures came dangerously close to being shut down![10] This generated a great deal of interest in the Health Care Industry Cybersecurity Task Force report.

Section 405(d) is the section referenced in the new law. Under Section 405(d), the HHS secretary is required to align healthcare industry security approaches. The 405(d) Task Group leveraged the Healthcare and Public Health Sector Critical Infrastructure Security and Resilience Public-Private Partnership.[11] The Task Group comprises a diverse set of members representing many areas and roles, including cybersecurity, privacy, healthcare practitioners, health IT organizations, and other subject-matter experts.

This Task Group's charge was to develop a document that is available to everyone at no cost and includes a common set of voluntary, consensus-based, and industry-led guidelines, practices, methodologies, procedures, and processes that serve as a resource to meet three core goals:

1. "Cost-effectively reduce cybersecurity risks for a range of health care organizations;
2. "Support voluntary adoption and implementation; and
3. "Ensure on an ongoing basis that content is actionable, practical, and relevant to healthcare stakeholders of every size and resource level."

The Task Group produced a four-volume publication, *Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients* (HICP).[12] The HICP publications define healthcare's top five most impactful cybersecurity threats and 10 best practices—and 89 subpractices—to mitigate them. I am honored to be a member of this Task Group and to have presented HICP's recommendations during HCCA's National Compliance Institute in 2018 and 2019 (see Table 1).

Top five threats	Top 10 mitigation strategies
1. Email phishing attacks 2. Ransomware attacks 3. Loss/theft of equipment or data 4. Insider data loss 5. Medical devices	1. Email protection systems 2. Endpoint protection systems 3. Access management 4. Data protection and loss prevention 5. Asset management 6. Network management 7. Vulnerability management 8. Incident response 9. Medical device security 10. Cybersecurity policies

Table 1: HICP recommendations

Volume 1, designed for the nontechnical and executives, is an easy-to-understand high-level overview explaining the complexity of securing healthcare, current threats, and how a variety of stakeholders can support improving cybersecurity. Volume 2 details the mitigation best practices for small organizations. Volume 3 addresses the same for medium to large organizations, providing additional best practices and considerations due to the larger and more complex ecosystems. Volume 4 provides templates and resources to assist in implementation.

Erik Decker, 405(d) private sector co-lead and chief information security officer and privacy officer for the University of Chicago Medicine, shared his thoughts on the impact of this new law: "Our industry is under attack, and this new law takes a significant step forward in raising the bar to protect our patients. The incentives that are offered by adopting recognized cybersecurity practices will go a long way to moving the needle in our industry. I am proud to serve and co-lead the 405(d) team and am incredibly proud of the *Health Industry Cybersecurity Practices* we have produced that will assist our industry. What a great way to start 2021."

Conclusion

OCR and the 405(d) Task Group have been clear in their statements that HICP is not a new regulation, nor a minimum baseline of practices to be implemented. It should not be used as a guideline for HIPAA, the General Data Protection Regulation, the Payment Card Industry Security Standards Council, or any other state law. It is a voluntary reference guide associating best practices to specific threats facing healthcare organizations. Each organization can decide which practices are applicable to reducing risk in their unique ecosystems.

Just as 100% compliance with HIPAA will not guarantee security, implementing all of the mitigations listed in the NIST CSF or HICP will not provide your organization with a HIPAA safe harbor. The frameworks referenced in the new law are work horses that, when effectively adopted due to either incentive or penalty, will lower the risk of cybersecurity incidents, increase HIPAA compliance, and potentially provide leniency from OCR.

Looking ahead

In May, the American Health Information Management Association responded to the HHS' request for information seeking public comment, which closed June 6.[13] In June 2021, the Office of Inspector General reported that the Centers for Medicare & Medicaid Services lacked consistent oversight of cybersecurity for networked medical devices.[14] In June 2022, Herman McKenzie, a director at The Joint Commission, was the closing speaker at the Association for the Advancement of Medical Instrumentation national conference. Director McKenzie stated that The Joint Commission had convened a Technical Advisory Council to address this issue and considers adding to the interpretive guidelines within the existing survey. It seems reasonable that the Centers for Medicare & Medicaid Services would consider including many of the suggested controls in already recognized security practices found in mitigation strategy number nine, medical device security.[15]

Takeaways

- The Health Information Technology for Economic and Clinical Health Act was amended to recognize security practices.
- Covered entities and business associates that comply with the law may see the Office for Civil Rights reduce its fines, audits, and corrective action plans in the event of a cybersecurity incident.

- The best practice cybersecurity mitigations suggested within this law are those produced by the National Institute of Standards and Technology and/or the 405(d) Task Group.
- Section 405 of the Cybersecurity Act of 2015 required an audit, report, and recommendations for aligning the heath industry's cybersecurity posture with other industry best practices.
- Compliance with the law requires an organization to document the usage of these best practices for one year.

1 U.S. Department of Health & Human Services, Office for Civil Rights, *2016-2017 HIPAA Audits Industry Report*, December 2020, https://www.hhs.gov/sites/default/files/hipaa-audits-industry-report.pdf.
2 "Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information," Office for Civil Rights, U.S. Department of Health & Human Services, accessed June 2, 2022, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.
3 "HIPAA Fines Listed by Year," Compliancy Group, accessed June 7, 2022, https://compliancy-group.com/hipaa-fines-directory-year/.
4 U.S. Department of Health & Human Services, "U.S. Department of Health and Human Services Announces Lisa J. Pino as Director for Office for Civil Rights," news release, September 27, 2021, https://www.hhs.gov/about/news/2021/09/27/hhs-announces-lisa-j-pino-as-director-for-office-for-civil-rights.html.
5 U.S. Department of Health & Human Services, Office for Civil Rights, "Risk Analyses vs. Gap Analyses – What is the difference?" April 2018, https://www.hhs.gov/sites/default/files/cybersecurity-newsletter-april-2018.pdf.
6 An act to amend the Health Information Technology for Economic and Clinical Health Act to require the Secretary of Health and Human Services to consider certain recognized security practices of covered entities and business associates when making certain determinations, and for other purposes, Pub. L. No. 116-321, 134 Stat. 5072 (2021).
7 U.S. Department of Health & Human Services, Office for Civil Rights, "HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework," February 2016, https://www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf.
8 Cybersecurity Information Sharing Act of 2015, S.754, 114th Cong., § 405(b) (2015).
9 Health Care Industry Cybersecurity Task Force, *Report on Improving Cybersecurity in the Health Care Industry*, June 2017, https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf.
10 U.S. Department of Homeland Security, Office of Cyber and Infrastructure Analysis, "Potential Impacts of WannaCry Ransomware on Critical Infrastructure," May 14, 2017, https://info.publicintelligence.net/DHS-OCIA-WannaCry.pdf.
11 U.S. Department of Health & Human Services, Office of the Chief Information Officer, "Fact Sheet: Cybersecurity Act of 2015, Section 405(d)," Fall 2018, https://www.nist.gov/system/files/documents/2018/10/18/hhs_fact_sheet_-_csa_405d_cleared.pdf.
12 U.S. Department of Health & Human Services, Healthcare and Public Health Sector Coordination Councils, *Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients*, accessed June 2, 2022, https://healthsectorcouncil.org/wp-content/uploads/2018/12/HICP-Main-508.pdf.
13 American Health Information Association, "Considerations for Implementing the Health Information Technology for Economic and Clinical Health (HITECH) Act, as amended," letter to the Office for Civil Rights director, May 23, 2022, https://www.ahima.org/media/tl2cdnyx/final-ahima-ocr-rfi-comment-letter_052322.pdf.
14 U.S. Department of Health & Human Services, Office of Inspector General, "Medicare Lacks Consistent Oversight of Cybersecurity for Networked Medical Devices in Hospitals," issue brief, OEI-01-20-00220, June

2021, https://oig.hhs.gov/oei/reports/OEI-01-20-00220.pdf.
15 U.S. Department of Health & Human Services, "Technical Volume 2: Cybersecurity Practices for Medium and Large Health Care Organizations," accessed June 8, 2022, 87, https://405d.hhs.gov/Documents/tech-vol2-508.pdf#page=87.