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.