

## **HITECH Addition to HIPPA**

Nicholas Jacob

University of Advancing Technology

February 26, 2023

The Health Information Technology for Economic and Clinical Health Act (HITECH), released in 2009, was meant to incentivize use of electronic health record systems in the health care industry as well as supplement the Health Insurance Portability and Accountability Act (HIPAA) (ASHA, n.d.). It also increased the penalties of HIPAA violations to organizations with repeat or uncorrected infringements (Petersen, 2018). Before HITECH was put into act, HIPAA was not regularly enforced, with HITECH not only were penalties increased but with periodic audits now required by the Department of Health and Human Services, organizations in violation are more likely to be caught without individuals needing to bring attention (ASHA, n.d.).

HITECH's main goal seemed to initially be just to get the health care industry into using electronic health care systems but there were some security related impacts. The act expanded who falls under HIPAA to not just the healthcare organizations but their business associates and service providers (Petersen, 2018). It also brought about a Breach Notification Rule which required entities covered by HIPAA to notify any individuals affected by a breach within sixty days of the breach's discovery (HIPAA Journal, 2023). The last security related item is a bit of a stretch but has to do with what is known as The HIPAA Wall of Shame. This wall of shame is a portal available is a published summary of data breaches within healthcare (HIPAA Journal, 2023), which may create more of a motivation to ensure security is being observed.

I wouldn't consider HITECH to be "in-depth" when it comes to security implementations. It mostly relies on the HIPAA Security Rules and is more of a backing and small expansion on it in ways such as its tougher penalties. HIPAA was already mandatory and had security implementation requirements, so HITECH just made these requirements relevant to more organizations (HIPAA Journal, 2023).

With HITECH incentivizing the switch to electronic systems, I would consider its main security implementation to be that it brought more organization under HIPAA. With these organizations now within the umbrella of HIPAA, enforcement has been expanded. More organizations now have to ensure they are in compliance of the privacy and security rules that HIPAA requires (HIPAA Journal, 2023). The Department of Health and Human Services conducting audits of not just the covered entities but the newly included business associates means that violations are being caught and enforced (ASHA, n.d.). More accountability, violation enforcement, and required breach notification are the main security implementations of the Health Information Technology for Economic and Clinical Health Act.

## References

- American Speech-Language-Hearing Association. (n.d.). *Health Information Technology for Economics and Clinical Health (HITECH) act*. ASHA. Retrieved February 27, 2023, from <https://www.asha.org/practice/reimbursement/hipaa/hitech-act/>
- Petersen, S. (2018, January 30). *What is Hitech (Health Information Technology for Economic and Clinical Health) act of 2009?: Definition from TechTarget*. TechTarget. Retrieved February 27, 2023, from <https://www.techtarget.com/searchhealthit/definition/HITECH-Act>
- What is the Hitech Act?* HIPAA Journal. (2023, January 3). Retrieved February 27, 2023, from <https://www.hipaajournal.com/what-is-the-hitech-act/>