Research and Analysis

Allan Wheelock

University of Advancing Technology

Author Note

This paper was prepared for NTS 435, International and Federal INFOSEC Standards and Regulations, taught by Joseph Pollock.

Research and Analysis

There are many different groups that aim to help provide a standard for security in different areas of business. For this paper I’ll be focusing on the healthcare industry, and more specifically HITECH.

Before we dive into how in-depth HITECH is we must first understand what HITECH is and what it does, as well as why that’s important. HITECH is an acronym for “The Health Information Technology for Economic and Clinical Health Act”. This act was enacted as part of the American Recovery and Reinvestment Act of 2009. The purpose of it was to promote the use health information technology. What this means is that it was to promote new technology for use in the healthcare industry. HITECH is often compared to HIPAA when it comes to the enforcement and implementation of it.

HITECH is relatively in-depth when it comes to security implementations. I personally believe HITRUST is more in-depth. However, I don’t have hands on experience working with HITECH like I do with HITRUST. One of the areas in which HITECH makes sure to include is releasing a notification of a breach for unauthorized uses and disclosures of what they call “unsecured PHI”. (hipaasurvivalguide.com). What HITECH classifies “unsecured PHI” as is simply “unencrypted PHI”. If any form of unsecured PHI is leaked the company responsible must notify the patients effected. If that breach effects more than 500 people, then the company must also notify HHS. If HHS is notified, then this will trigger posting that on the HHS website. Under certain more extreme conditions, the local media will also be notified. The part of this that really stuck out to me was the final line that states: “notification is triggered whether the unsecured breach occurred externally or internally” (hipaasurvivalguide.com). The reason this stuck out to me is that it shows HITECH is concerned with external parties getting this information, as well as unauthorized employees within that company. I think this is a good thing and incredibly important to monitor both external and internal breaches.

HITECH has a lot in common with HIPAA, but they also balance each other out through checks and balances. For example, HITECH has more details on business associates working with healthcare companies and more enforcement than HIPAA. Before HITECH, privacy and security requirements were imposed on businesses and their associates through contracts with covered entities. There are likely several small providers that have these requisite contracts in place. In other cases, these contracts may exist, but don’t meet the requirements of HIPAA’s rules. HIPAA has been relatively lax with this enforcement, in turn, HITECH is not lax with it. Under the HITECH act, businesses and their associates are now held accountable to this through a higher standard. Through HITECH these businesses and their associates are required to comply with the safeguards contained in the HIPAA Security Rule. With the advancements we are currently experiencing in technology the likelihood of an increase in ePHI and the exchange of it, brings more privacy and security not only to members and patients, but also the businesses, and stakeholders involved. With that, brings an increase in communication between providers and vendors.

The HITECH act also includes an area that has specific rules to ePHI. ePHI is electronic patient health information. With the increase in everything becoming digital in our world this is a very important policy. This is especially important when you take COVID-19 and its effects to the world in consideration. With the way the world is today more members and patients are requesting their records digitally than their paper counterparts.

In conclusion, HITECH is relatively in-depth with how it enforces security in healthcare. It considers more than just PHI and the members. It also ensures to include enforcement on the vendors involved, the stakeholders, and the businesses themselves.

References

HITECH Act Enforcement Interim Final Rule. (2022). Retrieved 24 February 2022, from <https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html>

HITECH Act Summary. (2022). Retrieved 24 February 2022, from <https://www.hipaasurvivalguide.com/hitech-act-summary.php>