Jackson Warren

Jeremy Bergen

CSCI 370

9/24/21

Week 4 Assignment: SOX vs HIPAA

Retention Requirements:

SOX has very clear guidelines for different sets of information, some of which differ based on what they are. For example, tax returns and payable ledgers must be retained for 7 years, while things like customer invoices must be retained for 5 years. Payroll and bank statements must be kept forever. HIPAA is very similar, but differs when it comes to territory and position of the keeper of said documents. In Florida, physicians must maintain documents for 5 years, while hospitals must for 7. Age also plays a role, as in Nevada, where minors must have their records maintained till they reach the age of 23. Needless to say, HIPAA is a very complex target when it comes to retention requirements.

Reporting Requirements:

SOX requires that all companies must create an end-of-year financial disclosure report. This then must be audited by an independent third-party that reviews this report as well as their policies and procedures. Once again, there is a swath of information on HIPAA reporting guidelines. Reporting is obviously a large issue for HIPAA, as its primary purpose is to protect information. Mostly, what I’ve found is the only reporting requirements for HIPAA is under the Privacy Rule, or has signed authorization from the individual. This privacy rule protects individuals from release of their information in many circumstances, and does not have an time allotment for needed reports.

Logging Requirements:

SOX is much more business oriented for this category as well. Specifically, SOX requires that Internal controls, Network activity, Database activity, Login activity (success and failures), Account activity, User activity, and Information Access are all logged, monitored, and reported. Obviously, HIPAA will require very thorough activity logs. Application usage logs, access requests, really any activity requesting any HIPAA information must be logged and kept, or even reported if unauthorized. Specifically, this includes each time a user logs in, whenver changes are made to databases, when new users are added, access levels for each user, file access by users, logins to operating systems, firewall logs, anti-malware logs. These logs must be kept for a minimum of 6 years, but this also differs by many different factors.

Security Requirements:

For actual security, SOX is mostly based off the idea of checks and balances. Those complying with SOX must comply with all the previously stated items or those responsible could face jail time. They also must provide evidence that they are following security policies and enforcement of the such. I couldn’t find anything on physical security or exact security measures required for SOX. For HIPAA, I could not find any specific security requirements either. As long as companies under HIPAA are capable and have proof of the ability to protect the personal data they state (which that in itself is very complex and long), they don’t state any other specific requirements for security (such as a specific set of programs or hardware).

References:

Compliancy Group. (2020, November 30). *What Are HIPAA Audit Trail and Audit Log Requirements*. https://compliancy-group.com/hipaa-audit-log-requirements/

Compliancy Group. (2021, May 25). *What is the HIPAA Security Rule: Safeguards & Requirements*. https://compliancy-group.com/hipaa-security-rule/

Journal, H. (2021, July 22). *Clarifying the HIPAA Retention Requirements*. HIPAA Journal. https://www.hipaajournal.com/hipaa-retention-requirements/

Myerson, J. (2019, June 13). *4 steps to remain compliant with SOX data retention policies*. SearchCompliance. https://searchcompliance.techtarget.com/tip/Four-steps-to-consolidate-SOX-data-retention-and-deletion-processes

Rights, O. F. C. (2020, December 10). *Privacy*. HHS.Gov. https://www.hhs.gov/hipaa/for-professionals/privacy/index.html

*Sarbanes-Oxley (SOX) Audit Requirements*. (2021, September 18). Https://Www.Sarbanes-Oxley-101.Com/Sarbanes-Oxley-Audits.Htm. https://www.sarbanes-oxley-101.com/sarbanes-oxley-audits.htm