GSPA HEALTH INSURANCE COMPLIANCE REVIEW

Revision 1

2/26/2023

Bilal Anarwala

Executive Summary

The health insurance company Green Sword, Purple Armor (GSPA) wanted to know what compliance requirements they needed to operate. They currently operate in the states of Illinois, Wisconsin, and Indiana. After evaluating GSPA's business practices, it was determined that they needed to be HIPAA, PCI, and SOX compliant. Optionally, they need to be NIST compliant as well if they want to have government contracts in the future. I have highlighted and explained the security controls that GSPA needs to legally and securely operate in the states listed above.

Compliance Requirements

When it comes to determining the compliance requirements, there are a couple of factors that determine the major laws, regulations, and standards that GSPA needs to comply with. The first factor is the state(s) that GSPA operates in with the second factor being the line of work that GSPA is involved in. Given GSPA is a health insurance/healthcare provider operating in the states of Illinois, Indiana, and Wisconsin, the following three are the major compliance requirements that GSPA has to adhere to:

The Health Insurance Portability and Accountability Act (HIPAA): This is a US federal law that regulates the use and disclosure of patient's health information by healthcare providers. Since GSPA is a healthcare provider, they are required by law to be HIPAA compliant to ensure the privacy of patient data. This compliance is important because it is needed to maintain trust between healthcare providers and the patients that they provide for. In order for that to be done, GSPA must do the following:

1. "Ensure the confidentiality, integrity, and availability of all e-PHI (protected health information)"
2. "Detect and safeguard against anticipated threats to the security of the information"
3. "Protect against anticipated impermissible uses or disclosures that are not allowed by the rule"
4. "Certify compliance by their workforce"

Source: CDC Website (sources cited in works cited page)

Failure to properly comply with HIPAA will result in fines for GSPA as well as damage to the reputation of GSPA as a whole.

The Payment Card Industry Data Standards (PCI-DSS): PCI compliance refers to a set of security standards that ensure that organizations that accept credit cards as a payment method will have secure ways to handle that sensitive information. GSPA mentioned that they allow their customers to pay their deductibles with their credit cards. This means that they have to be PCI compliant. To be compliant, there are 12 requirements that GSPA needs to implement. The following are those requirements:

1. “Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters
3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks
5. Use and regularly update anti-virus software or programs
6. Develop and maintain secure systems and applications
7. Restrict access to cardholder data by business need to know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data
10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes
12. Maintain a policy that addresses information security for all personnel”

(sources cited in works cited page)

Failure to properly comply with PCI standards can result in data breaches, fines, damage the reputation of GSPA, and overall jeopardize security.

The Sarbanes-Oxley Act (SOX): This is also a US federal law that is put into place to improve the accuracy and reliability of financial disclosures. This is there as a way to protect the general public/investors from fraudulent practices from publicly traded companies in the US. Since GSPA is publicly traded on the NASDAQ, they have to be SOX compliant. To be SOX compliant, GSPA needs to do the following:

1. “Establish safeguards to prevent data tampering
2. Establish safeguards to establish timelines.
3. Establish verifiable controls to track data access.
4. Ensure that safeguards are operational.
5. Periodically report the effectiveness of safeguards.
6. Detect Security Breaches.
7. Disclose security safeguards to SOX auditors.
8. Disclose security breaches to SOX auditors.
9. Disclose failures of security safeguards to SOX auditors.”

(sources cited in works cited page)

Failure of GSPA to comply with SOX can result in fines, and removal from the NASDAQ. If members of GSPA submit incorrect information, they can face jail time and expensive fines.

The National Institute of Standards and Technology (NIST): This framework provides a set of guidelines that aim to mitigate cyber risks. While this compliance is mandatory for organizations that want to contract with the federal government. While GSPA does not currently contract for the government, they might choose to in the future since they can receive government funding, and

becoming NIST compliant is a step in the right direction. The following framework needs to be implemented to be NIST compliant:

1. “Identify: The organization identifies their assets, systems, and data that need protecting.
2. Protect: The organization implements appropriate safeguards to protect the critical assets, systems, and data identified previously.
3. Detect: The organization must add a system in place to detect cybersecurity incidents and events in a timely manner.
4. Respond: The organization must have a plan in place to respond to and contain cybersecurity incidents and events appropriately.
5. Recover: The organization must have a plan in place to recover from cybersecurity incidents and events, and revert back to normal operations.”

(sources cited in works cited page)

Failure to be NIST compliant would not result in any negative effects on GSPA as of now since it does not contract out to the government. However, if they do contract to the government and fail to meet compliance requirements, their government funding and contracts will be severed.

Security Control Table:

Attached with this document is the security control table that highlights a list of security controls that GSPA needs to meet compliance requirements.

Security Controls

There are a handful of controls that need to be implemented for GSPA to be compliant. As a reminder, NIST is a framework that GSPA can optionally become compliant with if they want to contract out with the government. The following are the security controls that need to be implemented:

1. Install Firewalls
    a. This control sets up and installs firewalls at GSPA’s locations. The firewalls will act as a barrier blocking unwanted and malicious traffic from entering GSPA’s network. This is a good measure to make sure that only what’s allowed comes through the network. Installing firewalls falls under PCI, SOX, HIPAA, and NIST.
2. Do not use default system passwords
    a. This control also aims to prohibit unauthorized access by enabling specific passwords on GSPA’s devices/systems rather than using default passwords. This control falls under PCI, SOX, HIPAA, and NIST.
3. Protect stored cardholder data/patient data

   a. This control aims to secure cardholder and patient data. This is done in various different ways such as encrypting, monitoring, and securing the data. This control falls under PCI, HIPAA, and NIST.
4. Encryption
   a. This control seeks to encrypt all of GSPA's data and traffic. This falls under PCI, HIPAA, and NIST.
5. Regularly update antivirus and other programs
   a. This control aims to prevent unwanted parties from utilizing vulnerabilities to gain unauthorized access to your systems. By updating your antivirus and other relevant software, you mitigate that risk. This control falls under PCI, HIPAA, and NIST
6. Develop security systems
   a. This control involves implementing both physical and digital security systems to protect GSPA from breaches and unauthorized access. This falls under SOX, HIPAA, and NIST.
7. Restrict access to cardholder data(user privileges)
   a. This control limits cardholder data access to only those that are authorized to do so. This falls under PCI, HIPAA, and NIST.
8. Assign user ID's to anyone with computer access
   a. This control will assign user ID"s to anyone who has access to GSPA's network and their systems to keep tabs on everyone's activity. This falls under SOX, HIPAA, and NIST.
9. Restrict physical access to cardholder data
   a. This control branches off of control 7 aiming to physically secure sensitive data such as patient data and credit card information. This control falls under PCI, SOX, HIPAA, and NIST.
10. Track/monitor all access to network and cardholder data
   a. This control is meant to keep tabs on any user's access to cardholder data to make sure any activity can be traced back. This falls under PCI, SOX, HIPAA, and NIST.
11. Regularly test systems and processes (Security Testing)
   a. This control is meant to test and identify any vulnerabilities that can be fixed to prevent breaches/attacks. This control falls under PCI, SOX, HIPAA, and NIST.
12. Risk Assessment
   a. This control seeks to highlight and identify risks that are present in our systems. This falls under PCI, SOX, HIPAA, and NIST
13. Data Backups
   a. This control seeks to prevent data loss in the event of a natural disaster or data breach. This falls under PCI, SOX, HIPAA, and NIST.
14. Business continuity
   a. This control seeks to ensure that GSPA as a business can still operate in the event of a disaster or data breach. This falls under PCI, SOX, HIPAA, and NIST.
15. Security training

a. This control seeks to make sure that the staff at GSPA are aware of identifying threats and attempts of social engineering. Ensuring proper training can secure GSPA. This falls under

Implementation Plan

Below is the implementation plan for implementing the security controls elaborated on prior. This plan is in order of highest priority to lowest priority:

1. **Risk Assessment:** This should be the first thing to do before anything else should be done. This can help GSPA identify its vulnerabilities and determine the necessary action they need to take to fix them.
2. **Develop Security Systems:** After determining the risks and vulnerabilities that GSPA has, they can start developing the security systems they need to secure their locations.
3. **Install firewalls:** Installing firewalls can help prevent unauthorized access from outside parties and can help prevent attacks on their networks.
4. **Protect patient and cardholder data:** Given that GSPA handles a lot of sensitive patient and cardholder data, this should be a high priority and should be secured.
5. **Restrict access to cardholder data:** To protect patient and cardholder data, access to this data should be restricted to those who need to access this data.
6. **Restrict physical access to cardholder data:** After digitally restricting this data, the next step would be to physically do so such as putting records into locked rooms and offices.
7. **Encryption:** All data needs to be encrypted to add a layer of security
8. **Assign user ID's to anyone with computer access:** After securing all of the confidential data, efforts to keep tabs on employee activity needs to be made to ensure all activity can be traced back to each employee.
9. **Track and monitor all access to network and cardholder data:** After the proper measures are put into place, monitoring can be done to watch over GSPA's business operations.
10. **Do not use default system passwords:** There is no point in implementing any security measures if the passwords to them are weak. This is why this should be the next priority.
11. **Data backups:** Frequent data backups need to be made. In the event of a natural disaster or data breach, the backup data can be restored.
12. **Regularly update anti-virus and software:** Ensuring the latest version of antivirus and other software is installed can help prevent prior vulnerabilities from being exploited by hackers.
13. **Business continuity:** After all the controls have been implemented, a thorough business continuity plan needs to be created to ensure that GSPA can go back to standard operations after a breach or disaster.
14. **Regularly test systems and processes:** Regularly testing GSPA's security measures can help ensure that GSPA has been properly secured and that their backups function properly. It also

helps improve GSPA's systems and can determine how good or bad the business continuity plan is.

15. **Security training:** Finally, all employees need to have the proper security training to make sure that they remain vigilant and can identify when a security breach is happening. It can also help prevent attacks from occurring such as social engineering attacks.

Conclusion

After looking through GSPA's business operations, it was determined that they needed to be compliant with PCI, SOX, and HIPAA. Optionally they will need to be compliant with NIST if they want to contract out to the government in the future. Additionally, a list of security controls has been outlined that GSPA would have to implement at their locations in order for them to remain compliant with the laws listed above. Failure to do so would result in a multitude of negative consequences including their removal from the NASDAQ.

Works Cited

Anthony, Ronald. “NIST SP 800-53 Explained.” *CyberSaint Security*, https://www.cybersaint.io/blog/what-is-nist-800-53#:~:text=What%20is%20NIST%20800%2D53,confidentiality%2C%20integrity%2C%20and%20availability.

CDC. “Health Insurance Portability and Accountability Act of 1996 (HIPAA).” *Centers for Disease Control and Prevention*, U.S. Department of Health & Human Services, 27 June 2022, https://www.cdc.gov/phlp/publications/topic/hipaa.html#:~:text=The%20Health%20Insurance%20Portability%20and,the%20patient's%20consent%20or%20knowledge.

Chipeta, Catherine. “Top 8 Healthcare Cybersecurity Regulations and Frameworks: Upguard.” *UpGuard*, 16 Feb. 2023, https://www.upguard.com/blog/cybersecurity-regulations-and-frameworks-healthcare.

Group, Compliancy. “What Is HIPAA Compliance?” *Compliancy Group*, 8 Nov. 2022, https://compliancy-group.com/what-is-hipaa-compliance/.

HCS. “Health Insurance Portability & Accountability Act.” *What Is HIPAA*, https://www.dhcs.ca.gov/formsandpubs/laws/hipaa/Pages/1.00WhatisHIPAA.aspx.

Magnusson, Andrew. “What Is Sox Compliance? 2023 Complete Guide.” *StrongDM*, StrongDM, 9 Jan. 2023, https://www.strongdm.com/sox-compliance.

Nordlayer. “PCI DSS Compliance Checklist: Is Your Business Compliant?” *NordLayer*, 14 June 2022, https://nordlayer.com/blog/pci-dss-compliance-checklist/.

Oswal, Piyush. “What Are the 12 Requirements of PCI DSS Compliance?” *ControlCase*, 21 Feb. 2023, https://www.controlcase.com/what-are-the-12-requirements-of-pci-dss-compliance/.

Reciprocity. “Complete Guide to NIST: Cybersecurity Framework, 800-53, 800-171.” *Reciprocity* , 19 Nov. 2021, https://reciprocity.com/resource-center/complete-guide-to-nist-cybersecurity-framework-800-53-800-171/.

Rohena, Richard. “PCI-DSS Compliance - Requirements and Levels.” *Check Point Software*, Check Point Software, 11 May 2022, https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cspm-cloud-security-posture-management/pci-dss-compliance/.

Ross, Ron, et al. “Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.” *CSRC*, 28 Jan. 2021, https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final.

Ross, Ron. *NIST SP 800-171*. NIST, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf.

Suthers. “ Sarbanes Oxley.” *Sarbanes-Oxley Compliance Checklist*, https://www.sarbanes-oxley-101.com/sarbanes-oxley-checklist.htm.

Woock, Kurt, and Lisa Anthony. “What Is PCI Compliance? 12 Requirements & Guide.” *NerdWallet*, 18 Oct. 2022, https://www.nerdwallet.com/article/small-business/pci-compliance.