COMPLIANCE REVIEW AND COMPILATION, GREEN SWORD PURPLE ARMOR (GSPA) HEALTH INSURANCE

By Esteban Miranda

DePaul University
CSEC394

CONTENTS

PART 1: COMPLIANCE REQUIREMENTS

It is essential to understand that Green Sword, Purple Armor (GSPA) is a health insurance and managed healthcare provider. One significant compliance that GSPA must follow is the Health Insurance Portability and Accountability Act of 1996.[1] HIPPA is a guideline the United States Congress created to protect the personal healthcare records maintained by healthcare industries. HIPAA also prohibits healthcare providers from disclosing health information to anyone, but the patient and their authorized party. HIPAA protects the privacy and security of people's health records and gives them rights to their health information. GSPA is publicly traded on Nasdaq and must adhere to the Sarbanes-Oxley (SOX) Act of 2002.[2] The SOX Act is a law passed by the United States Congress that helps protect investors from fraudulent financial reporting by corporations due to several scandals in the early 2000s. GSPA allows its customers to pay for their deductibles via all major credit cards, which means they must follow the Payment Card Industry Data Security Standard (PCI DSS).[3] PCI DSS enforces security standards to ensure the protection and security of customers credit card information. The Payment Card Industry Security Standards Council (PCI SSC) manages the Payment Card Industry (PCI) security to improve payment security during transactions. PCI DSS is overseen and operated by the PCI SSC, which was created and organized by major credit card companies.

[1] HIPAA

[2] SOX

[3] PCI DSS

PART 2: SECURITY CONTROLS REQUIREMENTS TABLE

#	Control Name	HIPAA	SOX	PCI DSS	Mandatory or Optional
1	Encryption of Sensitive data	45 CFR Part 160 and Part 164, Subparts A and C.	SOX Section 302, 404, 409. Certified Sarbanes-Oxley Expert (CSOE)	Requirement 3 (Page 73), Requirement 4 (Page 102)	Mandatory
2	Administrative Safeguards	§164.308(a)(5)	SOX Section 302, 404, 409. Certified Sarbanes-Oxley Expert (CSOE)	Requirement 2 (Page 60), Requirement 6 (Page 124), Requirement 7 (Page 149), Requirement 12 (Page 259)	Mandatory
3	Access Control, Integrity, Authentication	§164.312(a)(1), §164.312(c)(1), $164.312(d)	SOX Section 302, 404, 409. Certified Sarbanes-Oxley Expert (CSOE)	Requirement 6 (Page 124), Requirement 7 (Page 149), Requirement 8 (Page 161)	Mandatory
4	Audit Controls	§ 164.312(b)	SOX Section 302, 404, and 409. Certified Sarbanes-Oxley Expert (CSOE)	Requirement 3 (Page 73), Requirement 5 (Page 111)	Mandatory
7	Network Security	§164.312(e)(1)	SOX Sections 302, 404, 409. Certified Sarbanes-Oxley Expert (CSOE)	Requirement 1 (Page 39), Requirement 4 (Page 102), Requirement 10 (Page 212),	Mandatory

				Requirement 11 (Page 231)	
8	Physical Security	§164.310(a)(1), § 164.310(b), § 164.310(c), § 164.310(d)(1)	SOX Section 302, 404, 409. Certified Sarbanes-Oxley Expert (CSOE)	Requirement 9 (Page 190)	Mandatory

PART 3: EXPLAIN THE CONTROLS.

ENCRYPTION OF SENSITIVE DATA:

The encryption and decryption of data fall under a couple of Security Rule standards for HIPAA compliance.[4] Under Technical Safeguards, there is a security standard for transmission security that addresses encryption.[5] Another security standard, named access control, also discusses the security standard of encryption and decryption.

According to SOX (Sarbanes-Oxley Act) Section 404, it is mandatory for financial reports to incorporate an internal control report.[6] This report assesses the management's evaluation of internal controls that are in place and their effectiveness in mitigating any risks. The sections do not go in-depth about information security controls, such as network security; they instead state internal controls. The internal control reports state management responsibilities for establishing internal control structures and procedures for financial reporting. The reports also include an evaluation conducted at the end of the issuer's fiscal year to review the effectiveness of the internal control structure and procedures related to financial reporting. An important note is that there is a SOX certification named SOX-certified with the Sarbanes-Oxley Expert (CSOE).[7] The certification can help follow the SOX Act 2002. The certification gives an in-depth look at the critical issues in SOX. The certification will discuss the importance of financial auditing. Encrypting financial reports when stored securely will prevent any altering, so it is required.

Protect Stored Account Data is Requirement 3. It contains much information on different categories and encryption. Section 3.6 is titled Cryptographic Keys Used to Protect Stored Account Data Are Secured. The guidance includes the importance of cryptographic keys since they can decrypt data. Requirement 4, titled Encrypt Transmission of Cardholder Data Across Open, Public Networks, contains two subsections, mainly on encryption. One of the crucial requirements for ensuring cardholder data security is encrypting the data traffic. The process in Requirement 4

[4] HIPAA Security Rule

[5] Technical Safeguards

[6] SOX Section 404 Summary

[7] CSOE

emphasizes the need to use strong cryptography to protect cardholder data during transfer over public networks. By implementing this requirement, organizations can reduce the risk of potential threats.

ADMINISTRATIVE SAFEGUARDS:

Under the Administrative Safeguards, one must follow many security standards for HIPAA. An important one that should be necessary is Security Awareness and Training.[8] The security measures would encompass security reminders, protection against harmful software, monitoring of logins, and management of passwords. The administrative safeguards would include the management process, security responsibilities, information access management, security incident procedures, contingency plans, evaluations, and other relevant arrangements.

PCI DSS Requirement 2, titled Do Not Use Vendor-Supplied Defaults for System Passwords and Other Security Parameters, outlines guidelines for securely configuring and managing all systems. The last subsection includes how to configure wireless environments. Requirement 6, titled Develop and Maintain Secure Systems and Applications, provides information on maintaining secure systems and software and securing system changes. Requirement 7, titled Restrict Access to Cardholder Data by Business Need-To-Know, contains information about restricting access to unauthorized users. It includes information on processes and mechanisms to prevent access to cardholder data.

ACCESS CONTROLS:

The HIPAA access controls include unique user identification, emergency procedures, automatic logoff, encryption, and decryption. These controls enable authorized users to perform activities on computer systems safely. Different types of computer privileges will be assigned to each employee. The CSOE covers knowledge of the development lifecycle controls, which include access controls, integrity controls, and many more. Requirement 6 includes information on maintaining secure systems and software and securing system changes. Requirement 7 provides information on restricting access to unauthorized users, processes, and mechanisms to prevent access to cardholder data. Requirement 8, titled Identify Users and Authenticate Access to System Components, provides much information on recommended ways to identify and authenticate users, such as assigning each person a unique identification number.

AUTHENTICATION:

HIPAA comprises regulations that dictate the management of protected health information. One of the specified Technical Safeguards is the authentication of individuals. These standards force the company to have procedures to verify that the person requesting access to Electronic Protected Health Information (ePHI) is who they claim to be. This requirement ensures that ePHI confidentiality, Integrity, and availability are maintained and protected against unauthorized access. Again, PCI DDS Requirement 8 is the security standard, mainly focusing on authentication. Six sections go over different authentication procedures.

INTEGRITY:

[8] Administrative Safeguards

HIPAA Integrity is a technical safeguard that implies the importance of protecting the ePHI, not allowing any alteration of the ePHI, and not having it destroyed. The Integrity of the ePHI is important since compromising it can lead to many adverse effects since it is a health record used to help and treat patients. SOX: Section 302 states that the CEO and CFO are responsible for the Integrity of financial reports.[9] The SOX Act does not give any remedies for securing financial reports with tampering. PCI DSS Requirement 7 includes information on restricting access to unauthorized users. It provides information on processes and mechanisms to prevent access to cardholder data. It is crucial not to allow unauthorized access to cardholder data since it would violate the Integrity.

AUDIT CONTROLS:

Another critical standard in the technical safeguards section of HIPAA is Audit Controls. There are no mandatory specifications. Audit controls expect systems, applications, or hardware to record and examine activity in networks that contain and use ePHI. According to PCI DSS**,** audits can be a reliable way to identify data tampering or unauthorized access, which falls under Requirement 3 and Requirement 5. Many applications have the benefit of auditing purposes.

NETWORK SECURITY:

Network security in HIPAA is called transmission security in the technical safeguards. The standard requires security measures to protect against unauthorized access to ePHI transmitted over the internet or electronic communications networks. Again, Section 404 of SOX requires financial reports to incorporate an internal control report. The sections do not go in-depth about information security controls, for example, network security, just internal controls. The internal control reports state management responsibilities for establishing internal control structures and procedures for financial reporting. The report includes an evaluation of the internal control structure and financial reporting procedures at the end of the issuer's fiscal year. PCI DSS has Requirement 1, known as Install and Maintain Network Security Controls. This standard outline various subsections related to network security, including implementing, and configuring security controls, limiting network access, authorizing network connections, and the risks associated with connecting to untrusted networks or sources. Implementing these security controls is critical to ensuring the secure transmission of financial data and should be given the utmost importance.

PHYSICAL SECURITY:

The HIPAA Security Rule defines physical safeguards as "physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment from natural and environmental hazards and unauthorized intrusion.".[10] PCI DDS Requirement 9, Restrict Physical Access to Cardholder Data, provides information on processes and mechanisms for defining physical access to cardholder data. It also discusses

[9] SOX Section 302 Summary

[10] Physical Safeguards

physical access controls for facilities and systems. Physical media must be securely stored, accessed, distributed, and destroyed.

PART 4: RECOMMENDATION FOR IMPLEMENTATION

The controls are necessary to meet most compliance requirements, as confidential data may be at risk of theft or alteration. Companies that do not follow compliance requirements face consequences and fines. All security controls can help GSPA stay compliant. These security controls fulfill the three compliances and strengthen GSPA's cybersecurity operations.

ENCRYPTION RECOMMENDATION:

Prioritizing encryption is important since GSPA handles sensitive data and ePHI. Implementing a cloud-based Electronic Health Record (EHR)[11] system could be a better route since it adds another layer of encryption. Hospitals and clinics use EHR or digital record keeping. A reputational EHR system will be the best choice. Encryption of private data is essential since only authorized individuals have the key to decrypt. Encryption policies would encrypt all devices. Certain employees will not be allowed to take any devices or resources home. Also, the use of personal devices should not be allowed at work. All company systems will require multi-factor authentication to comply with the encryption policy. There will be a policy on stolen and lost device procedures, tracking services on all devices, and locking and destroying data on devices that belong to the company if lost or stolen. Reputational encrypted email end-to-end services will be required.

NETWORK SECURITY RECOMMENDATION:

Network security or cybersecurity should come after data encryption since this will secure the company's network. There should be a cybersecurity operations team who can protect the company from cyberattacks. Multiple firewalls are in place in front of the most sensitive data. In case of hardware fails, there should be backup routers, servers, and firewalls. All data stored on computers should be encrypted and password-protected with multi-factor authentication. All systems should have endpoint detection and response (EDR) applications, an antivirus, security information, and event management (SEIM), vulnerability management, user and entity behavior analytics (UEBA), and threat intelligence.

ACCESS CONTROLS RECOMMENDATION:

Implementing Access controls to allow authorized people to access, modify, and transfer sensitive data and allow access to only the required data. Implementing access controls should be the responsibility of an administrator. The administrator can give specific privileges to workers depending on their roles in the company. Each user should have a unique login with requirements for their password. The login should be challenging to identify. Only specific people should be allowed to access ePHI or sensitive data during an emergency. To achieve this, Emergency Access Procedures will ensure that ePHI or sensitive data remains secure while providing access to those who need it during

[11] EHR

an emergency. Access control policies enforce the regular review of all records of information system activities. An information system activity review determines if sensitive data is misused. GSPA governing security policies will be responsible for individuals drafting and executing policies and procedures. Authorization for ePHI or sensitive data is needed to verify and identify the correct privileges to access the sensitive data.

AUTHORIZATION RECOMMENDATION:

Authorization and identification are necessary on all systems requiring access to ePHI or other sensitive data. Enforcement of minimum access to ePHI or sensitive data is essential, ensuring that only authorized personnel receive the necessary data. There must be procedures to supervise workers who work with ePHI and sensitive data and supervision where ePHI or sensitive data is accessed. Authorized employees will verify and provide authorized privileges for other employees to access specific systems containing sensitive data. The supervision will ensure that workers have the correct privileges to access confidential information. Clearance procedures should be in place to determine if a worker meets the requirements to access ePHI or sensitive data. Clearance procedures will verify whether workers can access ePHI or specific sensitive data to do their jobs. For security reasons, it is essential to have procedures to terminate access for employees who no longer work for the company. These procedures should be quick and updated immediately to ensure that access to company systems or physical locations are eliminated. Procedures and regulations for granting access to ePHI or sensitive data should align with the HIPAA Privacy Rule or other compliances. Strict procedures must be in place to authenticate certain people depending on the tasks they wish to perform. Procedures to keep accounts and sensitive data secure include implementing a unique password or PIN and enabling multi-factor authentication. The authentication process should have multiple steps to confirm your identity. When transferring sensitive data to other companies, keeping its functions separate and secure is essential. Other companies must establish and implement measures to secure sensitive data. Data transfer must have a written agreement. Policies, procedures, and assurance on creating and moving sensitive data should exist.

SECURITY INCIDENT RECOMMENDATION:

Security Incident procedures should be implemented for security incidents. Addressing security incidents in the company's environment is required. A GSPA dedicated cyber security team can help take on the role of security incident procedures. The team will monitor, track, identify, defend, document, and adjust accordingly to any internal attacks. Emergency planning is required to recover ePHI or sensitive data if the GSPA experiences any disaster. The plan should cover all disruptions for the company and how to resolve or recover from the disasters. The emergency plan will consist of a plan for backing up data, a plan for recovering from disasters, a plan for operating in emergency mode, procedures for testing and revising the plan, and an analysis of the importance of applications and data.

DATA BACKUP RECOMMENDATION:

HIPAA regulations require that data backup, disaster recovery, and emergency mode operation plans comply. All ePHI or sensitive data must have backups unless it needs to be destroyed. Backing up data must occur every day and every time there is an update or change in the systems. The backup storage location should be in a secure, monitored, and locked space. In an emergency, a disaster recovery plan should have the procedures to recover any ePHI, sensitive data, or any property belonging to the company. An emergency mode operation plan is required and should have procedures to continue business even during an emergency.

AUDIT CONTROL RECOMMENDATION:

Audit controls should be in place; this will allow the tracking of all activities occurring in the company systems. Recording work activity allows for examination and monitoring in case of an emergency. Financial audits are required. Therefore, GSPA must conduct audits to ensure compliance. It is essential to enforce various security standards to prevent disasters like damaging or changing sensitive data. It is crucial not only for HIPAA but also for SOX and PCI DSS. The company must avoid committing fraud or mishandling the sensitive data of many customers.

ADMINISTRATIVE CONTROL RECOMMENDATION:

Administrative controls will require all employees to receive cybersecurity education to help prevent human error, improve security knowledge, and help employees comply with the company's needs. It is essential to provide GSPA security awareness training to all employees. This training will ensure the company complies with all security standards and prevent potential risks. HIPAA requires such security training to help the company comply with SOX and PCI DSS. Regular security training is necessary, primarily when new company systems exist. Weekly reminders on security awareness can help remind people of the importance of cybersecurity. The company will establish administrative processes and procedures to have security rules in place. GSPA will create risk analysis and risk management policies to assist in developing company strategies to protect the confidentiality, integrity, and availability of sensitive data. GSPA risk analysis can identify potential security risks and determine the probability of occurrences and magnitude of risks. Risk management addresses the decisions on how to address security risks and vulnerabilities. Employees need to be aware of the sanctions policy and its implications. This policy ensures that employees comply with the security policies and procedures. Understanding the consequences of failing to comply can help avoid potential risks and maintain a safe and secure work environment.

PHYSICAL SECURITY RECOMMENDATION:

Per the security rule, physical safeguards are policies, procedures, and physical measures implemented to protect GSPS electronic information systems, buildings, and equipment. These safeguards protect the assets from natural and environmental hazards and unauthorized intrusion. By adopting physical safeguards, GSPA can ensure that their sensitive information and physical resources remain secure and protected from potential threats. Physical security must be in place to prevent unauthorized access to information systems, servers, and network hardware. During emergencies, a contingency plan must be in place to ensure the availability and Integrity of ePHI or sensitive data. Having security guards during the data restoration process during an emergency could be beneficial. The contingency plan could have all employees at work during the recovery process. A facility security plan must be in place; it will document the physical access controls. A facility security plan will prevent any unauthorized access to buildings belonging to the GSPA. A plan will be developed for the facility's security, ensuring that only authorized individuals can enter the premises and access sensitive information equipment. Procedures must be in place to govern access and validation processes. The rules that govern workstation usage must be enforced, and employees should be verified to ensure they use workstations according to their respective roles and responsibilities. All workstations that belong to the company must follow all rules and regulations. The systems should automatically log out if a user is not using the system for a particular time, and multi-factor authentication will be in place. The systems with access to ePHI or sensitive data should be in a secure location where authorized access is required. The computer systems will also have security measures to prevent anyone from accessing the ePHI. Policies should be created to remove all hardware, software, and media controls. The policy should also include the movement of devices within locations. Their policy should have remedies for properly handling electronic devices and media, including data destruction or hardware reuse. Disposing of hard drives or computer systems containing ePHI, it must be verified that the hardware is no longer usable. Reusing hard drives or computers that used to contain ePHI or sensitive data should not be allowed. Authorized professionals who destroy hard drives will be responsible for hardware and media controls. Reuse of computers will be allowed, but procedures to make sure data is unrecoverable for subsequent use are required. If equipment is not necessary for reuse, then donating or reselling the equipment can be allowed. Documentation of all equipment should be implemented, and users responsible for the equipment for job duties should be documented. Registered users should be noted for all equipment, hardware, or media belonging to the company.