HAP2 TASK 1: CYBERSECURITY MANAGEMENT I – STRATEGIC

Damian J. Yates

WGU

Student# 000478522

# Synopsis

In response to the discussion during our recent board meeting, Psinuvia, Inc. hired Autojor Security Consultants to conduct a comprehensive security audit of our existing cyber security posture and business processes. Last week Autojor provided a high-level report based on a comprehensive assessment of our security situation. This document will act as an acknowledgement and proposed response to Autojor’s Security assessment and high-level report.

# Overview

Autojor Security Consultants (ASC) conducted both a passive and active assessment of Psinuvia, Inc network, operations, and business policies. With the use of cyber security specialists and numerous tools, ASC actively probed the exterior of our security defenses seeking entry points and data leakage. At the same time ASC specialists were operating within our security perimeter seeking vulnerabilities within the organization, as well as its technology infrastructure, operational and business policies, and procedures. ASC will provide our technology team with a comprehensive detailed report with recommended actions needed to remediate the discovered deficiencies with the existing security posture. To quote ASC, “…there were a number of issues surrounding Psinuvia, Inc’s implementation of a strong cybersecurity posture as well as the subsequent projects and programs to enforce that security.” Below are some of the points of concern addressed in the high-level report:

* Insufficient structured cybersecurity program.
* Devices produced by Psinuvia, Inc. have no visible data security for the information they collect, store, and transmit.
* Failure to adhere to federal, state, local and international laws concerning PII, medical, and credit card data.
* The existing business continuity plan is rudimentary and lacks sufficient mitigation of potential business impacting events at any of the organization’s sites.
* Cybersecurity risk management policies and procedures do not address all logical and physical threats to organizational assets.
* Functional roles and responsibilities have not been properly identified and documented.

This document will acknowledge these deficiencies, explain their importance of remediation of the deficiencies to the success and security of Psinuvia, Inc., and provide potential solutions to allow for proper adherence to cyber security best practices.

# **Key Area of Deficiency**

## **Deficient Cybersecurity Program**

Below are a few key areas of concern detected in the assessment. Numerous physical and logical vulnerabilities, failure in or lack of policy and procedures, as well as several areas for improvement have been identified. Each item gives a summary of the deficiency as well as its impact to the company and its overall importance in establishing a sound cybersecurity program.

### **Assessment**

Currently, cybersecurity at Psinuvia, Inc. is driven solely by the CTO with no clearly defined standards, policies, or procedures in place.

### **Importance**

Adhering to one or multiple industry Cybersecurity Frameworks and Standards will aid Psinuvia, Inc. in developing, implementing, and maintaining a viable cybersecurity program. Having a robust Cybersecurity program, in turn, reduces the organizations’ asset vulnerability to unauthorized access, theft and damage. This lack of a defined Cyber Security program prevents Psinuvia, Inc. from gauging the effectiveness of its security standards within the company, conduct proper security self-assessments, and provide its customers, clients, partners, and regulators with the assurance that the information entrusted to the company is secured and safe. In addition, the lack of clearly defined policies, procedures, and standards addressing Psinuvia, Inc security posture prevents the organization from detecting security deficiencies within Psinuvia, Inc network both on premise and in the cloud. This leaves Psinuvia, vulnerable to external and internal threat actors and prevents proper detection, isolation, remediation, and reporting of security events.

### **Physical Organizational Vulnerabilities**

Without clearly defined regulations, standards, policies, and procedures, Psinuvia, Inc have a high susceptible to the following:

* Tailgating
  + This occurs when unauthorized persons gain access to sensitive locations. Currently, the lack of a security training program and ingress/egress policies increase the likelihood of employee’s allowing and not reporting a physical threat to the organization.
* Unaccounted Persons
  + Visitors to Psinuvia, inc. occur frequently and for different reasons. Currently, the organization has no policy and procedure on managing non-employee persons nor is there any accountability the visitor or the sponsoring individual. This inadequacy allows those unaccounted persons free unsupervised access to all areas of Psinuvia.

### **Physical Organizational Threats**

The above vulnerabilities leave Psinuvia, Inc. open to attack by threat actors, both internally and externally. Some of these threats include:

* Malicious employees
  + Lack of accountability, detection controls, and non-repudiation makes identifying malicious acts by internal employees, vendors, contractors, or visitors.
* Natural Disasters
  + Lack of proper threat assessment and planning leaves Psinuvia unprepared for natural disasters, both seasonal and unexpected which increases the likelihood that recovery will not be possible.

### **Logical Software Vulnerabilities**

Failure to adhere to government and industry standards in securing client data, at rest and transit, makes Psinuvia, Inc. vulnerable to massive financial penalties and/or criminal liability by state and federal entities. In addition to the loss of capital, a loss of confidence in Psinuvia, its products and services is also a high possibility caused by potential bad press, public scrutiny of displeased clients and/or partners.

Implementation of the Software Development Life Cycle would greatly mitigate the following vulnerabilities found in Psinuvia’s existing process and procedures:

* Violation of least privilege
  + Ensuring that applications, users, and processes have only the privileges and access needed to perform their tasks.
* Data input validation controls
  + Lack of data validation at the database server allows for malformed input as well as the malicious code.

### **Logical Software Threats**

The above logical vulnerabilities in Psinuvia’s development process for its products make the following threats highly probable:

* Information Disclosure
  + Poor software development practices can lead to the loss of confidentiality of client and company data by means of eavesdropping or unintended access to privileged information.
* Denial of Service
  + Failure to detect flaws or properly secure application code and lead to a malicious attempt to compromise the availability of the application or data.

# **Cyber Security Industry Standards**

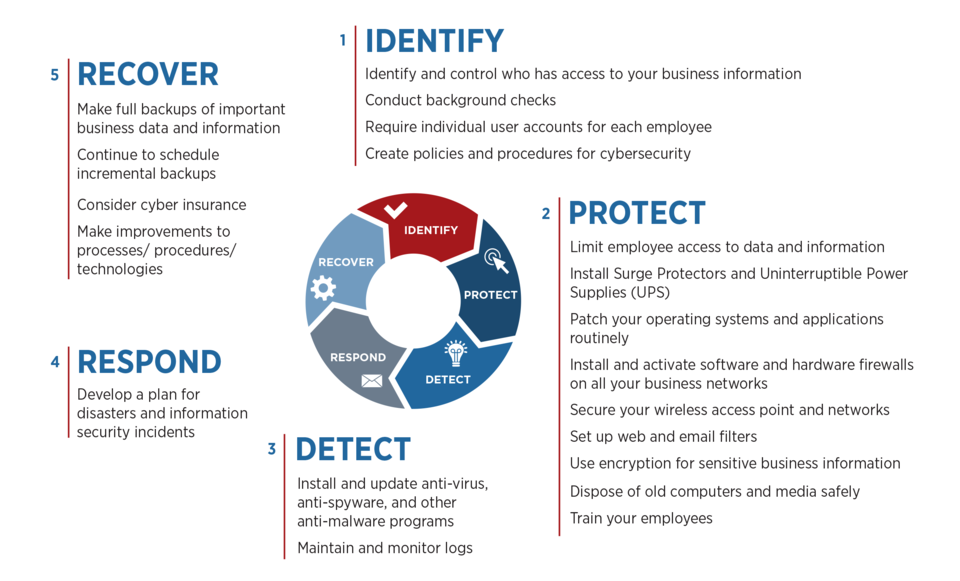
The following provides several industry standards as well as a review of a few Cybersecurity Frameworks that Psinuvia, Inc. could leverage to remediate the discovered deficiencies. These industry standards and frameworks are crucial to the development of policies, procedures, and standards meant to secure Psinuvia, Inc and its interests.

## **The NIST Cybersecurity Framework**

The National Institute of Standards and Technology (NIST), an arm of the Department of Commerce, was tasked by the White House, via the issuance of Executive Order 13636, requiring the agency to develop a foundation that would foster “the sharing of cybersecurity threat information, and on building a set of current and successful approaches, a framework, for reducing risks to critical infrastructure.” (History and Creation of the Framework, 2019). This framework established a common language for understanding, managing, and expressing cybersecurity risks for stakeholders of any organization or agency. The Core of the NIST Cybersecurity framework consists of 5 functions that are concurrently and continuously performed to form a culture within an entity that can address the dynamics of cybersecurity risk. These functions are as follows:

* **Identify** - Establish an organizational understanding of the business, the physical and logical resources used to support the critical functions, and the related cybersecurity risks to the organization.
* **Protect** – The physical and logical safeguards that are created and established that ensures ongoing operations.
* **Detect** – The development and implementation of procedures used to identify cybersecurity incidents.
* **Respond** – Policy, procedures, and guidelines used to shape the response given to a detected cyber security event.
* **Recover** – The procedures used to ensure business resiliency and the restoration of any services or functions that were affected by a cybersecurity event.

Image 1 - NIST Process



(MEP Centers Aid Manufacturers on Cybersecurity, 2018)

## **Mitigation of key areas of concern**

### **Lack of a Cybersecurity framework**

At the heart of the deficiencies found is Psinuvia, Inc failure to develop, implement and maintain a cybersecurity initiative based on industry standards for securing organizational assets regarding policies for acceptable use, mobile devices, passwords, and personally identifiable information (PII). One such framework is the NIST Cybersecurity framework. This well-known framework is a combination of standards, guidelines, and best practices that “provides a common taxonomy and mechanism for organizations to:

1. Describe their current cybersecurity posture.
2. Describe their target state for cybersecurity.
3. Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process.
4. Assess progress toward the target state.
5. Communicate among internal and external stakeholders about cybersecurity risk.”

(National Institute of Standards and Technology, 2018)

The following are a few of the policies that should be developed with the standards, guidelines and best practices found in the NIST Cybersecurity Framework as a roadmap:

#### Acceptable Use Policy

Establishment and enforcement of an Acceptable Use Policy (AUP) will provide employees guidance on what devices and software are allowed on the organizations network and issued devices. This policy establishes a “duty of care” with the user of the company device and reduce misuse of said asset. Even 15 years ago VA Department of education states that AUP’s “focuses on responsible use of computer networks, including the Internet, and access and transmitting of information” (Acceptable Use Policies: A Handbook, 2007) by employees, to/from the company.

#### Bring Your Own Device (BYOD) Policy

With the workforce becoming more mobile, Laptops, Cell Phones, Tablets and IOT are major areas of concern. Psinuvia, Inc. in addition to securing physical access to its network also needs to address the mobile devices. An “Effective Unified Endpoint Management (UEM) maintains user experience for employees regardless of device ownership, while enforcing BYOD policy” (Chickowski, 2020). Implementation of a UEM, such as Microsoft Intune, will allow Psinuvia, Inc. to maintain control over its data and devices as well as how the data is used and stored on the devices.

#### Data Classification Policy

Due to the sensitivity of the data transmitted and stored within and out of Psinuvia, Inc., having a policy outlining when, where, and how data classification is handled within the organization is paramount. Data Classification Policy defines the potential risks to the data that is created, transmitted, and stored by the organization and places a specific classification on each data item based on its value, level of sensitivity, and importance to the organization. The policy will also define the security levels and the restrictions placed on the data at each classification security level. Implementation of this policy will ensure adherence to standards and regulatory requirements on securing personal identifying information (PII) and reduce the liability surface of the organization.

### **Identity and Access Management (IAM)**

This framework is a collection of policies and tools used to manage and control access to organizational resources. It achieves this with the use and monitoring of object permissions, credentials (passwords, certificates, user accounts, etc.) and periodic reviews of those credentials and permissions to ensure that the necessary changes are made to ensure the security of the object. Implementation and enforcement of the policies derived from IAM Framework will ensure that users have the appropriate level of access to the specific objects they need to always fulfill their roles and responsibilities.

# Department Roles and Responsibilities

Having a knowledge of the security roles involved with the framework will aid in communication between teams and members as well as allow for the implementation and enforcement of all security policies within the framework. The proceeding table lists a few of the key roles that should be clearly defined and staffed.

|  |  |
| --- | --- |
| Compliance and Risk Department | Security Department |
| Conduct internal audits and reviews to ensure compliance. | Identify deficiencies in existing processes and develop mitigation steps to remediate the deficiency. |
| Ensure organizational compliance with government regulations. | Enforce security guidelines, policies, and procedures |
| Facilitates internal/external audits to ensure policies are enforced and current. | Monitor and address alerts generated by vulnerability and security scanning and intrusion detection systems |
| Perform risk assessments | Maintain systems hosting security and compliance services |
| Document organizational processes and workflows | Develop annual admin security training |
| Evaluate analysis of access to all systems annually | Confirm efforts to remediate vulnerabilities found in systems. |

Table 1 – Role & Responsibilities

# PCI-DSS policy recommendations

Psinuvia, currently accepts payments from its clientele using purchase orders, checks, and credit cards. Because of the processing of credit card data, Psinuvia IT Security professionals are required to ensure proper adoption, implementation, and maintenance of data security measures required by the Payment Industry’s Data Security Standards (PCI-DSS). PCI DSS provides a baseline of technical and operational requirements designed to protect account data (PCI Security Standards Council, LLC, 2022). The PCI-DSS standard has 12 security requirements that are meant to protect sensitive data, mitigate potential risks and adhere to local, state, and federal regulations.

Image 2 - PCI DSS Requirements

Graphical user interface, text, application

Description automatically generated

(PCI Security Standards Council, LLC, 2022)

Collaboration between the IT security professionals and the Compliance Department of Psinuvia will be needed to ensure these PCI standards are met and always maintained across the organization. The following are key areas of importance:

### **Build and Maintaining a Secured Network Infrastructure**

The IT Security Department will be responsible for evaluating the current operational environment including both physical and logical network and systems, policies, procedures, and existing standards. With this information in hand, network security controls will be designed and implemented to secure all systems and their associated configurations within the infrastructure. The compliance department will be tasked with reviewing adherence of the established policies and procedures as well as documenting and retaining compliance status throughout the lifetime of the network security controls.

### **Protect Sensitive Card Holder Data**

Protection of cardholder sensitive data will be the responsibility of the IT Security Department. This data must remain confidential, its integrity maintained, and secured from exfiltration while in Psinuvia care at rest, process, and transit.

Image 3 - Account Data Defined

Table

Description automatically generated

(PCI Security Standards Council, LLC, 2022)

IT Security can accomplish this by utilizing methods such as encryption, truncation, hashing, salting, and masking the sensitive data. Additionally, ensuring that the data is only stored, in memory or on a persistent storage medium, when necessary and properly protected when at rest. Securing this data while in transit in or outside of Psinuvia’s network is also required at every point along the journey of the data.

### **Vulnerability Management Program Established**

IT Security will be tasked with implementing and maintaining a robust vulnerability management and logging system to protect all Psinuvia network, data, and systems. This program should provide protection from and detection of malicious software, code, and activities within and outside Psinuvia’s Infrastructure. IT Security Department will also remediate and document all vulnerabilities identified by the vulnerability program. The Compliance Department will be responsible for review of policies and procedures supporting the Vulnerability Management Program as well as documenting compliance and violations of said policies and procedures. This program should include a comprehensive list of accepted risks along with documented reasoning for their acceptance.

### **Develop Strong Logical and Physical Access Controls**

IT Security will be mandated to establish Mandatory and Discretionary access controls for all data, systems, people, and network traffic while at rest or in transit. Implementation of “Need to know” and “Least Privilege” used in conjunction with compartmentalization will provide Psinuvia a high degree of control over the access to PCI-DSS restricted data. Identity management will be essential with ensuring only authorized individuals are allowed access. Use of MFA, proper account lifecycle management, and logging will be key tools of the IT Security Department. These concepts will be in use at the physical and logical areas of system, data, and network access. The IT Security Department will also be required to ensure that logging of all privileged access is not repudiable. All logged access should be retained in accordance with PCI-DSS, local, state, and federal requirements.

### **Periodically Test and Monitor all Network Access Controls**

IT Security Department will develop processes and procedures to monitor all established network access controls used to secure data and property. The data collected by these monitors will need to be securely stored and secured to always maintain non-repudiation and availability of the data. The Compliance Department will use the data collected by these processes and procedures to periodically review these logs for anomalies and access violations. Reports will be generated from the reviews which can be used to add, remove, or change existing policies and procedures, develop improvements & address shortcomings identified in the accumulated data.

# Compliance Requirements of the GDPR

Because Psinuvia does business with customers worldwide, the Compliance Department must ensure that compliance with GDPR included with the development of the policies and procedures governing the Network Access Controls of Psinuvia. GDPR protects the data of the EU citizens regardless of where the data is being processed. (THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION, 2016, pp. 32-33). The following are a few of the GDPR requirements surrounding “Lawful basis and transparency, Data Security, Accountability & Governance, and Privacy Rights of EU Citizens (European Union, 2022) that should be included in Psinuvia, Inc security goals.

### **Lawful basis and transparency**

GDPR requires organizations wishing to process its citizens data to have a “need to process” or handle said data. Psinuvia Compliance Department will need to ensure that the organization can justify its need to process the data by meeting at least one of the conditions in Article 6 of the GDPR. (GDPR, 2022) This justification should state the purposes for which processing the data is used, an indication of the type of data to be processed, how the data will be protected, how and when the data will be disposed of, and lastly, who will have access to the data. GDPR Article 12 (GDPR, 2022) requires that the Compliance Department ensures that Psinuvia discloses to each of its European customers the same information used to justify processing of the data in a clear and concise manner at the time the citizens information is collected.

### **Data Security**

“Article 5” (GDPR, 2022) of the GDPR outlines the protections needed on the data being processed. IT Security Department will need to work with the Compliance Department to ensure that the appropriate measures are taken to secure, dispose of, and reduce the amount of data used to be processed. These policies and procedures should reside in Psinuvia’s Security Policy that is required acknowledgement by all employees. The IT security Department, at the direction of the Compliance Department, should conduct “data protection impact assessments” (GDPR, 2022) periodically to ensure that Psinuvia has minimized risks to GDPR protected data. Both the IT Security and Compliance Departments must understand the importance of reporting any suspected data breach of GDPR data to the data subjects of the affected data.

# HIPAA Compliance

Due to the products that Psinuvia manufactures and the protected health information (PHI) that is collected, stored, and transmitted by them, the Compliance Department in coordination with the IT Security Department must incorporate, document, and maintain security controls to meet the requirements set forth int the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Currently, Psinuvia has no documented policy and procedures to address this federal regulation. The four areas of focus for compliance with HIPAA are Privacy, Security, Breach Notification, and Compliance & Enforcement (Office for Civil Rights (OCR), 2022).

### **Privacy**

HIPAA Privacy Rule specifies what information and persons are protected under the rule as well as how the PHI data can be used or disclosed. Those who are included within the scope of the rule are Health Care Providers, Clearinghouses, some Plans and any Business that handles or transmits PHI. PHI is defined by the Privacy Rule as “any identifying health information held or transmitted by a covered entity” (Office for Civil Rights (OCR), 2022). The Privacy rule also specifies permitted, authorized uses and disclosures of PHI. Psinuvia’s Compliance Department will need to ensure that security policies and standards are written to address the requirements of the Privacy Rule and the IT Security Department will be required to implement controls, policies and procedures to meet the standards set by the compliance department.

### **Security**

The HIPAA Security rule was established to provide protection to a person’s electronic PHI that is generated or maintained by any entity covered by HIPAA. The security rule mandates that administrative, physical, and technical measures are implemented to enforce confidentiality, integrity, and security of PHI. The compliance department should ensure that during its risk assessment of Psinuvia, it includes the use of tools like the “HHS Security Risk Assessment Tool” (Office of the National Coordinator for Health Information Technology (ONC), 2022) and the “NIST HIPAA Security Rule ToolKit” (NIST, 2022). The IT Security Department should implement, adjust, and remediate network and physical access controls based on the results of the risk assessments.

### **Breach Notification**

The HIPAA Breach Notification Rule requires all HIPAA covered entities to provide prompt and detailed notification to the affected data subjects, the Secretary of HHS, and if warranted local, and regional media outlets (Office for Civil Rights (OCR), 2022). This notification should include a brief description of the breach, type of information that was disseminated, steps that the data subject can do to mitigate the damage to themselves, and an explanation of what the covered entity is doing to investigate the breach, mitigate the damage caused by and prevent future occurrences of the breach. The Compliance Department will include an Incident Response procedure in the security policy, which will be used to provide guidance on how to report a breach internally as well govern how and when the Compliance Department reports a breach.

### **Compliance and Enforcement**

The Office of Civil Rights (OCR) in HHS is responsible for enforcing and imposing civil money penalties for each violation of HIPAA. The OCR also has the authority to submit complaints deemed criminal to the Department of Justice for federal prosecution. The Compliance Department should review 45 CFR Part 160 –General Administrative Requirements which outlines the penalties that are incurred for each reported incident. As of the writing of this report, fines are as follows:

|  |  |  |  |
| --- | --- | --- | --- |
| **Neglect Level** | **Min. Fine per violation** | **Max Fine per violation** | **Annual Cap** |
| Low (160.404.b.2.i) | $100 | $50,000 | $1,500,000 |
| Medium (160.404.b.2.ii) | $1,000 | $50,000 | $1,500,000 |
| Willful Neglect (160.404.b.2.iii) | $10,000 | $50,000 | $1,500,000 |
| Fail to comply (160.404.b.2.iv) | $50,000 | None | $1,500,000 |

(National Archives, 2022)

Table 2-HIPAA Civil Penalties

# Business Continuity Plan (BCP)

Psinuvia, Inc currently has a rudimentary BCP which covers only the Texas facility and lacks controls and procedures to address possible natural disasters that may interrupt business operations. The compliance and IT Security Departments will need to perform a thorough business impact assessment (BIA) to identify all current potential operational impacting natural disasters. This BIA should include every remote site that is integral to the proper operations of the organization. As each location is subject to its own unique climates and dangers, it is imperative that each location is assessed individually. Once the assessment is completed, policies, procedures, and standards need to be established to ensure that business continuity can be executed in a timely and orderly manner. A determination of how business continuity will be achieved will be based on the results of the BIA. At a minimum a suitable location owned by Psinuvia with the least susceptibility to disaster should be evaluated as a disaster recovery site (DRS). A review of Autojor’s Independent Security Report should be conducted to ensure that each of the defined deficiencies have been addressed.

# References

*Acceptable Use Policies: A Handbook*. (2007, 3 31). Retrieved from Virginia Department of Education: https://web.archive.org/web/20070331155213/http://www.pen.k12.va.us/VDOE/Technology/AUP/home.shtml

Chickowski, E. (2020, 9 24). *BYOD security explained: what is a BYOD policy?* Retrieved from AT&T Business: https://cybersecurity.att.com/blogs/security-essentials/bring-your-own-device-security-explained

European Union. (2022, 08 13). *GDPR Compliance Checklist*. Retrieved from gdpr.eu: https://gdpr.eu/checklist/

GDPR. (2022, 08 16). *Art. 12 - Transparent information, communication and modalities for the exercise of the rights of the data subject*. Retrieved from GDPR: https://gdpr.eu/article-12-how-controllers-should-provide-personal-data-to-the-subject/

GDPR. (2022, 08 17). *Art. 35 GDPR - Data protection impact assessment*. Retrieved from GDPR: https://gdpr.eu/article-35-impact-assessment/

GDPR. (2022, 08 16). *Art. 5 GDPR - Principles relating to processing of personal data*. Retrieved from GDPR: https://gdpr.eu/article-5-how-to-process-personal-data/

GDPR. (2022, 08 15). *Art. 6 GDPR - Laefulness of processing*. Retrieved from GDPR.eu: https://gdpr.eu/article-6-how-to-process-personal-data-legally/

*History and Creation of the Framework*. (2019, 11 21). Retrieved from NIST: https://www.nist.gov/cyberframework/online-learning/history-and-creation-framework

*MEP Centers Aid Manufacturers on Cybersecurity*. (2018, 5 3). Retrieved from NIST: https://www.nist.gov/news-events/news/2018/05/mep-centers-aid-manufacturers-cybersecurity

National Archives. (2022, 08 23). *45 CFR Part 160*. Retrieved from Code of Federal Regulations: https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-160

National Institute of Standards and Technology. (2018, 4 16). Framework for Improving Critical Infrastructure Cybersecurity.

NIST. (2022, 08 23). *Security Content Automation Protocol*. Retrieved from CSRC: https://csrc.nist.gov/projects/security-content-automation-protocol/hipaa

Office for Civil Rights (OCR). (2022, 08 24). *Breach Notification Rule*. Retrieved from HHS.gov: https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

Office for Civil Rights (OCR). (2022, 08 20). *HIPAA for Professionals*. Retrieved from HHS.gov: https://www.hhs.gov/hipaa/for-professionals/index.html

Office for Civil Rights (OCR). (2022, 08 22). *Summary of the HIPAA Privacy Rule*. Retrieved from HHS.gov: https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

Office of the National Coordinator for Health Information Technology (ONC). (2022, 08 23). *Security Risk Assessment Tool*. Retrieved from HealthIT.gov: https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool

PCI Security Standards Council, LLC. (2022, 03). Payment Card Industry Data Security Standard: Requirements and Testing Procedures, v4.0.

Rittenberg, J., & Bottorff, C. (2022, 2 21). *Forbes Advisor*. Retrieved from https://www.forbes.com/advisor/business/what-is-asset-tracking/

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION. (2016). REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL . *Offical Journal of the European Union*.