Stetson Mobley

ISAT B409

Risk Management Project

Part 1: System Description

The system I will be covering in the Healthcare industry is the Medicaid enrollment system. The Medicaid system is a federal government-funded health coverage program eligible for those of low income. The enrollment system takes the data of the individual via documents or online forms, determines if they are qualified for the coverage, and puts them into the insurance program if they are.

First, the system needs to take the necessary information of the individual. Then, it reads the data and determines if the income parameters are met. If they are not met, then the system will store their information, and the mailing system will send a denial letter to the individual’s address. If the individual is eligible for Medicaid, then the system will store their information, mark them as eligible, and tell the mailing system to send an approval letter to the individual’s address. The system will also tell the Medicaid card system to create a card with the individual’s name, the individual’s date of birth, and an ID number.

The enrollment system will handle Personally Identifiable Information like the individual’s full name, address, birthdate, social security number, telephone number, and email address. The insurance information itself and the insurance identification number is considered Protected Health Information. When used in the context of informing the individual of their eligibility, the person’s name, address, email, birthdate, and other included information become PHI. The system will also need financial information in the form of the user’s income, employer information, tax statements, and W-2 forms to determine eligibility.

The system is important for signing users up for the program. The enrollment system needs to be separated from other information systems because it will handle a lot of ineligible people, as well as data that isn’t required for maintaining the program. Without an enrollment system, data could more easily be lost during the process.

Part 2: Network/ Data Flow Diagram

A computer icons and symbols

Description automatically generated with medium confidence

Ports and Protocols

|  |  |
| --- | --- |
| HTTPS (Hyper Text Transfer Protocol Secure) 443 | Used for secure communication over networks between the browser and web servers. |
| SMTPS (Simple Mail Transfer Protocol Secure) 587 | Used to send encrypted email transmission. For the system, this will be used to send acceptance or denial emails. |
| SFTP (Secure/SSH File Transfer Protocol) 22 | Securely transfer files using SSH key authentication. For the system, could be used to transfer data between database server and enrollment review. |

Information Types

|  |  |  |  |
| --- | --- | --- | --- |
| **Information Type** | **Confidentiality** | **Integrity** | **Availability** |
| D.14.1 Access to Care | Low | Moderate | Low |
| D.14.3 Health Care Administration | Low | Moderate | Low |
| D.14.4 Health Care Delivery Services | Low | High | Low |
| C.3.5.5 Information Security | Low | Moderate | Low |
| **Overall CIA** | Low | High | Low |
| **Overall** | High |  |  |

D.14.1 Access to Care – This type focuses on the access to the appropriate care, which encompasses determining eligibility, which is what my system does.

D.14.3 Health Care Administration – This information type assures that federal health care resources are expended effectively to ensure quality, safety, and efficiency. My system ensures that only those who qualify get access to the healthcare, which ensures quality and efficiency.

D.14.4 Health Care Delivery Services – Medicaid is a healthcare service, and this information type covers providing the delivery of health care to its beneficiaries.

C.3.5.5 Information Security – involves securing Federal data and systems through security policies, procedures, and controls. My system deals with sensitive PHI, and since Medicaid is a federal program, this data is a part of this information type.

Part 3: Security Controls

**1) SC-5 - DENIAL-OF-SERVICE PROTECTION Control:**

1. Low, Moderate, High
2. *[Selection: Protect against; Limit]* the effects of the following types of denial-of-service events: *[Assignment: organization-defined types of denial-of-service events]*; and

Employ the following controls to achieve the denial-of-service objective: *[Assignment: organization-defined controls by type of denial-of-service event].*

1. My Medicaid enrollment system protects against denial-of-service events such as flood attacks, distributed denial-of-service attacks, and ICMP flood attacks; and employs detection software and well-configured firewalls to detect and stop denial-of-service events.

**2) SI-4(4) – SYSTEM MONITORING – INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC Control:**

1. Moderate, High

2. Determine criteria for unusual or unauthorized activities or conditions for inbound

and outbound communications traffic;

Monitor inbound and outbound communications traffic *[Assignment: organization defined frequency]* for *[Assignment: organization-defined unusual or unauthorized activities or conditions].*

3. My system will monitor inbound and outbound traffic every ten system minutes for unusual or unauthorized activities or conditions, including: malicious code, unusual traffic to external systems, and unauthorized usage of credentials or information.

**3) SC-7(21) - ISOLATION OF SYSTEM COMPONENTS Control:**

1. High

2. Employ boundary protection mechanisms to isolate *[Assignment: organization-defined system components]* supporting *[Assignment: organization-defined missions and/or business functions].*

3. My system will employ boundary protection mechanisms to isolate our servers and card systems that support the storage of enrollment in the program and creation of cards for those approved in the system.

**4) SC-8 - TRANSMISSION CONFIDENTIALITY AND INTEGRITY Control:**

1. Moderate, High

2. Protect the *[Assignment (one or more): confidentiality, integrity]* of transmitted information.

3. Protect the confidentiality and integrity of transmitted information.

**5) SC-8(1) - CRYPTOGRAPHIC PROTECTION Control:**

1. Moderate, High

2. Implement cryptographic mechanisms to *[Assignment (one or more): prevent unauthorized disclosure of information, detect changes to information]* during transmission.

3. Implement cryptographic mechanisms to prevent unauthorized disclosure of information during transmission from external sources into our network.

**6) AC-6(2) - NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS Control:**

1. Moderate, High

2. Require that users of system accounts (or roles) with access to [Assignment: organization-defined security functions or security-relevant information] use non-privileged accounts or roles, when accessing nonsecurity functions.

3. The system will require that users of system accounts with access to firewalls and intrusion prevention systems use non-privileged accounts or roles when accessing non-security functions.

**7) AC-11 – DEVICE LOCK Control:**

1. Moderate, High

2. Prevent further access to the system by *[Assignment (one or more): initiating a device lock after [Assignment: organization-defined time period] of inactivity, requiring the user to initiate a device lock before leaving the system unattended]*; and

Retain the device lock until the user reestablishes access using established identification and authentication procedures.

3.Prevent further access to the system by initiating a device lock after five minutes of inactivity, requiring the user to initiate a device lock before leaving the system unattended; and retain the device lock until the user re-establishes access using established authentication procedures.

**8) SI-3 – MALICIOUS CODE PROTECTION Control:**

1. Low, Moderate, High

2. Implement *[Assignment (one or more): signature based, non-signature based]* malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code;

Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures;

Configure malicious code protection mechanisms to:

Perform periodic scans of the system *[Assignment: organization-defined frequency]* and real-time scans of files from external sources at *[Assignment (one or more): endpoint, network entry and exit points]* as the files are downloaded, opened, or executed in accordance with organizational policy; and

*[Assignment (one or more): block malicious code, quarantine malicious code, take [Assignment: organization-defined action] ]*; and send alert to *[Assignment: organization-defined personnel or roles]* in response to malicious code detection; and

Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.

3.My system will implement both signature and non-signature based malicious code protection mechanisms at system entry and exit points to detect and eliminate malicious code; automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures; configure code protection mechanisms to periodically scan the system every hour and real-time scans of files from external sources at network entry and at endpoints as the files are downloaded and opened in accordance with the organization's policy; and quarantine malicious code for review; and send alerts to IT admins and cybersecurity personnel in response to the detection; and address the receipt of false positives during malicious code detection and eradication and the resulting impact on the availability of the system.

**9) SI-4(10) - VISIBILITY OF ENCRYPTED COMMUNICATIONS Control:**

1. High

2. Make provisions so that *[Assignment: organization-defined encrypted communications traffic]* is visible to *[Assignment: organization-defined system monitoring tools and mechanisms]*.

3. Make provisions so that encrypted incoming traffic from customers enrolling for Medicaid on the web is visible to the intrusion prevention system and firewalls.

**10) SI-10: INFORMATION INPUT VALIDATION Control:**

1. Moderate, High

2. Check the validity of the following information inputs: *[Assignment: organization-defined information inputs to the system].*

3. Check the validity of the following information inputs: Make sure the birthdate entered only contains valid numbers and that the months and days are not out of range; make sure the social security and telephone numbers are only numerical, and make sure attached forms like tax statements and W-2 forms are in pdf, png, or jpg formats.