4.1.4 Privacy and security

ii. For the password reset, only the System

Administrator is authorized to reset the

user account password. The user is

necessary to provide the requirements:

1. Letter (Signed by the Supervisor

or Higher to the Escalation)

2. Employee ID

3. Account ID

C. User Access to Business Functions

The user access is based on the user account

role together with its specific user’s view and

capabilities.

D. Audit Logs

I. The PrecisionCare Hospital Website maintains

the Login Logs that include the following:

1. Account ID

2. Ip Address

3. Date and time

4. Records of system access

attempts (success/failed)

II. The PrecisionCare Hospital Website maintains

the Action Logs that include the following:

1. Account ID

2. Ip Address

3. Date and Time

4. Records of system action

(transaction log and maintenance

log)

E. Data Checking and Validations

In this section will elaborate what checking and

validation implemented in the system such as data

fields are validated upon input to detect the following

errors by the users.

I. Login Interface

i. The Login Interface is supported by a

Double-Checking Feature that will

prevent the vulnerabilities of Account

IDs and Passwords.

ii. The first layer of checking will identify if

the user input a right format or

parameter in the input fields or if the

attacker changes a certain line of code

in browser terminals.

iii. The second layer of checking is focused

on the backend side, the system will

process the credentials inputted by the

user to verify if its match on the system's

database.

II. Required and Non-Required Input Fields

i. The best practices are implemented for

input validation included:

1. Define length of the input data,

minimum and maximum.

2. Notify the user if the input field

has missing or incomplete data.

3. Implement a restriction based on

the requirements that are allowed

in the input type.

F. Service or Connection IDs

The credential gathered from the authentication

of the PrecisionCare Hospital website is encrypted

and stored in the database. The privilege access level

given by the PrecisionCare Hospital website depends

on credentials provided by the user.

G. Website Authentication

The PrecisionCare Hospital website is

activated with an SSL certificate that declares the

PrecisionCare Hospital website is a safe and

legitimate website for the users.

H. Encryption

This category of Privacy and Security

implements standard practices when it comes to

encrypting. This will fortify the digital data of

PrecisionCare Hospital by using one or more

techniques to decrypt the information including the

third-party service implemented in the system.

226

I. The Encryption used by PrecisionCare Hospital

is Secure Shell (SSH) and Socket Layer (SSL)

for the encryption process. The SSH is an

encrypted key for connection to the server. The

SSL Encrypts the transaction and

communication within the PrecisionCare

Hospital website to the server.

II. The SSL transaction within the PrecisionCare

Hospital website is encrypted between the

website, Cloudflare, and the server. Before the

data is transferred from the PrecisionCare

Hospital website to the Server, the

PrecisionCare Hospital Website should

connect to Cloudflare first before connecting to

the server.

III. When communicating at the shell, All the data

in SSH sessions between the client and the

server is encrypted.

IV. Exchanging data between the PrecisionCare

Hospital to the Cloudflare and server is

encrypted, the data can be sent to the internet

having a lesser chance of being intercepted

during the transaction.