|  |  |  |
| --- | --- | --- |
| S.No. | Old comment | New comment |
| 4. | Only Stryker’s service engineer is authorized to manage user account | Only Stryker’s service engineer has an user account and been provided with the authorization to access |
| 4. | HDO/hospital staff is only authorized to manage the user account on the Nurse Station web application | HDO/hospital staff has an user account and been provided with the authorization to access |
| 4. | Stryker will provide the personal authentication credentials for the same. | Stryker provides the unique authentication credentials for the same. |
| 5. | Only Stryker’s service engineer is authorized to access the SmartMedic solutions component whenever needed, at the time of maintenance | Only Stryker’s service engineer has authorization to access the Smart Medic solutions components (device, tablet) whenever needed, at the time of maintenance |
| 5. | Stryker will provide the personnel with authentication credentials for the same. | Stryker provides the personnel with authentication credentials for the same. |
| 6. | Only Stryker’s service engineer is authorized to access the SmartMedic solutions component device whenever needed, at the time of maintenance. | Only Stryker’s service engineer has authorization to access the Smart Medic solutions component (device) whenever needed, at the time of maintenance. |
| 6. | HDO is not allowed to access and manage the device and tablet component | The access and management of the device and tablet is not provided for HDO. |
| 7. | Only Stryker’s service engineer is authorized to perform testing and maintenance of the SmartMedic Solution’s component device, whenever needed, at the time of incident response. | Only Stryker’s service engineer is authorized to perform verification & validation of the Smart Medic solutions component (device) whenever needed, at the time of incident reported. |
| 19. | The customer is not allowed to access this component*.* | Customer don’t have to consider this. |
| 22. | The customer is not allowed to access SmartMedic Device and Tablet component*.* | Access of the SmartMedic device and tablet is not provided for customer (HDO). |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**25. Health data storage**

1. What are the health data items
2. Patient details are anonymized and mapped to patient id and that can be retrieved the patient details.

**20. Security Program Integration**

Security planning and information security program plan are shared responsibilities:

(1) Stryker general: SYK has established QMS procedures and trainings for security and safety to be considered during the design & development and post market surveillance of any SW driven Medical Device from SYK. These procedures include the specification of roles & responsibilities.

(2) Application specific security planning: The PSSA, the security architecture and the PS risk analysis define application specific security controls which shall be implemented in the application and considered in accompanying material (e.g service manual)

(3) Customer specific provisions: The SOM establishes application specific security controls and guidance to be considered by the HDO for his security program planning purposes

SOM D001020115 - 3.5 System Security Context and Intended Environment

SOM D001020115 - 06. Security awareness training

SOM D001020115 - 20. Security Program Integration

**22. cryptographic protection & management**

SYK owned devices & HDO (NSA, Wi-Fi Access Point) both should employ the cryptographic elements.

Only stryker made/authenticated devices should communicate with smart medic device & tablet

Safeguard the Sensitive data - Cypto data (eg: keys, tokens, certs)

-Safeguard the sensitive data, such as crypto data (eg: keys, tokens, certificates)

Sensitive data- at rest: offline authentication, tablet map SHA details

- For tablet, offline authentication to be done for sensitive data at rest.

The customer only needs to provide the secure encrypted channel for the communication between the SmartMedic solution’s component i.e., the Device & Tablet, the Tablet & SmartMedic Cloud Application, SmartMedic Cloud Application & the Nurse Station Application. HDO Wifi access point, used in secure communication channel should be protected along with authentication credentials. Hence, communication between the SmartMedic solution’s component i.e., the Device & Tablet, the Tablet & Stryker Cloud, Stryker Cloud & the Nurse Station Application can be cryptographically protected.

**23. malware detection/protection**

Tablet- antimalware is present

- SmartMedic solutions contain malware protection embedded within the SmartMedic tablet.

For NSA – Customer need to install

-Customer (HDO) needs to provide the malware protection for NSA

->SmartMedic solutions contain malware protection embedded within the SmartMedic tablet.

17. Security alerts, adv

No runtime alerts configured for SM platform

SYk can be alerted the following kinds of incidents:

* Any suspected/confirmed malware found on the system
* Any unexpected system behavior observed
* Any suspected misuse of the device (can confirm through logs)
* Incorporated methods detect that any data inappropriately accessed or copied from the device
* From the report of forensic inspection of the device

If any reported vulnerability in the product, the Stryker follows the practice of issuing security advisory along with the corresponding directives.

Malware detection is crucial as attackers exploiting the system in multiple ways and hence it can serve as an early warning to the system regarding cyberattacks. Only Stryker Technical Team is authorized to repair or resolve issues whenever a severe malware is detected.