J&J MedTech

Cybersecurity and Privacy Guide

Ethicon™ Visible Patient™ Ordering Software

Version 1, Rev.003

Help Desk Contact Information		
Hours of Operations: Business Days from 9 am - 6 pm (local country time)		
Phone (by Country)		
France	Toll Free Number	0805543072
Germany	Toll Free Number	08006645633
Belgium	Toll Free Number	080081548
Italy	Toll Free Number	800931565
Saudi Arabia	Mobily and Zain:	8008501204
	Saudi Telecom - STC:	8008447465
Switzerland	Toll Free Number	800111695
Luxembourg	Toll Free Number	80025074
Netherlands	Toll Free Number	08003837002
Qatar	Toll Free Number	00800101113
Spain	Toll Free Number	900810666
Ireland	Toll Free Number	1800800380
United Arab	Toll Free Number	80004441083
United Kingdom	Toll Free Number	08004565933
Email		
Available for all countries		support@ethiconvisiblepatient.com

Contents

1. Overview

1.1. About Ethicon Visible Patient Ordering Software

Ethicon, part of the Johnson & Johnson Family of Companies, is the exclusive global marketing and sales partner for the Visible Patient Planning solution.

The Ethicon Visible Patient Solution helps surgeons create a clear roadmap for surgery. The solution is comprised of two software applications:

Ethicon Visible Patient Ordering Software

Ethicon Visible Patient Ordering Software is used for uploading a patient's CT or MRI medical images and requesting a 3D model. The Visible Patient team then processes the medical images and order requests. Upon order completion, the Ethicon Visible Patient team sends the 3D model to the order requestor. The order requestor then can download the Ethicon Visible Patient 3D model file (file extension ".vpz") and save to a local hard drive or cloud based storage. Ethicon is responsible for the secure transfer of data to Visible Patient for the purpose of fulfilling customer 3D model orders.

Users have two options for uploading CT or MRI medical images. The first option is to upload the data through the Siemens Teamplay* PACS integration. If this method is used, Direct Patient Identifiers (DPI) are removed based on the hospital's Teamplay* integration. The second option is manual upload of the medical images. With this method, Direct Patient Identifiers are stored encrypted in Teamplay*, and the DPI are removed before the medical images are downloaded by Visible Patient.

Ethicon Visible Patient Ordering Software solution leverages the Siemens Healthineers Teamplay* Digital Health Platform. The Teamplay* Digital Health Platform meets industry best practices for security and privacy and is compliant with GDPR (General Data Protection Regulation) and ISO/IEC 27001.

Ethicon Visible Patient Ordering Software is deployed on regional isolated clouds, making it compliant with the data storage rules for each individual region, and preventing data leaving the region.

The Siemens Teamplay* Digital Health Platform is based on Microsoft Azure+ Cloud and provides protected storage and role-based access control for specific organizations (hospital or hospital system). DICOM studies including Direct Patient Identifiers (DPI) are encrypted in the Teamplay* Digital Health Platform. Only modules related to the DICOM studies contain the key required to access, decrypt, and review the case.

The Ethicon Visible Patient Ordering Software stores select Direct Patient Identifiers. DPI are encrypted during transit and storage in the cloud.

Visible Patient Planning Application

After delivery of the Ethicon Visible Patient 3D model, one of the Visible Patient Planning Applications is used to view the 3D model. Refer to the Visible Patient Planning Application for more information (https://www.visiblepatient.com/en/professionnals/software-documentation/).

Note: This Cybersecurity and Privacy Guide is for Ethicon Visible Patient Ordering only.

Security of systems and data are a core commitment of Johnson & Johnson MedTech (JJMT), to its customers and a core obligation under evolving laws.

This Security Policy summarizes the security measures JJMT applies to protect the Care4Today systems and the data processed within them.

2. Introduction

2.1. Audience

The intended audience includes healthcare institution's systems administrator, network administrator, and/or cybersecurity personnel. The intended audience should have working familiarity with their institution's computer assets, operating systems, networking, cybersecurity, and privacy guidelines.

2.2. Remarks

It is recommended that the healthcare institution's systems administrator implement and maintain a set of facility security and privacy policies and procedures. These policies and procedures should be designed to address the following, and is not limited to:

a. Discretionary access control
b. Methods of auditing
c. Disaster Recovery Plans / Business Continuity Plans
d. Password reset policy
e. Perimeter security (such as firewalls, IDS, proxy servers)
f. Internal security (such as network monitors, log file review, standard vulnerability scans)
g. Physical Security (such as biometrics, locks, cameras)
h. Security Awareness

It is the customer's responsibility to manage the confidentiality, integrity and availability of the information technology resources in its healthcare organization.

2.3. Personal data processed and purpose of processing

Ethicon Visible Patient 3D Model Ordering Portal can process the following types of personal data:

- User account information
- Personal data of patients within DICOM studies including Metadata
- Personal data about institution employees (for example, technologists or physicians) and other persons (for example, referring physicians).

For secure user management, Ethicon Visible Patient Ordering Software leverages Teamplay* Digital Health Platform features for federated single sign on. On behalf of the institution, Ethicon Visible Patient Ordering Software and Teamplay* process the personal data of patients, institution's employees, and others contained in DICOM studies to provide the institution with the functionalities of Ethicon Visible Patient (3D Model Ordering Portal).

2.4. Terms and Definitions

Abbreviation, Acronym, or Term	Definition
3D	Three-Dimensional
AES	Advanced Encryption Standard
API	Application Programming Interface
DICOM	Digital Imaging and Communications in Medicine
DPI	Direct Patient Identifier
GDPR	General Data Protection Regulation
HSM	Hardware Security Module
IDS	Intrusion Detection System
MFA	Multi Factor Authentication
OTP	One Time Password
PACS	Picture Archiving and Communication System
PHI	Protected Health Information
PII	Personally Identifiable Information
RBAC	Role Based Access Control
TLS	Transport Layer Security

2.5. References

ISO/IEC 27001 Information Security Management

Siemens Healthineers Teamplay: https://www.siemens-healthineers.com/how-can-we-help-you

Microsoft Azure: https://Azure.microsoft.com/

3. System Design

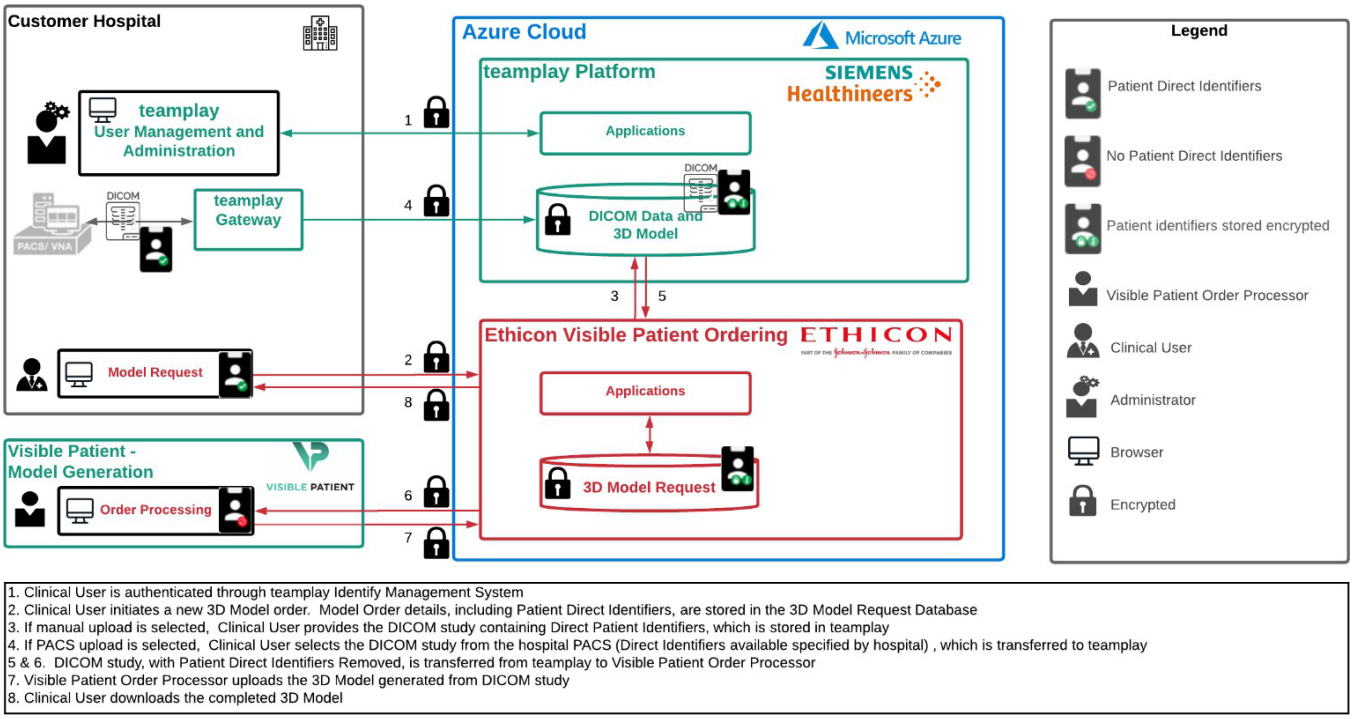

Figure 1. Network Diagram

The DICOM images required for the clinical user's order are securely uploaded to the cloud by one of two methods:

> *Via PACS*: Data can be uploaded using a secure (encrypted) channel from the hospital PACS through the locally installed Teamplay* Gateway. The user only has access to the PACS at the institution to which they are authorized.
>
> *Via Manual Upload*: Data is manually uploaded to the Siemens Healthineers Teamplay* Cloud Platform using a secure (encrypted) channel.

In the case where Manual Upload is used, the DICOM study is stored in the Siemens Healthineers Teamplay* Digital Health Platform encrypted with institution specific keys. The DICOM header data is available to the clinical user with Direct Patient Identifiers. Only user's authorized within the Hospital tenant will have access to view this data.

Order data is stored within the Microsoft Azure+ Cloud platform. The order data includes the name and email of the clinical user placing the order, and the name, MRN, and date of birth of the patient, information provided by the clinical user related to the order. This data is encrypted in the database.

A Visible Patient Order Administrator is responsible for the creation of a 3D model and has access to the Ethicon Visible Patient Ordering application. The DICOM study is downloaded

by the Visible Patient Order Administrator for the creation of the 3D model. Prior to this the Ethicon Visible Patient Ordering Software solution leverages the Siemens Healthineers Teamplay* Digital Health Platform to provide functionality to remove all direct patient identifiers from the DICOM study downloaded by a Visible Patient Order Administrator. In addition, if Teamplay* is integrated into hospital PACS, this functionality is also applied for a DICOM study uploaded to the cloud based on the hospital administrator's selected privacy settings in Teamplay*.

The confidentiality, integrity, and authenticity of all data transmitted from the hospital site is protected by cryptographic means during transport, using TLS (Transport Layer Security).

For managing the solution users and permissions, the solution is equipped with three layers of protection:

1. Microsoft Azure+ Cloud platform has up-to-date security to avoid breaches and malicious attacks.
2. Siemens Healthineers Teamplay* Digital Health Platform is continuously monitored and undergoes regular penetration testing. It is responsible for users' management, Direct Patient Identifier management, case storage, and GDPR compliant environment.
3. Ethicon Visible Patient Ordering application is regularly monitored and undergoes regular vulnerability scans.

	Local Teamplay* Receiver	Ethicon Visible Patient Ordering Software	Siemens Healthineers Teamplay* Digital Health Platform	Visible Patient Applications
Hosting Service	Hospital-specific	Microsoft Azure+	Microsoft Azure+	Docaposte
Data Stored	1. DICOM Data with direct patient identifiers from the Hospital PACS	1. Order details containing Patient and Clinical User information	1. DICOM data from Manual Upload (contains Patient Direct Identifiers) 2. DICOM data from PACS (Patient Direct Identifiers removed) 3. 3D Model	1. DICOM data with Patient Direct Identifiers removed 2. 3D Model
Access	1. Clinical Users can access DICOM studies from PACS through the Ethicon Ordering software via the local Teamplay Installation 2. Users can only access the Teamplay installation for the hospital that they are assigned.	1. Clinical Users can create orders, view all orders from their institution, upload DICOM studies, and download 3D models. 2. Visible Patient Users can view all orders with Patient information removed, download DICOM studies with Patient Direct Identifiers removed, and upload 3D models.	1. Data is accessed through the Ethicon Ordering Software	1. Only Visible Patient Users can access data

Table 1. Summary of System Hosting Services, Data Storage, and Access

4. IT Security Measures provided by Microsoft Azure+ Cloud

Secure Cloud-Based Smart Storage Solution:

The Ethicon Visible Patient Ordering Software solution provides secure storage meeting industry best practices of security and privacy and supports compliance with GDPR.

Microsoft has established a data security policy for Microsoft Azure+ Core Services that complies with the ISO / IEC 27001 standard for Information Security Management Systems, the ISO / IEC 27002 code of best practices for information security controls, and the ISO / IEC 27018 code of practice for protection of personally identifiable information (PII) in public clouds acting as PII data processors. An annual independent audit is performed according to ISO / IEC 27001 standards.

The data centers hosting the data have strong physical security measures in place to shelter data from unauthorized access and from environmental threats. Access to customer data by Microsoft operations and support personnel is denied by default. When granted, access is carefully managed and logged. Data center access to the systems storing customer data is strictly controlled.

5. Data Management

5.1. Data Privacy

The Ethicon Visible Patient Ordering Software Privacy Policy is accessible online at www.visiblepatient.jnjmedicaldevices.com.

The Hospital/Institution is the Data Controller of the Ethicon Visible Patient 3D Ordering System, as defined by the GDPR, for the purpose of provision of healthcare.

Ethicon represented by Cilag GmbH International acts as Processor, with Visible Patient S.A.S., Siemens Healthineers GmbH, Telerx Marketing Inc. d/b/a C3i Solutions, an HCL Technology company and EPAM Systems, Inc. acting as Sub-Processors, for the purposes defined by the agreement with Hospital/Institution.

The principle of Data Minimization is applied throughout the Ethicon Visible Patient 3D Ordering System. To submit and access 3D Model Orders, data including Patient Direct Identifiers is collected and only available to Clinical Users within the Institution's account which they are authorized to access. Patient Direct Identifiers are not displayed to Visible Patient Order Administrators and are removed from DICOM studies that are downloaded to create the 3D Models.

Data is stored in Azure+, with the primary data center located in the Netherlands and backup located in Ireland using smart storage encryption. DICOM Studies which include Patient Direct Identifiers are encrypted with institution-specific keys and individual hospital (or hospital system) data is stored in a logically separated datastore in the Siemens Healthineers Teamplay* tenant on Azure+. The solution uses Azure's+ geo-redundant backup for enhanced data durability in case of a major regional data center disaster.

5.2. Data Retention & Erasure

5.2.1. DICOM studies & Ethicon Visible Patient Ordering system data within Teamplay* Digital Health Platform

The DICOM studies uploaded to Ethicon using the automated forwarding within the Teamplay* Receiver are temporarily retained within Teamplay* Digital Health Platform. The retention period can be configured within the Teamplay* Receiver "Images AETs and Privacy" settings. A retention period of 120 days is recommended for Ethicon.

Ethicon Visible Patient Ordering system data will be retained, as per our Privacy Policy, and Customer requirements.
Please reference your contract for additional data retention information.

5.2.2. DICOM study data within Teamplay* Receiver

The Teamplay* Gateway software temporarily stores DICOM files locally. These files typically contain medical information retrieved from the configured PACS or other systems. After the DICOM files are successfully uploaded to Teamplay* Digital Health Platform, the original files are deleted automatically.

In addition, key material required for the Teamplay* “Data Minimization” function is stored. During the uninstallation of the Receiver software, stored data can be deleted. Deletion is done using means of the underlying Operating System.

5.2.3. Storage media within the Teamplay* Receiver

The Teamplay* Receiver software is installed on a system on the institution’s premises. It is the institution’s responsibility to maintain the system in a secure way and handle the hard disks according to local requirements for storage media that may contain patient information.

5.2.4. Data within Ethicon for Research or Secondary Use

Ethicon Visible Patient Ordering system data including DICOM Studies are only stored within Ethicon databases, for secondary use purposes, if there is a separate Research Agreement entered into with the hospital and dependent on individual Patient Consent. Data is de-identified before further use and its use is proscribed by the agreement and consent terms.

5.3. Access Controls

Access Control to the Ethicon Visible Patient Ordering system is fully managed by the hospital IT personnel. The Teamplay* Digital Health Platform provides secure access management based on the Auth0 authentication service.

The user passwords are stored by Auth0 using a salted hash encryption. The Siemens Healthineers Teamplay* user password follows NIST recommendations and is 8 characters in length and 3 factors of complexity. Session timeout is set to 25 minutes if the user is inactive, and the user must log in again.

The controls around password reset and/or recovery are governed through Auth0. There is a reset functionality which sends a one-time password (OTP) to the email account from which the user can click on a link in the email to the website and provide a new password. Teamplay* implements Role-Based Access Control (RBAC) for User and API access.

The Teamplay* Digital Health Platform management administrator accounts for Azure+ follow the Microsoft guidance for High Security, including Multi-Factor Authentication (MFA). Hospital administrators are required to enable MFA in the Teamplay* Digital Health Platform to use the Ethicon Visible Patient Ordering system.

The Teamplay* Digital Health Platform supports RBAC. The hospital administrators have access to the configuration, including service entitlement and user authorization. The Ethicon Visible Patient Ordering Software users access permission is controlled by the hospital administration. The Ethicon service providers, including Microsoft, Siemens Healthineers, and Ethicon Visible Patient do not have access to the access management environment, except for special dedicated maintenance purposes on behalf of the customer.

5.3.1. Access Control of Application

All users are authenticated through the Teamplay* User Management system prior to accessing the Ethicon Visible Patient 3D Model Ordering Software. Once authenticated, users are only authorized to view orders from the institution they are assigned in Teamplay*.

5.3.2. Data Protections

The Login page is under the purview of Siemens Healthineers; their code development and security scanning prevent tampering and injection of code by malicious clients, and this has been confirmed through penetration testing. The Ethicon application databases do not have an internet-facing endpoint and require direct authentication through the Azure+ management console.

5.3.3. Service Accounts Controls

There is a hierarchy of roles pre-defined in Azure+ which guarantees that access to data must be requested using Access Control Lists (ACLs) so that only specified services can communicate with certain end points.

5.3.4. Security Incidents Management

The incident response team follows established procedures for incident management, communication, and recovery, as well as knowledge management. The security policy found in the Ethicon Visible Patient Ordering Software outlines the recommended process for incidents management.

5.4. Data Security and Regulatory Compliance

The Ethicon Visible Patient Ordering Software is developed in accordance with all the applicable privacy laws and regulations, including GDPR. All sensitive data is stored in Microsoft Azure+, a provider that is developed in accordance with ISO / IEC 27001 global security standard, publishes SOC reports, and is a member of the Cloud Security Alliance.

All server traffic is encrypted in transit using the recommended protocols and ciphers as recommended by ISO / IEC 27001. Our solution containing PII is hosted with Microsoft Azure+ which is certified compliant with the ISO / IEC 27001 global security standard. Microsoft Azure+ publish a full set of compliance reports including SOC 1 (SSAE16) Type II, Soc 2 Type II, and SOC 3. Microsoft Azure+ are both members of the Cloud Security Alliance's Security, Trust and Assurance Registry.

6. Physical Security

Customers should follow their institution guidelines on device security.

7. Securing Operating Systems

Customers should follow their institution guidelines on operating system security.

8. Frequently Asked Questions (FAQ)

8.1. What categories of data are being processed when using the Ethicon Visible Patient Ordering Software?

Personal Data, including Data relating to an individual's health (Special Category data as defined by the GDPR). This consists of patient data necessary to provide the Visible Patient service such as First Name, Last Name, Date of Birth, MRN, and DICOM images.

8.2. Where is the data stored?

Data is stored on the Microsoft Azure+ cloud. Individual hospital (or hospital system) data is stored in a logically separated datastore in the Teamplay* tenant, on the Microsoft Azure+ cloud.

8.3. How is the clinical data classified and categorized?

Data is classified as PII (Personally Identifiable Information) Special Category based on GDPR definitions.

8.4. Does Patient Personal data leave the hospital?

Patient direct identifiers (or "PII") – including Patient Full Name, MRI – are stored encrypted in the Ethicon Ordering Software database. If data is uploaded via Manual Upload, Patient direct identifiers (Patient Full Name, Date of Birth, MRN) are also stored in Siemens Healthineers Teamplay* and transmitted and stored in encrypted format on the cloud. Patient direct identifiers are only viewable by the Clinical Users at the institution where the information was uploaded. Other users are identified as non-clinical and do not have access to PII.

8.5. What are the solution's certifications?

Microsoft Azure+ certifications are accessible online at https://www.microsoft.com/en-us/TrustCenter/Compliance/ISO-IEC-27001 More specifically, the data centers hosting the data have strong physical security measures in place to shelter data from unauthorized access as well as from environmental threats. All Azure+ services use approved media storage and disposal management services. See https://docs.microsoft.com/en-us/Azure/security/Azure-physical-security and the facility SSAE 16 SOC 2,3 compliant https://Azure.microsoft.com/de- de/blog/security-privacy-compliance-update-availability-of-ssae-16-isae-3402- attestation/.

The Teamplay* Digital Health Platform, together with selected Teamplay* applications, e.g., Teamplay* Images, operated in European data centers has been awarded the European Privacy Seal (EuroPriSe). The seal confirms that Teamplay* complies with GDPR data privacy and security requirements. For more information see https://www.european-privacy-seal.eu/EPS-en/ Siemens Healthineers-healthcare-Teamplay.

Siemens Healthineers has established and applies an Information Security Management System for the provisioning of secure design, development, and operations of Teamplay*. Teamplays' Information Security Management System (ISMS) is certified to be compliant with ISO/IEC 27001:2013 regarding the secure design, development, and operations of the Teamplay* Digital Health Platform In addition, it allows customers to be HIPAA compliant.

Ethicon Visible Patient Ordering Software is an application running on these platforms, following each platform's Security & Privacy guidelines. In addition, it follows the Johnson & Johnson Cybersecurity and Privacy guidelines.

8.6. Do the Ethicon service providers have a Computer Security Incident Response Team?

Microsoft Azure+ is protected by Microsoft's Computer Security Incident Response Team as part of their Azure+ cloud protection.

Siemens Healthineers makes use of a 24/7 incident response team to react to any attacks on its systems. In the event of a data breach involving institutional data, Siemens Healthineers will notify customers in compliance with the applicable data protection law and respond according to the Siemens Healthineers privacy incident management process.

Johnson & Johnson has a Security team available for its customers' needs.

8.7. How is data encrypted in transit and at rest within the system?

Data in transit is encrypted using TLS v1.2 with strong ciphers enforced. Data at rest is encrypted using AES256. In addition, if Teamplay* images are configured to upload data without its "data minimization" function, the uploaded data is encrypted using an institution specific key (RSA 2048 Bit/AES 256 bit) stored in a Hardware Security Module (HSM). The Reidentification backup requires a 4096 bit RSA key for encryption.

The local Teamplay* Gateway authenticates securely against the Teamplay* cloud backend. The integrity of the receiver software is checked regularly through an automated backend service.

8.8. What is the authentication protocol used to authenticate users and service IDs to the application?

The authentication tokens are valid for 25 minutes and all authentication sessions are secured by TLS.

8.9. How does the user authentication work?

Auth0 authentication rules are used, and users must enable multi-factor authentication (MFA).

8.10. How are components such as config files, run-time environments, interpreters, and other third-party components, including open-source components, controlled?

All third-party components are treated as Software of Unknown Pedigree (SOUP), regardless of the source. Integration and testing of all SOUP is in accordance with the Johnson & Johnson Information Asset Policies.

8.11. How are versions of the source-code, working binaries and other components securely stored and controlled?

All Siemens Healthineers and Ethicon source code, including third party components, are version-controlled on the Azure+ DevOps Services server, which meets the strictest medical device level in the US, according to FDA standards.

8.12. How does the solution prevent the loss of data?

The solution uses Microsoft Azure's geo-redundant backup for enhanced data durability in case of a major regional data center disaster. The geo-redundant backup is located in the same region, to follow the demand of storing the data only in the allowed region. The data is backed up every five minutes and retained for a minimum of 30 days.

8.13. What is the role of any client-side code used within the application architecture, and how are unauthorized actions by this code controlled?

The Ethicon client-side code is JavaScript, which allows the user to view the Ethicon data on the web. The access is protected by the Siemens Healthineers authentication API.

8.14. How are inputs and outputs protected from tampering and injection by a malicious client?

The Login page is under the purview of Siemens Healthineers; their code development and security scanning prevent tampering and injection of code by malicious clients, and this has been confirmed through penetration testing.

8.15. How are application components such as databases, files, and directory services protected from direct access?

The databases do not have an internet-facing endpoint and require direct authentication through the Azure+ management console.

8.16. How are service accounts controlled, such that they cannot be used to compromise the data and the application and ensure adherence to the Least Privilege principle?

There is a hierarchy of roles pre-defined in Azure+ which guarantees that access to data must be requested using Access Control Lists (ACLs) so that only specified services can communicate with certain end points.

8.17. How are segregation of duties (SoD) conflicts identified and prevented?

Hospital IT Admin adds and removes users for their institution. SoD is adhered to for both the platform and application administration.

8.18. How are digital certificates, which are used for server identity and enabling encrypted communication, managed, and checked for validity?

Each digital certificate in the certificate chain is checked against a locally available trusted root certificate for acceptance of validity and certificate use. In addition, within TLS certificates, the domain name in the certificate is checked for a match against the accessed domain name.

8.19. How are the log contents determined? What are logs? How it will be reviewed?

8.19.1. Logging

The runtime behavior of the Teamplay* and Ethicon Visible Patient Ordering Software is logged and monitored for quality assurance purposes.

8.19.2. Audit Logs

The Ethicon Ordering Software generates audit logs for all changes made to the system, as well as security and privacy related actions. Audit logs are regularly reviewed.

The Teamplay* Digital Health Platform generates audit logs for security or privacy relevant actions. This particularly means that audit logs are generated for all Teamplay* user login and logout actions managed by Teamplay*.

In addition, for the following actions audit logs are generated including the requesting UserID and the StudyInstanceUID if applicable:

- Configuration Changes in Teamplay* portal
- DICOM Query and related operations
- DICOM Retrieve and related operations
- DICOM download operations (study, series levels)
- DICOM study attachments download operations

Please note that if data minimization has been applied to UIDs, the audit log will contain the modified StudyInstanceUID. Retention periods for audit logs are defined according to the purpose of processing.

8.20. What is the escalation process for service related issues and notifications of data breaches?

If the hospital suspects a data breach, or incident, their first point of contact is with the Ethicon support organization. In the event of Siemens Healthineers becoming aware of a data breach, they will notify Ethicon

8.21. How are security incidents managed?

Siemens Healthineers makes use of a 24/7 incident response team to react to any attacks on its systems. In the event of a data breach involving institutional data, Siemens Healthineers will notify customers in compliance with the applicable data protection law and respond according to the Siemens Healthineers privacy incident management process.

Ethicon and Siemens Healthineers incident response teams follows established procedures for incident management, communication, and recovery, as well as knowledge management.

8.22. Who is responsible for reviewing and data sharing access rights?

The review and data sharing of access rights for Teamplay* and Ethicon Visible Patient Order Software users is the responsibility of the hospital administrator. There is no elevation of privileges within Teamplay*. For the Azure+ platform access, Teamplay* has defined roles and duties.

8.23. How are patches assessed and implemented to address known security vulnerabilities?

Siemens Healthineers and Ethicon are continually monitoring for vulnerabilities affecting its products including the related risk. Depending on the risk specified by Microsoft, patches are automatically installed.

8.24. What are the encryption standards?

Data in transit is protected with TLS 1.2 with a 256 bit cipher strength. Data at rest is stored in Azure+ databases with AES 256.

Visible Patient™ Planning is a medical device software designed to be used by trained professionals (including physicians, surgeons, and technicians) and is intended to assist the clinician who is solely responsible for making all final patient management decisions.

For complete indications, contraindications, warnings, precautions, and adverse reactions, please reference full Indications for Use and User Manual here: https://www.visiblepatient.com/en/professionnals/software-documentation/.

* For additional Siemens Healthineers Teamplay* questions, please contact Siemens Healthineers directly: https://www.siemens-healthineers.com/how-can-we-help-you.

+ For additional Microsoft Azure questions, please contact Microsoft directly: https://Azure.microsoft.com/.

The third-party trademarks used herein are trademarks of their respective owners. Cilag

GmbH International, Gubelstrasse 34, 6300, Zug, Switzerland
©Cilag GmbH International 2021, www.jnjmedicaldevices.com