ETHICON VISIBLE PATIENT SOLUTION
Johnson & Johnson Security Policy

A. General regulations

- The 3D model ordering and delivery system is a web-based solution controlled by an IT administrator, created by the Customer. Without the IT administrator's consent, operations will not be possible or permitted.
- Access rights are granted only by the IT administrator to the extent necessary for the execution of initiating the 3D model order request and reviewing or retrieving the order.
- Deployment of new program versions and updates, as well as changes to configurations, will be automatically pushed to registered users.
- All users will gain access only via interactive login and multi-factor authentication.
- Application data is stored in Siemens Healthineers regional data centres
- DICOM data is de-identified by Siemens Teamplay
- Images are processed by Visible Patient S.A.S
- **For France Only:** Visible Patient S.A.S stores anonymized data in Docaposte, a French Health Data Hosting Company

B. Confidentiality of data processing (Art. 32, paragraph 1, lit. b of the GDPR)

1. Admission/Access Control

(*Measures to prevent unauthorized persons from gaining access to data processing systems with which personal data are processed or used*.)

- Application is web-based and controlled by Siemens Teamplay
- No physical access to data processing infrastructure
- Data is stored in local Azure data centres and managed by Siemens Healthineers
- The Siemens Healthineers platform removes PII and ensures Non-clinical users can only access non-identifiable data and DICOM images for 3D model rendering
- Non-clinical users will not have access to PII Clinical users will have access to PII

2. Access Control

(*Measures to safeguard:*

- *data processing systems from being used by unauthorized persons*
- *that the attempt of unauthorized access does not remain unnoticed*.)

- Order Management: Login and access is controlled by Siemens Teamplay Platform
- Passwords: A minimum of 8 characters with at least 3 complexity classes and MFA
- Suspicious Login Attempts: The system uses suspicious IP throttling and brute-force protection
- Hospital PACS: Secure access is managed by Siemens Teamplay Gateway
- Defined group of persons with access to systems, applications and data carriers
- All users are administered centrally and are assigned a unique master record, and respectively personalised user accounts
- Technical and organisational measures ensure that authorisations which are no longer needed will be revoked as soon as possible
- Firewall systems

3. User access control

(*Measures to ensure that*

- *persons entitled to use a data processing system have access only to the data to which they have a right or need to access, and - especially by using state of the art encryption methods - that personal data cannot be read, copied, modified or removed.*
- *that the attempt of unauthorized access does not remain unnoticed*.)

- Personal and individual user login for the system respective to the company network; additional system login for certain applications;
- Administration of differentiated authorisations, profiles and roles; all users are administered centrally and are assigned a unique master record and personalised user accounts;
- Applications for assignment to protectable resources are only requested and assigned by authorised persons;
- Documentation of authorisations; defined group of persons with access to systems, applications and data carriers;
- Technical and organisational measures ensure that authorisations which are no longer needed will be revoked as soon as possible.

4. Separation Control
(*Measures for separation control guarantee that the personal data processed for different purposes are processed separately*.)

- Separated systems
- Separated databases
- Access rights (see No. 3)
- Monitoring / inspection of external service providers has occurred to the extent that they have the ability to access personal data

C. Pseudonymisation (Art. 32, paragraph 1, lit. a of the GDPR; Art. 25, paragraph 1 of the GDPR)
(*The processing of personal data in a manner in which the data no longer can be associated with a specific data subject without adding additional information, as long as such additional information is retained in a separate location and is subject to corresponding technical and organizational measures*.)

- The data collected for order submission is stored by Siemen's Healthineers
    - Non-clinical users will not have access to PII which is redacted in the Siemens Healthineers platform
    - Clinical users will have access to PII

- While taking the state of the art of technology, the implementation costs and the type, scope and circumstances of the purposes for processing as well as the different probabilities of occurrence and severity of the risk to the privacy of natural persons into account, the possibilities for pseudonymisation and anonymisation shall be reviewed and implemented to the extent possible.

D. Integrity (Art. 32, paragraph 1, lit. b GDPR)

1. Transmission Control
(*Measures to ensure that:*
- *personal data cannot be read, copied, modified or removed without authorization during electronic transmission or (physical) transport or storage on data carriers, especially by using state of the art encryption methods.*
- *data carriers containing personal data may only be transported to a shredder only in closed containers/repositories and in closed vehicles, so that no material will get lost*.)

- Data is encrypted in transit and at rest relying on Siemens Gateway and Teamplay platforms
- Connections such as APIs are via secure channels with Public / Private keys
- SSL-encryption on web-access
- PII data processing is handled within regional data centres
- Application sits behind a WAF

2. Input Control
(*Measures to ensure a retrospective verification and determination of and by whom personal data in data processing systems has been entered, changed or deleted*.)

- User access control
- All users of the 3D model ordering system have access only to the data necessary within the scope of their function/role (principle of minimal rights).

E. Availability Control and Resilience (Art. 32, paragraph 1, lit. b of the GDPR)
(*Measures for data protection (physically / logically) against random destruction or loss*.)

- Data backup
    - Siemens Healthineers Teamplay Cloud Services via Microsoft Azure Storage
    - Microsoft Azure Storage
    - Azure SQL Database
    - High availability with geo-redundant storage
    - SQL – backups are taken every 5 minutes and maintained for at least 30 days
- Recovery procedure are conducted on a weekly basis
- Implicit validation of backups and recovery procedure are conducted on a weekly basis
- Explicit Validation, a formal validation plan for the critical SQL Database backup process, is performed and verified with every software release, at least every four months.

F. Procedure for regular review, analysis and evaluation (Art. 32, paragraph 1, lit. d of the GDPR; Art. 25, paragraph 1 of the GDPR)

1. Data protection management
(*Organization and implementation of procedures that ensure that the legal and operational requirements of data protection are systematically planned, organized, managed and controlled*.)

- Regular data protection training for all users;
- General data protection documentation in accordance with the legal regulations;
- Close cooperation between management and the Data Protection Officer.

2. Incident response management
(*The presence of organizational and technical processes to respond to detected or suspected data protection breaches, security incidents or malfunctions in the IT areas as well as preventive measures in this respect*.)

- All users are obligated to immediately report data protection breaches or malfunctions of the operational or procedural processes to submit to our support centre, delivered by our sub-contractor C3i (customer service centre)
- Regular data protection training for all users;
- Monitoring of IT systems;
- Close cooperation between management and the Data Protection Officer.

3. Order supervision
(*Measures to ensure that personal data being processed on behalf of the Controller may only be processed according to the Controller's instructions*.)

- A Data Protection Officer is appointed;
- There is a written contract for contract data processing according to Art. 28 of the GDPR;
- The Controller has comprehensive contractual rights of instruction;

- A data security concept is available with respect to the technical and organisational measures taken regarding data protection;
- Instructions and changes to the process will be made in written form;
- All users with access rights are committed to data secrecy and maintaining confidentiality;
- Training sessions have taken place for all users with access rights;
- The Controller will be immediately informed if errors occur in the scope of data processing or if data protection rules have been violated;
- All authorised persons and instructions are defined by contract.

4. Precautionary measures in favour of data protection (Art. 25, paragraph 2 of the GDPR)

- All processes only include processing the data that is necessary for the specific case
- By means of an activated access rights system, all users of the system only have access to the directories and information that are necessary to perform their role / function.