M2S

APPROVED

Maintaining Patient Confidentiality

1. PURPOSE/SCOPE AND HIPAA DATA USE:

1.1. This procedure describes the requirements for maintaining the confidentiality of patient data for all patient data that are maintained by or for M2S.

1.2. Any misuse of PHI outside the data use scope will be sanctioned following the M2S HIPAA Sanction Policy & Procedure SEC-WRK-0-08.

2. DEFINITIONS:

2.1. Patient Protected Health Information - shall have the same meaning as the term "protected health information" in 45 CFR 164.501, limited to the information created or received by Business Associate from or on behalf of Covered Entity. This includes, but is not limited to such information as patient name, social security number, driver's license number, street address, telephone number, and email.

3. References:

3.1. SEC-POL-0-01:	General Privacy and Security Policy and Procedures
3.2. SEC-WRK-0-04:	Commercial Vascular, Clinical Trial Project Management, and Independent Reader Processes PHI Data Flow
3.3. SEC-WRK-0-05:	Pathways/VQI PHI Data Flow
3.4. SEC-WRK-0-08:	M2S HIPAA Sanction Policy & Procedure
3.5. TRN-SOP-1-00:	Employee Training Program: General
3.6. TRN-SOP-2-00:	Employee Training Program: Certifications

4. PROCEDURE AND RESPONSIBILITIES:

4.1. QA:

4.1.1. Confirms procedures are in place for ensuring the confidentiality of patient information from the receipt of patient information through the production, shipping and storage of the information.

4.1.2. Confirms procedures are established in compliance with HIPAA regulations and SEC-POL-0-01 for the control of customer supplied products and patient protected information.

4.1.3. Trains M2S personnel annually regarding the guidelines and company policies related to privacy and security. This may be performed during the new hire or annual quality refresher trainings.

4.1.4. The M2S Privacy Officer is responsible for ensuring authorization is appropriate for PHI access.

4.1.5. The M2S Privacy Officer, along with the appropriate supervisor and HR as appropriate, is responsible for ensuring sanctions are applied appropriately according to SEC-WRK-0-08.

4.2. Production Manager:

4.2.1. Documents procedures for control, verification, storage, processing, maintenance and shipping of patient information and customer-supplied products.

4.2.1.1. Ensures conformance with these procedures within the Production Dept.

4.2.1.2. Ensures adequate training in these procedures for all Production employees.

4.2.2. Works with QA as appropriate to determine training needs for an individual or group based on the job requirements and the experience, education and training of an individual or group.

4.2.2.1. Provides the training as required and ensures that it is effective in accordance with TRN-SOP-1-00 and TRN-SOP-2-00 as appropriate.

4.2.2.2. Determines, with QA as appropriate, the training needs of current employees through periodic evaluations.

4.3. All Employees:

4.3.1. Responsible for ensuring the confidentiality of customer supplied patient information during all stages of production.

4.3.2. Responsible for following the privacy and security protections outlined in SEC-POL-0-01 and related documents.

4.3.3. All employees are responsible for using the minimum amount of PHI and ePHI to perform the required job functions. PHI and ePHI may be used to perform contracted activities required by controlled procedures.

4.3.3.1. Applicable procedures are controlled documents found in EtQ which describe the processes and work instructions to perform roles and job functions related to M2S products and services.

4.3.3.2. Reference the applicable PHI data workflows Commercial Vascular, Clinical Trial Project Management, and Independent Reader Processes PHI Data Flow SEC-WRK-0-04, and Pathways/VQI PHI Data Flow SEC-WRK-0-05.

4.3.4. All employees are required to train to the appropriate procedures to perform their job functions. Procedures are located in EtQ and assigned to each employee as appropriate. Training records are maintained in EtQ.

4.3.5. Employees are responsible for following the Systems Security Policy and User Guidelines procedure ITS-POL-0-01.

4.3.5.1. Employees are responsible for understanding their unique username and password electronic signature is equivalent to their handwritten signature as described in the Electronic Signatures procedure QMS-POL-0-07.

4.3.5.2. Passwords are required to be kept confidential and not shared with anyone.

4.3.5.3. Strong Passwords are required as described in the Password Policy procedure SEC-WRK-0-02.

4.3.6. Employees are responsible for following the Facility Security/Alarm System procedure HRA-WRK-0-02 to help ensure physical security measures are in place in ePHI areas.

4.3.6.1. This includes the use of key-card access and signed out visitor badges.

4.3.7. All complaints received at M2S are to be entered into the CAPA system in EtQ without delay. Reference the Complaint, Failure Investigation and Medical Device Reporting procedure CCF-SOP-1-00, and the Customer Feedback and Complaint Logging procedure CCF-WRK-1-01.

4.3.8. Employees understand that violations to the M2S privacy and security program as described in the General Privacy and Security Policy and Procedures SEC-POL-0-01, including misuse of PHI or ePHI, will be subject to disciplinary sanctions as described in the M2S HIPAA Sanction Policy & Procedure SEC-WRK-0-08.