Special Terms for Centralized Management of Apple Mobile Devices without Customer-owned User Accounts (Apple ID) ("MDM Terms")

(Version: 17.05.2024)

These MDM Terms govern the centralized management of Apple mobile device(s) without customer-owned user accounts via an online connection in addition to (i) the Commercial Form and (ii) the General Terms, the Supplemental General Terms and any other terms or schedules referenced in the Commercial Form (together "Terms"). These MDM Terms shall be read as complementary to the Terms and prevail in case of conflict.

0. Definitions

In addition to the definitions in the Terms the following definitions apply:

0.1. "Device" means the Apple mobile device(s) which is (are) sold or otherwise made available to Customer and which is (are) specified in the Commercial Form.

0.2. "MDM Agreement" means the agreement addressing the MDM Connection to the Device(s) and the MDM Services comprising of these MDM Terms (including the Security Concept) and the Terms.

0.3. "MDM Connection" means an online connection between Siemens Healthineers, its Affiliates or service providers contracted by Siemens Healthineers and the relevant Device(s) at Customer's site.

0.4. "Security Concept" means the IT security concept of Siemens Healthineers AG, to which general information can be found under the following link https://www.siemens-healthineers.com/support-documentation/cybersecurity, and to which modality-specific information can be found at fleet.siemens-healthineers.com or which Siemens Healthineers will send to Customer upon request.

0.5. "Technical Data" means information available through the MDM Connection and may include:

(i) technical status information, including Device or application logfiles, errors occurred, Device properties and status, quality control;

(ii) asset and general configuration data, including asset and device configuration, software versions, patches, licenses, network settings and Device service history;

(iii) and any other data explicitly agreed

in each case not related to an identified or identifiable natural person.

1. Use of MDM Connection and MDM Services

Siemens Healthineers, its Affiliates and/or service providers engaged by Siemens Healthineers or its Affiliates are authorized to manage the Device(s) through the MDM Connection, which may include, but is not limited to, access, maintain, repair, calibrate, monitor, update, or patch the Device(s), and to access and use the Technical Data collected through the MDM Connection for these activities (collectively, "MDM Services").

2. Use of Data

Subject to applicable data privacy laws Customer permits Siemens Healthineers, its Affiliates and service providers of Siemens Healthineers or its Affiliates to use any Technical Data related to Siemens Healthineers' or its Affiliates' products, software and services on a non-exclusive basis without restriction in terms of time, location, transferability and sublicensing for the business purposes of Siemens Healthineers and its Affiliates such as (i) facilitating and advising on a continued and sustained use of products, software and services; (ii) the substantiation of marketing claims for their products, software and services by means of aggregated data; (iii) benchmarking; (iv) research or development purposes (for example to determine usage trends, or to improve existing and/or develop new products, software and services); or (v) fulfilment of legal or regulatory obligations, including product surveillance.

3. Obligations of the Parties

3.1. Siemens Healthineers shall setup the technical and organizational process for MDM Connection and IT infrastructure used by Siemens Healthineers for the establishment of the MDM Connection according to the Security Concept.

3.2. Siemens Healthineers may provide information to Customer about the MDM connectivity status and general information on how to restore the connection in case it is not properly working.

3.3. Customer shall regularly check, e.g., on the link as per Section 0.4, whether an updated version of the Security Concept is available and take measures to support compliance with the current Security Concept.

3.4. Customer shall permit the MDM Connection to be established by connecting the Device(s) at Customer's own expense to the secured telecommunications link via a broadband connection. Customer shall bear the costs of any technical requirements for any such a connection not being part of the Device(s), e.g., establishing a broadband connection.

3.5. In order to protect the Device(s) against cyber threats, it is necessary that Customer implements - and continuously maintains - a comprehensive, holistic, state-of-the-art security concept protecting Customer's IT infrastructure, including regular vulnerability scanning, but subject to the proviso that (i) scanning or testing shall not be performed during clinical use, and (ii) the system configuration and/or IT security controls of the Device(s) must not be modified. Customer shall also support Siemens Healthineers in protecting against cyber threats. This means Customer shall particularly not

3.5.1. connect any hardware to the Device(s) or the MDM Connection or install any software on the Device(s) that does not comply with state-of-the-art security policies or that is not otherwise approved by Siemens Healthineers; or

3.5.2. use the MDM Connection in a way that impairs or disrupts the integrity of the MDM Connection, or Siemens Healthineers' IT infrastructure; or

3.5.3. transmit any data containing viruses, Trojan horses or other programs that may damage or impair the MDM Connection, or Siemens Healthineers' IT infrastructure.

4. Limited Warranty

4.1. Unless explicitly otherwise regulated, the MDM Connection and MDM Services are provided "as is" and Siemens Healthineers does not provide Customer with any warranty or guarantee regarding the availability, performance, or quality of the MDM Connection or the MDM Services other than addressed in the Security Concept.

4.2. Siemens Healthineers will not provide an MDM Connection and/or MDM Services, if

4.2.1. the provision is prevented by any impediment, e.g., arising out of national or international foreign trade or custom requirements, embargoes, or other sanctions; or

4.2.2. there is a defect, malfunction, or other problem with the telecommunications network or the MDM infrastructure; or

4.2.3. there is a defect, malfunction, insufficient configuration, or other problem with Customer's infrastructure.

5. Update of Terms and Security Concept

5.1. Siemens Healthineers is entitled to modify and/or update these MDM Terms and/or the Security Concept to reflect technical progress, changes in law and further developments of offerings.

5.2. Such modifications and/or updates shall not jeopardize the quality and execution of the MDM Connection and/or the MDM Services.

5.3. Siemens Healthineers shall inform Customer of changes by giving Customer a reasonable period of notice of at least 30 days. Siemens Healthineers will provide Customer with access to the updated terms.

6. Certification

Siemens Healthineers AG - operating the MDM infrastructure together with service providers - shall maintain a certified information security management system for the purposes of the MDM Connection. In this regard, Siemens Healthineers AG shall be subject to regular external audits by independent third parties. The scope and details of the certification are determined in the current Security Concept.

7. Termination and Suspension

7.1. This MDM Agreement may be terminated by either Party in writing at any time, giving a notice period of 4 weeks. The validity of any other agreements between Customer and Siemens Healthineers shall be unaffected by a termination of this MDM Agreement.

7.2. Either Party shall be entitled to terminate this MDM Agreement with immediate effect if the other Party breaches this MDM Agreement and such breach is not cured within a period of 14 days from receipt of notice of the breach of the other Party.

7.3. Siemens Healthineers shall be entitled to suspend the MDM Services and/or the MDM Connection with immediate effect if Customer is in breach of this MDM Agreement or if Siemens Healthineers - acting reasonably - is of the opinion that the MDM Connection to one or more of Customer's Device(s) contains a risk for the security and/or performance of the IT infrastructure used by Siemens Healthineers.

8. Intellectual Property

Siemens Healthineers will own all right, title and interest in and to all intellectual property rights relating to improvements derived from Technical Data and any suggestions, ideas, enhancement requests, feedback, recommendations, or other information provided by Customer which are hereby assigned to Siemens Healthineers.