GDPR（EU 一般データ保護規則）第 28 条に基づく Siemens Healthineers 個人情報取扱い規定

本 GDPR（EU 一般データ保護規則）第 28 条に基づく Siemens Healthineers 個人情報取扱い規定（以下「DPA」という）は、当社と取引先（以下、総称して「両当事者」といい、個別に「当事者」という）との間で締結される契約（以下「主たる契約」という）のデータ保護義務を補足し明確化することを目的とする。本 DPA は、主たる契約において、当社の従業員または当社と契約関係にある第三者が、主たる契約の相手当事者（以下「顧客」という）の個人データを取り扱う場合において、当該主たる契約に関連するすべての行為に適用される。

第 1 条 取扱いの対象事項、性質、目的及び取扱期間

(1) 本 DPA は、当事者間で締結される主たる契約を補足するものである。本 DPA は、主たる契約に基づき当社（「処理者」）が顧客（「管理者」）に代わって個人データを取り扱う場合に適用され、また、当事者間のデータ保護義務を規定する。
(2) 取扱いの性質および目的：当社は、主たる契約において特定・合意されたサービスを提供するために必要な範囲で個人データを取り扱う。
(3) 当社および顧客は、それぞれ、適用されるデータ保護に関する法令を遵守することについて責任を負う。顧客は、個人データを取得するための手段について単独で責任を負う。また、顧客は、法令上許容され、顧客が法律上取扱うことができる場合に限り、個人データを当社に開示するものとする。
(4) 取扱いの期間は、主たる契約の期間と同一とする。

第 2 条 個人データの種類およびデータ主体の分類

主たる契約の規定に応じて、データ主体は、特に従業員、患者、顧客の担当窓口となる者および顧客の契約上のパートナーに分類される。取扱い対象となる個人データの種類は、特に連絡先情報、識別子、健康情報、遺伝データ、生体データ、位置データおよび財務情報に分類される。

第 3 条 指示

(1) 当社は、顧客による書面による指示に基づいてのみ個人データを取り扱う。本 DPA および主たる契約は、個人データの取扱いに関する顧客の当社に対する完全かつ最終的な書面による指示である。
(2) 追加または代替の指示は、顧客が書面で発行しなければならず、また、当社が書面で確認した場合に限り効力を有する。当社は、顧客による指示が GDPR（EU 一般データ保護規則）またはデータ処理者である当社に対して適用されるデータ保護規定に違反すると考える場合、顧客に通知するものとする。当社は、包括的な法的検討を行う義務または法令に違反する指示に従う義務を何ら負うものではない。
(3) 顧客は、追加または代替の指示の結果当社が負担することとなったすべての追加費用を負担するものとする。ただし、当該指示が当社に適用される法令上の義務を遵守するために必要な場合はこの限りでない。

第 4 条 機密

当社は、個人データの取扱いを許可された個人が契約により継続的な秘密保持義務を負い、または法令に基づき当該義務を負うことを保証する。

第 5 条 取扱いにおけるセキュリティ

(1) 当社は、GDPR 第 32 条に基づき義務づけられる全ての対策を講じるものとする。
(2) 到達水準、実施の費用、取扱いの性質、範囲、文脈および目的、ならびに引き起こされる自然人の権利および自由に対する様々な可能性および重大性のリスク、また特に取扱いによって生じるリスク、特に偶発的または違法な破壊、滅失、改変、送信、保存もしくはその他の取扱いがなされた個人データの不正開示または不正アクセスに基づくリスクを考慮し、当社は、付属書類 TOM に定める技術的およびび組織的対策を実施するものとする。
(3) 顧客および当社は、付属書類 TOM に定める技術的および組織的対策の実施により、GDPR に基づく適切な保護水準が確保され、データ主体の権利保護のために十分な予防措置が講じられることに合意する。
(4) 付属書類 TOM に定める技術的および組織的対策は、技術的進歩とさらなる進展に依存しており、適切である場合は当社により調整することができる。ただし、当該調整により、付属書類 TOM に規定する保護水準より低い水準とならないことを条件とする。

第 6 条 復処理者

(1) 当社は、顧客に代わり特定の取扱行為を遂行する復処理者（別の処理者）を使用することがある。復処理者は、個人データが当社に提供されることとなった目的の範囲に限り、当該個人データを取り扱うことが認められ、それ以外の目的で個人データを取り扱うことは禁止される。当社が使用する復処理者は、書面化されたデータ保護義務の適用対象となり、本 DPA に定める保護レベルと同等以上の保護を実施する。当社は、特に、取扱いが GDPR の要件を満たす適切な技術的および組織的対策を実施することにより、十分な保護措置を提供し、関係するデータ主体の権利を保護し、データ移転の記録を保持し、適切な保護措置を文書で記録することを確実にするものとする。
(2) 当社が現在使用している復処理者のリストは https://fleet.siemens-healthineers.com/welcome にて入手することができる。当社は、随時、当該 URL を更新する権利を留保する。
顧客は、当社に対し、当該リストに記載された会社を復処理者として使用することを承認する。顧客は、復処理者に関する情報および復処理者の使用状況または変更等の異動情報を受領するため、上記当社のウェブサイトを確認するものとする。
(3) 復処理者の追加または変更は、当社が事前に顧客に通知するものとし、通知後 3 ヵ月以内に顧客が書面（電子形態を含む）をもって当社に対し反対の意思表示をしない場合、承認されたものとみなされる。
(4) 顧客は、反対する場合、その理由の詳細を当社に通知するものとする。
反対する旨の通知があった場合、当社は、その裁量により以下の措置を行うことができる。
a. 拒否された復処理者に代わる別の復処理者を提案すること、または、
b. 顧客の懸念に対処し、その反対を解消するための手段を講じること
(5) 本 DPA 第 6 条(4)a.および b.の措置を合理的に行うことができない場合またはその他の方法により反対が解消されない場合、当社は、通知することなく主たる契約の全部または一部を解除することができる（例として、顧客の反対により当社による契約上の義務の履行がさらに困難または不可能となる場合等）。

Confidential

(6) 使用を拒否された復処理者の業務開始予定日から別の復処理者が業務を開始するまで、応答時間または利用可能性についての合意事項は、一時停止され、この点において当社にかかる契約履行に代わる損害、遅延、または合意済みの約定損害賠償もしくは契約上の違約金としての賠償請求などいかなる請求も適用されない。当社の履行義務が一部終了する場合、当該一部終了による影響を受けないサービスに対する報酬は、当社において当該サービスに適用されている当社の標準料金表に従い決定される。
(7) 復処理者が自身のデータ保護義務を履行しない場合、当社は、主たる契約の責任規定に従い、顧客に対し、復処理者の義務の履行について全面的に責任を負う。当社は、本 DPA 第 3 条(2)の顧客による追加または代替の指示に起因する損害および請求については責任を負わない
(8) 当社は、第三国(EU／EEA 域外)において復処理者を使用する場合、GDPR 第 44 条以下に準拠するデータ移転のメカニズムを利用する。
(9) 当社が EU 委員会決定 2010/87/EU に基づく標準的契約条項または GDPR 第 46 条に従う標準データ保護条項(「標準データ保護条項」)等により十分な保護措置を提供する場合、顧客は、当社が顧客の名において顧客のために当該標準データ保護条項を締結する代理権を付与する。更に、顧客は、当社が当該標準データ保護条項を締結する際、各復処理者を代理することについても明示的に許可する。これは、当社が顧客および復処理者に代わり行為する権利を有することを意味する。当社は、また、標準データ保護条項に基づく顧客の権利および権限を復処理者に対し行使する権利を有する。

第 7 条　支援

(1) 主たる契約および本 DPA に記載する取扱いの性質を考慮の上、当社は、要請があれば、顧客の費用負担により、GDPR 第 12 条ないし第 23 条に規定されるデータ主体の権利を行使するための要請に応じる顧客の義務の履行を目的として、可能な限り、適切な技術的および組織的対策をもって顧客を支援する。
(2) 当社は、GDPR 第 12 条ないし第 23 条に規定されるデータ主体の権利(特に個人データにアクセスする権利、訂正の権利、消去の権利(「忘れられる権利」)、取扱制限の権利、データポータビリティの権利、異議を述べる権利、または個人に対する自動化された意思決定の対象とならない権利に関するもの)を行使するための要請について、遅滞なく顧客に通知する。
(3) 主たる契約および本 DPA に記載する取扱いの性質ならびに当社において入手可能な情報を考慮の上、当社は、顧客が GDPR 第 32 条(取扱いの安全管理)、第 33 条(個人データ侵害に対する監督機関への通知)、第 34 条(個人データ侵害に対するデータ主体への通知)、第 35 条(データ保護影響評価)および第 36 条(事前協議)の義務を遵守することについて、顧客の費用負担により顧客を支援する。

第 8 条　削除

取扱いに関するサービスの提供終了後、顧客の選択に従い、顧客のすべての個人データは、削除または返却される。顧客は、ここに、EU またはその加盟国の法令が個人データの保存を義務付ける場合をのぞき、取扱いに関するサービスの提供終了後、顧客のすべての個人データを削除し、かつ存在するコピーを削除するよう当社に指示する。

第 9 条　情報および監査の権利

(1) 主たる契約に基づく取扱いに関して、当社は、顧客が書面をもって要請する場合、GDPR 第 28 条に定める義務の遵守の立証に必要なすべての情報を顧客に提供する。
(2) 当社は、GDPR 第 28 条に定める義務の遵守を立証するため、主たる契約に基づく取扱いに関して、顧客が監査(検査を含む)を実施すること(以下「監査等」という)を承諾し、それに協力する。監査等は、顧客が委任する独立した第三者たる監査人によって実施することも可能とするが、その場合、当該監査人が当社にとって承諾可能な者であり、主たる契約に基づき顧客に適用される秘密保持義務と同等以上の秘密保持義務に拘束されることを条件とする。顧客は、当社に対し、合理的な事前の通知をもって、監査等を要請する。監査等に先立ち、両当事者は、その範囲、時期および監査期間について合意するものとする。顧客は、監査等に関して当社が負担したサービスがあれば、現行有効な当社のサービス料率に基づき、当社に対し、支払いを行うものとする。当該サービス料率は、顧客から要請がある場合、提供されるものとする。
(3) 顧客は、当社に対し、監査等の範囲および結果に関する社外秘の要約を含む報告書をすみやかに提供する。前記にかかわらず、当社は、自身の目的のために当該報告書を使用する権利を有する。

SIEMENS Healthineers

付属書類“TOM”：Technical and Organizational Measures (“TOM”) Siemens Healthineers

1. 個人データの仮名化および暗号化
当社は、追加情報なしに、取扱い後のデータを特定個人と識別し、または識別され得ることができないよう、個人データを、取扱い後のデータとは分離して、安全に保管する。当社は、対称鍵または非対称鍵を用いて個人データを暗号化する。

2. システムおよびサービスの秘密保持、完全性、利用可能性および復元力

a) 当社は、以下の対策を講じることにより、秘密保持および完全性を確保する。

アクセス制御：

当社は、自身の建物を、そのセキュリティ区分および適切に定められたアクセス承認概念に基づく適切なアクセス制御システムをもって保護する。すべての建物は、カード読み取りシステムを用いたアクセス制御対策により保護される。セキュリティ分類に従い、財産、建物または個々のエリアが追加の対策により保護される。これらには、特別なアクセスプロファイル、生体認証、ピンパッド、DES ドングル、分離ロック、ビデオ監視および保安要員が含まれる。承認を受けた者のアクセス権は、規定の基準に従い、個別に付与される。これは、外部の者にも適用する。

システムへのアクセス制御：

データ取扱システムへのアクセス権は、以下の対策を用いる、役割ベースによる承認概念に基づき認証されたユーザーに限り付与される：ネットワーク内および個人の PC ならびにモバイル機器上におけるデータの暗号化、個別化パスワード（8 文字以上とし、定期的に自動終了する）の割当、PKI 暗号化機能付き従業員 ID カード、動作していない状態ではパスワードで保護されるスクリーンセーバー、侵入検知システムおよび侵入防止システム、定期的に更新されるアンチウィルスおよびスパイウェアのフィルター

データへのアクセス制御：

個人データへのアクセス権は、役割ベース承認概念に基づき付与される。ユーザー管理システムは、各ユーザーの承認を含むユーザーデータベースを特定するよう配置されており，データ取扱システムにリクエストすることによりネットワーク内で集中的に検索に利用できる。更に、データの暗号化により個人データへの不正アクセスを防止する。

データの送信制御：

当社は、クローズドネットワークおよびデータ暗号化手順を設定することにより、安全な電子通信経路を確保する。物理データ記憶媒体を輸送する場合、データへの不正アクセスまたは物理的紛失を防ぐために、検証可能な輸送手順が実施される。データ記憶媒体は、データ保護規則に従い処分される。

b)当社は、以下の対策を講じることにより、システムおよびサービスの継続的な利用可能性ならびに信頼性を確保する：

当社は、十分なバックアップおよびシステムの冗長化を実施し、電源システムの冗長化を実施し、かつ定期的にシステムおよびサービスをテストすることにより、重要な IT およびネットワークのコンポーネントを隔離し、システムおよびサービスの利用可能性ならびに復元力を確保する。テストおよび作動中のシステムは、完全に分離される。

3. インシデント発生時における個人データの利用可能性および個人データへのアクセス
当社は、物理的または技術的なインシデントが発生した場合、以下の対策を講じることにより個人データの利用可能性および個人データへのアクセス権を復旧する：

当社は、セキュリティマーキングに従い、RAID システムに個人データを保存し、冗長化システムを統合する。当社は、データセンター内の電力供給を確保するため、連続電力供給用のシステム（UPS、バッテリー、発電機等）を使用する。

データベースまたはデータセンターは、物理的に異なる場所に対に置かれる。

包括的な緊急対策書類が作成される。緊急時の手順およびシステムは、定期的に見直される。

4. 取扱いの安全性確保のための制御手順
当社は、取扱いのセキュリティ確保のための技術的および組織的対策の有効性を定期的に見直し、判断し評価するため、連邦情報セキュリティ庁(BSI)の基本 IT 保護カタログおよび ISO/IEC 27001 の要件を考慮して、リスク管理手法に基づく制御手順を実施する。これにより、該当する情報、アプリケーション（品質および安全性の検査手法を含む）、動作環境（有害性に対するネットワークのモニタリング等）の保護および保護手法の技術的実施（脆弱性分析等の方法による）を確保する。脆弱性を系統的に検知し排除することにより、保護対策を継続的に再検証し、改善する。

5. 従業員に対する対策
当社は、個人データが、法令、本 DPA および顧客による関連の指示（本 DPA に記載する技術的および組織的対策を含む）を遵守してのみ取り扱われることを確保するため、作業指導書を作成し、個人データへのアクセス権を有する従業員に対し、定期的にトレーニングを実施する。

Confidential