**データ処理契約**

1. *定義:* 　本データ処理契約 (以下「DPA」という。) では、次の用語は次の意味を持つものとします。

* 「適切な国」　欧州委員会、情報コミッショナー事務局、または連邦データ保護および情報コミッショナー (該当する場合) が、それぞれの管轄分野について適切なレベルの保護を確保していると判断した国。
* 「適用されるデータ保護法」 該当する場合、米国データ保護法、EU データ保護法、英国データ保護法、およびスイスデータ保護法を含む、適用されるデータ保護およびプライバシー法。
* 「管理者」、「処理者」、「データ主体」、「個人データ」、「処理」(および「処理」)、および「個人データの特別なカテゴリ」は、適用されるデータ保護法に規定されている意味を有するものとします。
* 「EEA」とは、欧州経済領域を意味します。
* 「US」とは、アメリカ合衆国を意味します。
* 「EC」とは、欧州委員会を意味します。
* 「EU データ保護法」 (a) EU 一般データ保護規則 (規則 2016/679) (GDPR)、 (ii) EU e-プライバシー指令 (指令 002/58/EC)、および (iii) 上記のいずれかに基づいてまたは上記のいずれかに従って制定されたすべての EU 加盟国の法律。いずれの場合も随時修正されるまたは置き換えられます。
* 「スイスのデータ保護法」 1992 年から 2022 年 12 月まではスイス連邦データ保護法 (FADP)、2023 年 1 月 1 日以降は 2020 年改正スイス連邦データ保護法 (改訂 FADP) 、随時修正されるまたは置き換えらます。
* 「英国データ保護法」は、欧州連合 (2018 年撤回法) のセクションに従い、随時修正されるまたは置き換えられる、2018 年データ保護法 (英国 DPA) および英国の GDPR (Retained Regulation (EU) 2016/679 (UK GDPR)の条件によって補足された、2019年データ保護、プライバシー、および電子取引 (改正等) (EU 離脱) 規則 2019/419 によって採択されたデータ プライバシー法。
* 「米国データ保護法」 (a)、2020 年カリフォルニア州プライバシー権法 (CPRA) により修正かつ統合された、及び施行規則に従う2018 年カリフォルニア州消費者プライバシー法 (CCPA)、(b) 2021 年バージニア州消費者データ保護法 (VCDPA)、 (c) 2021 年コロラド州プライバシー法 (CPA)、 (d) 2022 年コネチカット データ プライバシー法 (CTDPA)、および (e) 2022 年ユタ州消費者プライバシー法 (UCPA)、いずれの場合も随時修正されるまたは置き換えられます。
* 「Hydrafacial」とは、Hydrafacial LLC を意味します。
* 「デバイス」とは、Hydrafacial Syndeo デバイス、システム、およびソフトウェアを意味します。
* 「消費者」、デバイス治療を受ける者。
* 「コスチューマ」、デバイス治療を提供するクリニックまたはセンター。
* 「認定ユーザー」とは、お客様、その関連会社、およびデバイス治療を行うそれぞれの従業員、請負業者またはコンサルタントを意味します。

1. *両当事者間の関係:* 　Hydrafacial (管理者) は、本 DPA の第 16 項に記載されている目的または両当事者が書面で合意したその他の目的 (「許可された目的」) のために、本 DPA の第 14 項に記載されている個人データ (以下「データ」という。) を処理するお客様 (処理者) を指名します。お客様は、許可された目的以外の目的でデータを保持、使用、または開示してはなりません。お客様は、データを売買してはなりません。 各当事者は、適用されるデータ保護法に基づくそれぞれの義務を遵守するものとします。
2. *国際転送およびデータローカリゼーションに関する法律:* 　お客様およびその認定ユーザーがデバイスを介して入力およびアクセスするデータは、米国でホストされ、 [\*SCCへリンク\*] (以下「SCC のウェブページ」という。) で承認された該当する標準契約条項 (以下「SCC」という。) は、適用されるデータ保護法を遵守するために、この DPA に組み込まれているとみなされるものとします。 お客様が完全に締結されたバージョンを必要とする場合は、SCC のウェブページで該当する署名済みバージョンに副署し、コピーを dpo@hydrafacial.com に電子メールで送信することができます。データローカライゼーション法により、データの保存と転送に関する法的制限が適用される EEA 域外の国 (以下「第三国」という。) では、データは地域外に転送またはホストされることはなく、現地のサーバーに保存されます。データを米国に転送する前に、Hydrafacial は、転送されたデータが郡または転送元で提供されるものと実質的に同等の保護レベルに服することを保証するための合理的な措置を講じました。英国 (以下「英国」という。) またはスイスから発信されたデータについては、このセクション 3 で、(a) 「EEA」は、該当する場合、「英国」または「スイス」に置き換えられるものとする、 (b) 「EU データ保護法」は、該当する場合、「英国データ保護法」または「スイス データ保護法」に置き換えられるものとする、及び (c) 「EC」は、該当する場合、「情報コミッショナーのオフィス」または「連邦データ保護及び情報コミッショナー」に置き換えられるものとすること、と言及されています。
3. *セキュリティと機密保持:* 　処理の性質を考慮して、Hydrafacial とお客様は、(i) 偶発的または違法な破壊からデータを保護するため、および (ii) データの損失、改ざん、不正な開示、またはデータへのアクセス (以下「プライバシー侵害」という。) からデータを保護するために、リスクに適したレベルのセキュリティを確保するための適切な技術的および組織的措置を講じるものとします (EU 一般データ保護規則の第 32 条に規定されているとおり)。お客様は、データを処理する認定ユーザーが機密保持に明示的に同意していることを確認するものとします。
4. *サブプロセシング:*　適用されるデータ保護法の下で、認定ユーザーがサブプロセッサと見なされる可能性がある処理の性質を考慮して、お客様は少なくとも、許可された目的のためにのみ、本 DPA に規定されている要件と条件を確実に遵守するものとします。
5. *協力とデータ主体の権利:*　 処理の性質を考慮して、処理者は可能な限り、適切な技術的および組織的措置によって管理者を支援するものとし、および必要に応じて、お客様は、Hydrafacial が、(i) 適用されるデータ保護法に基づくデータ主体からの権利の行使の要求 (該当する場合、アクセス、修正、異議、消去、データポータビリティの権利を含む)、および (ii) データの処理に関連して、データ主体、規制当局、またはその他の第三者から受け取ったその他の通信、要求、または苦情に対応できるように、合理的かつタイムリーな支援を提供するものとします。かかる要求、通信、問い合わせ、または苦情がお客様に直接行われた場合、お客様は速やかにその詳細を Hydrafacial に通知するものとします。
6. *評価、コンサルテーションおよび支援*:　 処理の性質を考慮して、必要に応じて、お客様は, Hydrafacial が、(a) データ保護または転送の影響評価を実施する、および (b) 適用されるデータ保護法で要求される場合、処理の前に管轄の監督当局に相談することができるように協力するものとします。
7. *プライバシーの侵害:*お客様がプライバシー侵害に気付いた場合、お客様は直ちに Hydrafacial に通知し、Hydrafacial が適用されるデータ保護法に基づく違反通知義務を遵守できるように、合理的な情報と協力を Hydrafacial に提供するものとします。お客様はまた、データ侵害の影響を軽減するために合理的に必要な措置およびアクションをとるものとし、データ侵害に関連するすべての重大な進展についてお客様に情報を提供し続けるものとします。同じ要件がサブプロセッサにも適用されます。
8. *データの削除又は返却:* 　お客様は、契約の終了時に、データの非保持の証明書を Hydrafacial に提供するよう求められる場合があります。
9. *適合性の確認:* お客様は、本データ処理契約に定められた義務を確実に遵守するために、Hydrafacial (またはその被指名者) による手順および文書の検査または監査を許可するものとします。
10. *透明性レポート:* Hydrafacial は、法律で義務付けられている場合を除き、政府当局にデータを開示する又はデータへのアクセスを提供することはありません。データに関連する公的機関からの要求 (以下「法的要求」という。) に対処するための Hydrafacial のポリシーは、法的要求に関する Hydrafacial の透明性レポートと共に、[\*リンク\*]で入手できます。 Hydrafacial は、(a) 法的要求の合法性を検討し、合法かつ適切である場合は異議を申し立て、および (b) 法的要請が GDPR の第 46 条または個人データの合法的な転送に関するその他の関連条項に準拠していない場合は、そのことを公的機関に通知します (いずれの場合も、法的要請に適用される適用データ保護法で要求される範囲でとします)。

**付属書I – 情報セキュリティ管理**

1. *セキュリティ管理:*
2. Hydrafacial は、プライバシーおよびセキュリティプログラムをサポートするために、次のポリシーと手順を維持します。

* 情報セキュリティに関するポリシー: ビジネス要件および関連法令及び規制に従って、情報セキュリティに関する管理上の指示とサポートを提供するため。
* 情報セキュリティの組織: 　Hydrafacial での情報セキュリティの実装と運用を開始および管理するためのフレームワークを確立するため。
* 人的資源のセキュリティ: すべての従業員が自分の役割と責任に適しており、理解していることを確実にするため。すべての従業員が情報セキュリティの責任と義務を認識して履行するため。雇用前から雇用終了まで雇用プロセス全体を通じて組織の利益が確実に保護されるようにするため。すべての従業員が守秘義務を負うことを確実にするため。
* データの分類: Hydrafacial の情報とデータの分類を特定し、それらを確実に保護するために適切な責任を定義して割り当てるため。機密レベルと組織にとっての重要性に応じて、情報とデータを適切なレベルで確実に保護するため。メディアに保存されている情報の不正な開示、変更、削除、または破壊を防止するため。
* アクセス管理: ユーザー、システム、アプリケーションのアクセス制御と管理、およびユーザーの責任のためのフレームワークを提供します。情報および情報処理施設へのアクセスを制限するため。許可されたユーザー アクセスを確保し、システムやサービスへの不正アクセスを防ぐため。認証情報を保護する責任をユーザーに負わせるため。システムやアプリケーションへの不正アクセスを防止するため。
* 物理的および環境的セキュリティ: Hydrafacialの情報および情報処理施設への不正な物理的アクセス、損傷および干渉を防止するため。Hydrafacial の資産の損失、損傷、盗難、侵害、およびその運営の中断を防止するため。
* 運用上のセキュリティ: 情報および情報処理施設が安全に運用され、マルウェアやデータの損失から保護されていることを確実にするため。セキュリティイベントが適切に記録されることを確実にするため。運用システムの完全性が維持され、技術的な脆弱性の悪用が回避されることを確実にするため。
* 通信セキュリティ: ネットワークおよび関連施設内の情報を保護するための制御を確立するため。Hydrafacial 内および外部関係者と転送される情報のセキュリティを確保するため。
* サプライヤーとの関係: サプライヤーがアクセスできる Hydrafacial 資産の保護を確保するため。サプライヤーとの合意に従って、合意されたレベルの情報セキュリティとサービス提供を維持するため。
* 情報セキュリティのインシデント管理: インシデントや脆弱性を含む情報セキュリティイベントを管理するための一貫した効果的なアプローチを確保するため。
* リモートアクセス用の VPN (仮想プライベートネットワーク): ユーザーが ウェブベースのサービスやサイトに接続するときに、セキュリティと匿名性を追加します。VPN は、ユーザーの実際のパブリック IP アドレスを隠し、ユーザーのデバイスとリモートサーバー間のトラフィックを「トンネリング」します。
* 保存中および転送中のデータの暗号化: 　移動中のデータとも呼ばれます。保存中のデータとは、デバイス間またはネットワーク間を移動しない非アクティブなデータを指し、データアーカイブに保存される傾向があります。一方、転送中のデータは、デバイス間または 2 つのネットワークポイント間を移動しています。
* バックアップと復元の機能: データを複製し、紛失や損傷に備えて安全な場所に保管し、そのデータを元の場所または安全な代替場所に復元して、再びオペレーションで使用できるようにするプロセスです。
* ファイアウォール: 　組織の以前に確立されたセキュリティポリシーに基づいて、受信および送信ネットワークトラフィックを監視およびフィルタリングするネットワーク セキュリティ デバイスです。 最も基本的なこととして、ファイアウォールは本質的に、プライベートな内部ネットワークと公共のインターネットの間にあるバリアです。
* アンチウイルスソフトウェア: コンピュータからウイルスを防止、スキャン、検出、および削除するために使用される一種のソフトウェアです。
* 多要素認証 (MFA): ログインまたはその他のトランザクションでユーザーの身元を確認するために、資格情報の独立したカテゴリから複数の認証方法を必要とするセキュリティ技術です。
* 電子メールセキュリティフィルタリング: ユーザーを不審なウェブサイトにリダイレクトする、望ましくない、または潜在的に悪意のあるコードまたはリンクをブロックするプロセスです。システムに侵入して機密データにアクセスしようとする電子メールを防ぎます。
* セキュリティ意識向上トレーニング:　組織のメンバーが、その組織の物理的資産の保護、特に情報資産の保護に関して持つ知識と態度です。

1. お客様は、適用されるデータ保護法に従って、不正または違法な処理に対する保護、および偶発的な損失、破壊、または損害に対する保護を含む、適切な技術的または組織的措置を講じるものとします。

**付属書Il – データ処理の詳細**

1. データ主体のカテゴリ: (i) 消費者、 (ii) 認定ユーザー、 (iii) コスチューマ
2. 処理されたデータのカテゴリ: (i) 氏名、電話番号、電子メール アドレス、役割、IP アドレスなどの、データ主体の連絡先およびアカウント情報、 (ii) 治療歴と実績
3. 特別なカテゴリのデータ: デバイス内で処理される特別なカテゴリのデータはありません。
4. 処理操作の目的: 個人データは、デバイスサービスの提供に必要な場合に処理されます。処理された個人データは基本的な処理活動である収集、通信による開示、およびコンサルテーションの対象となる場合があります。特に、処理操作には (i) 消費者がアカウントの作成を希望する場合、消費者が SMS/電子メールを受信して登録プロセスを完了するように、お客様と認定ユーザーはデバイス システムに詳細を入力することを含みます。(ii) 消費者は、治療履歴をお客様および認定ユーザーと共有するオプションがあります。同様に、デバイスを使用する場合、お客様と認定ユーザーは、プロバイダーの治療履歴の記録を保持するために、アプリケーションアカウントをデバイスと同期させるオプションを有します。お客様および認定ユーザーは、提供した治療に関する集計された治療データを閲覧できます。また、お客様および認定ユーザーが閲覧する治療に、消費者である個人を特定できる情報が関連付けられることはありません。
5. 処理期間: 個人データは、Hydrafacial デバイスサービスとの契約期間中処理されることがあります。