別紙3 個人情報の取扱いに関する覚書（雛形）

（委託者）　　（以下「甲」という）と株式会社MedSelf（以下「乙」という）は、甲乙間の産業医業務委託基本契約（以下「原契約」という）に基づき乙が取り扱う個人情報について、次のとおり合意する。

第1条（目的と定義）

1. 本覚書は、乙が原契約に基づく業務（以下「本業務」という）の実施に伴い、甲から委託を受けて取り扱う個人情報の安全管理について定める。

2. 「個人情報」「個人データ」「要配慮個人情報」は、個人情報の保護に関する法律（以下「法」という）の定義による。本業務で取り扱う健康に関する情報は要配慮個人情報にあたる。

第2条（取り扱う個人情報の範囲）

乙が取り扱う個人情報は別表1に定める。甲は別表1に定めのない個人情報を乙に提供しない。乙は、本業務に必要のない個人情報の提供を受けたときは、甲に通知し、甲の指示に従い返却または削除する。

第3条（利用目的の限定）

乙は、個人情報を本業務の実施、甲からの照会への対応、および乙の法的義務の履行の目的に限って取り扱い、目的外に利用しない。乙は、個人情報を乙の他の事業（医療機関の運営を含む）の目的に利用しない。

第4条（安全管理措置）

乙は、個人情報の漏えい、滅失、毀損の防止その他の安全管理のため、次の措置を講じる。

(1) 組織的措置：責任者の設置、取扱規程の整備、取扱状況の点検

(2) 人的措置：従業者および乙が契約する医師に対する秘密保持義務の課与と教育

(3) 物理的措置：電子媒体の暗号化、紙媒体の不作成または返却・廃棄、執務環境の管理

(4) 技術的措置：役割に基づくアクセス制御、本人認証、通信および保存時の暗号化、追記型の操作記録、脆弱性の検査と是正、文書のファイル名・フォルダ名における案件識別子による管理（識別子と氏名の対応表の分離保管。文書本文には業務上必要な氏名等を含む）

(5) 外的環境の把握：個人情報を保管する外部サービスの所在国・地域の把握と、当該国の制度の確認

第5条（従業者および委託医師の監督）

乙は、個人情報を取り扱う従業者および乙が契約する医師に対し、本覚書と同等の義務を課し、必要かつ適切な監督を行う。

第6条（再委託）

1. 乙は、本業務の一部を乙が契約する医師に再委託することができる。この場合、乙は事前に当該医師の氏名および資格を甲に通知する。

2. 乙は、個人情報の保管および処理のため、別表2に掲げる外部サービスを利用する。別表2の追加・変更は、乙が事前に甲に通知する。甲は正当な理由がある場合、異議を述べることができる。

3. 前2項以外の再委託は、甲の事前の書面による承諾を要する。

4. 乙は、再委託先に本覚書と同等の義務を課し、再委託先の行為について甲に対し責任を負う。

第7条（外国にある第三者）

1. 乙は、別表2の外部サービスの利用が法第28条の「外国にある第三者への個人データの提供」に該当するかを、各サービスの所在と契約内容（当該事業者が個人データを取り扱わない旨の定めの有無を含む）に基づいて整理し、その結果を甲に報告する。

2. 前項の整理により提供に該当する場合、乙は法第28条に基づき必要な措置（本人の同意の取得、または基準に適合する体制の整備と本人への情報提供）について甲と協議し、これに協力する。

3. 別表2の「保管リージョン」欄には所在を記載し、確認できていない項目は「確認中」と記載する。乙は確認の結果を速やかに甲に通知する。

第8条（漏えい等の報告）

1. 乙は、個人情報の漏えい、滅失、毀損またはそのおそれを知ったときは、知った時点から速やかに、遅くとも72時間以内に甲に通知する。

2. 乙は、原因、範囲、影響、講じた措置および再発防止策を甲に報告し、法第26条に基づく個人情報保護委員会への報告および本人への通知について甲に協力する。

3. 乙から甲への前2項の通知は、個人情報の保護に関する法律施行規則第8条第2項に定める委託先から委託元への通知として行う。

第9条（報告と確認）

1. 甲は、乙における個人情報の取扱状況について、合理的な範囲で報告を求め、または事前に協議のうえ確認（書面による質問、オンラインでの説明を含む）を行うことができる。乙はこれに協力する。

2. 甲は、必要があるときは、事前に協議のうえ合理的な範囲で乙の執務場所への立入による確認を行うことができる。執務場所の事情により立入が困難な場合、乙はオンラインでの確認により代替する。

第10条（保管期間、返却および削除）

1. 乙は、別表1に定める保管期間、個人情報を保管する。

2. 原契約の終了時または甲の求めがあるとき、乙は保管する個人情報を企業単位で棚卸しし、返却物の一覧を甲に提示し、甲の受領確認の後に乙の保管分を削除する。

3. 削除の事実、対象の識別子のハッシュ値、実施者および日時は、乙の記録として残る。乙は、削除の実施を甲に報告する。

4. 医師のみが参照する記録および本人の同意なく提供できない情報は返却物に含めない。乙はこれらを第3項と同じ方法で削除する。

第11条（本人からの請求）

乙が本人から開示、訂正、利用停止または消去の請求を受けたときは、乙は甲に通知し、法定保存義務の及ぶ期間かを含めて甲の判断を得たうえで、甲の指示に従い対応する。

第12条（有効期間）

本覚書は原契約と同時に効力を生じ、原契約の終了後も、乙が個人情報を保管する間、効力を有する。

令和　年　月　日

甲：

乙：東京都港区新橋一丁目18番21号　第一日比谷ビル　株式会社MedSelf　代表取締役　宮部大輔

別表1　取り扱う個人情報と保管期間

区分	項目	取得元	保管期間
企業担当者	会社名、氏名、メールアドレス、電話番号（予約時は必須）	甲	原契約終了まで
対象者（労働者）	氏名（予約時に企業担当者が入力）、社員番号、所属、職種、勤務状況、業務内容、面談の目的	甲	面談実施日から5年
甲が提供する資料	面談の目的に必要な範囲の、健康診断結果の写し、主治医の診断書・意見書の写し、勤務情報提供書等（文書として受託保管する）	甲	同上
対象者（労働者）	面談における本人の申述、医師の所見（医師のみが参照する記録を含む）	本人・医師	同上
意見書	就業の可否、就業上の措置の要否と内容、期間、再評価の時期、理由として必要な範囲の情報	医師	同上
決済	決済の識別子、金額、日時（カード情報は乙が取り扱わない）	決済事業者	法定の帳簿保存期間

予約画面では入力を受け付けないもの：病名・症状の自由記述、診断書の本文、対象者のメールアドレス。予約画面の入力項目として健康診断の検査値は取得せず、甲が提供する写しを文書として保管する。

別表2　個人情報の保管・処理に利用する外部サービス

サービス	用途	取り扱う情報	所在（保管リージョン）	契約・DPA
Microsoft Azure	実行基盤・データベース・監視	個人情報・要配慮個人情報	確認中	確認中
Box	文書保管	面談記録・意見書	確認中	確認中
Cal.com	予約管理	担当者の氏名・メール、予約日時、面談種別	確認中	確認中
Microsoft Entra ID／Graph	認証	識別情報	確認中	確認中
Microsoft Teams（予定）	オンライン面談	音声・映像（録画等の取扱いは個別に案内）	確認中	確認中

サービス	用途	取り扱う情報	所在（保管リージョン）	契約・DPA
Stripe	カード決済・請求書の発行と銀行振込の受付	決済情報（カード情報は乙を通らない）・請求先の会社名・宛名・メールアドレス	確認中	確認中
SendGrid／Gmail	通知メール	担当者の氏名・メール、通知本文（対象者の氏名・面談種別を含むことがある。診断などの健康情報の本文は含めない）	確認中	確認中
企業間後払い決済	導入準備中・現在は未利用	-	-	-
マネーフォワード クラウド請求書／CloudSign	請求書発行・電子契約（基本契約・月末締め払いの場合）	企業情報・請求情報・契約書	確認中	確認中