情報セキュリティ・個人情報の取扱い

0. 前提（先方に最初に伝える）

- 本サービス（SPOT産業医面談）で当方が取り扱う情報は、①企業担当者の会社名・氏名・メールアドレス・電話番号（予約時は必須）、②面談する方の氏名（予約時に企業担当者が入力します。従業員のメールアドレスは収集しません）、③医師の面談記録、④意見書、⑤決済に関する情報（カード情報は決済代行会社が扱い、当方を通りません）です。

- 予約画面の入力項目として健康診断の検査値は取得しません。貴社が面談の目的に必要な範囲で提供する健康診断結果の写し・主治医の診断書や意見書の写し・勤務情報提供書は、文書として受託保管します（記録の正本は貴社）。医師のみが参照する記録は、企業向けの出力に含まれません。

- 法定の記録保存義務を負うのは事業者（貴社）です。当方の保管は受託によるもので、記録の正本は貴社にあります。

1. 組織的安全管理措置

質問	回答
情報セキュリティの責任者	代表取締役（医師）が情報セキュリティおよび個人情報保護の責任者です。
規程の有無	情報セキュリティ方針、データ分類、アクセス制御、監査ログ、インシデント対応・復旧の手順を文書化しています。方針・適用範囲には承認手続きが未了のものがあります。
第三者認証	ISO/IEC 27001、プライバシーマーク、SOC 2は取得していません。
内部監査・点検	内部監査・マネジメントレビューの実施は未了です。
事故対応体制	インシデント対応手順を定め、漏えい等を知ったときは速やかに、遅くとも72時間以内に委託元へ通知します。机上訓練は未実施です。

2. 人的安全管理措置

質問	回答
従業者の守秘義務	業務を行う医師は刑法第134条および労働安全衛生法第105条に基づく秘密保持義務を負います。当方が医師を追加する場合、契約で同等の秘密保持義務と個人情報取扱義務を課します。
教育	健康情報の取扱いと事故時の報告手順を周知する方針です。教育の実施記録は整備中です。
業務を行う者の範囲	対応医師は3名です。企業の担当者が他社の情報を見ることはできません（会社単位のアクセス制御）。

3. 物理的安全管理措置

質問	回答
紙媒体	面談記録・意見書は電子で作成し、紙に出力しません。貴社から紙で受領した資料は電子化後に返却または溶解します。
端末	ディスク暗号化、画面ロック、OS更新、紛失時の遠隔消去を運用ルールとしています。実機ごとの設定確認は継続中です。

質問	回答
執務場所	面談はオンラインで、医師が第三者の立ち入らない場所から行います。

4. 技術的安全管理措置

質問	回答
アクセス制御	役割（運営・医師・企業担当者）ごとに参照できる範囲を定め、企業担当者は自社の案件のみ、医師は担当する案件のみを参照できます。医師のみが参照する記録は企業向け出力から除外しています。これらはテストで検証しています。
記録の保管と命名	文書保管（Box）に置く面談記録・意見書は、ファイル名・フォルダ名に氏名を含めず、案件の識別子（ID）で管理します。文書の本文には、業務上必要な範囲で対象者の氏名等を含みます。文書保管へのアクセスは権限を持つ者に限定しています。
認証	SPOT担当者はメールのワンタイムコード（10分有効・試行回数制限）で確認し、注文・会社・担当者を照合します。管理者のEntra ID認証を整備していますが、一部管理APIに共有シークレット認証が残り、多要素認証の全面適用は確認中です。
通信の暗号化	外部通信をHTTPS（TLS）で保護する構成です。Function AppのHTTPS強制は確認済みですが、カスタムドメインごとの現行TLS設定は確認中です。
保存時の暗号化	Azure・Boxの管理サービスによる保存時暗号化を利用する構成です。実リソースの個別設定は確認中です。
監査ログ	主要操作を記録し、追記とハッシュ連鎖による改変検知を実装しています。対象操作の網羅性と保持期間は確認・整備中です。
脆弱性管理	ソースと依存パッケージの検査を行い、検出事項を是正またはリスク管理します。第三者による侵入テストは未実施です。過去の検査結果を現在の安全性の保証には用いません。
開発・配備の統制	変更はプルリクエストと自動テスト・検査を経て、GitHub Actions経由で配備します。開発者端末からの本番直接配備は禁止し、対象システムに応じた管理された資格情報を使用します。
ネットワーク	APIはFront Doorの背後に配置し、データベースにはプライベート接続を用いる構成です。個別の稼働環境の証跡は照会に応じて確認します。
バックアップ	バックアップ・復旧手順を文書化しています。復旧訓練は未実施です。

5. 外的環境の把握（外国にある第三者・クラウド）

サービス	用途	取り扱う情報	保管リージョン	契約・DPAの確認
Microsoft Azure	実行基盤・データベース・監視ログ	個人情報・要配慮個人情報（健康情報）・運用ログ	確認中	確認中
Box	文書保管（面談記録・意見書・資料）	要配慮個人情報を含む文書	確認中	確認中
Cal.com	面談の予約管理	氏名・メールアドレス・予約日時・面談種別	確認中	確認中
Microsoft Entra ID / Graph	認証・アカウント管理	識別情報	確認中	確認中

サービス	用途	取り扱う情報	保管リージョン	契約・DPAの確認
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
Stripe	カード決済・請求書の発行と銀行振込の受付	決済情報（カード情報は当方を通らない）・企業担当者情報・請求先の会社名・宛名・メールアドレス	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（基本契約の場合）	企業情報・請求情報・契約書	確認中	確認中
SendGrid／Gmail	メール送信（予約通知・意見書の閲覧案内）	企業担当者の氏名・メールアドレス、通知本文（対象者の氏名・面談種別を含むことがある。診断・検査値などの健康情報の本文は含めない）	確認中	確認中
GitHub	ソースコード・配備・証跡成果物	ソースコード・設定（顧客の個人情報は含まない）	確認中	確認中
Slack	運用通知	運用メタデータ（個人情報を含めない）	確認中	確認中

健康情報、または健康に関わる情報（面談の種別など）を保管・通過するのは、文書保管（Box）、実行基盤（Microsoft Azure）、予約管理（Cal.com：面談の種別）、オンライン面談（Microsoft Teams：面談の音声・映像）、メール送信（SendGrid：意見書の閲覧案内に対象者の氏名・面談種別。診断などの本文は含めません）です。保管リージョンと契約（DPA）の確認状況は上表のとおりで、確認できていない項目は『確認中』とお伝えします。確認前に『国内保管』とは申しません。

6. 委託先管理（再委託）

質問	回答
再委託の有無	当方が契約する医師に面談を再委託することがあります。事前に氏名・資格を通知し、同等の義務を課し、当方が責任を負います。情報システムとして上表のクラウドサービスを利用します。それ以外への再委託は貴社の事前承諾を要します。
再委託先の監督	契約・一覧による管理と、サービスの監視を行います。

7. 個人情報の取扱い

質問	回答
取得する項目	0章のとおり。予約画面の入力項目として健康診断の検査値は取得しません。貴社が面談の目的で提供する資料の写しは、文書として受託保管します。
利用目的	面談の実施、意見書の作成・提供、貴社からの照会への対応、当方の法的義務の履行に限ります。
本人への提供・同意	面談で知り得た本人の秘密は、本人の同意または法令に基づく場合を除き、貴社を含む第三者に開示しません。貴社に提供するのは、就業上の措置に関する意見と、その理由として必要な範囲の情報です。

質問	回答
保管期間	面談記録・意見書は、面談実施日から5年間（労働安全衛生法の面接指導記録の保存期間に合わせる）、文書保管（Box）で保管します。期間満了時は年1回の棚卸しで貴社と協議のうえ削除します。
契約終了時の返却・削除	会社単位で棚卸しし、返却・削除を調整する方針です。企業単位の一括削除、Boxのごみ箱を含む削除手順は確認・整備中で、完全消去を保証しません。
本人からの開示・消去の請求	窓口で本人性と保存義務を確認し、委託元企業と調整します。本人確認様式は整備中です。

8. 事業継続

質問	回答
障害時の連絡	面談ができない場合は速やかに担当者へ連絡し、日程を再調整するか全額返金します。
代替手段	会議障害時は企業担当者と再調整します。電話への切替えを自動的に行うものではありません。
医師の不在	対応医師は3名です。医師の都合で面談ができない場合は日程を再調整するか、全額返金します。