（別紙）　PHRサービス提供者による健診等情報の取扱いに関する基本的指針に係るチェックシート

確 認 日	2025/9/1
組織名	サービス開発部
担当者名	日吉　永瑞　※ 公表時は役職名でも可

1．PHRサービス提供者への該当確認

「PHRサービス提供者による健診等情報の取扱いに関する基本的指針（以下「本指針」という）」について、「1．1．本指針対象とする情報の定義」及び「1．2．本

1．1．本指針の対象とする情報の定義

個人が自らの健康管理に利用可能な「個人情報の保護に関する法律」（平成15年法律第57号。以下「個人情報保護法」という。）上の要配慮個人情報で次に掲げ
・個人がマイナポータルAPI等を活用して入手可能な健康診断等の情報

1．2．本指針の対象者

利用者に対して、直接的もしくは間接的に健診等情報を取り扱うPHRサービスを提供する者（以下「PHRサービス提供者」という。）であること
※専ら個人が自ら日々計測するバイタル又は健康情報等のみを取り扱うPHRサービスを提供する者は、PHRサービス提供者としては含めない。

2．情報セキュリティ対策

2．1．安全管理措置

（1）法規制に基づく遵守すべき事項

項目番号	内容	チェック	対応内容詳細（公表不要）
①	**個人情報保護法に基づく適切な取扱い**		
	健診等情報を取り扱うに当たって、その漏えい、滅失又は毀損の防止その他の安全管理のために必要かつ適切な措置を講じていますか	✔（対応済）	講じている。
②	**その他の法令等に基づく適切な取扱い**		
	上記①のほか、機密情報、知的財産等、法令又は契約上適切な管理が求められている情報については、その法令・契約等に基づいて、必要な措置を講じていますか	✔（対応済）	遵守すべき法令・レギュレーション一覧を管理しており、毎年変化点の確認を行い、追加対策の検討を含め、必要な措置を講じている。

（2）本指針に基づく遵守すべき事項

① 情報セキュリティに対する組織的な取り組み

項目番号		内容	チェック	対応内容詳細（公表不要）
A)	**提供するサービスの目的・範囲等が明らかにされている**			
	1	セキュリティ対策の対象となる情報を明確化し、求められる適切なセキュリティレベルを設定するため、PHR サービス提供者が利用者に提供するサービスの目的や範囲を、組織内に対して明確化していますか	✔（対応済）	利用者に提供するサービスの目的と範囲を組織内に対して明確にしており、必要なセキュリティ対策を行っている。また、利用者に提示する内容を利用規約及びセキュリティホワイトペーパーにて明確にしている。
B)	**情報セキュリティに関する経営者の意図が従業員に明確に示されている**			
	1	経営者が情報セキュリティポリシーの策定に関与し、実現に対して責任を持っていますか	✔（対応済）	持っている。
	2	情報セキュリティポリシーを定期的に見直していますか	✔（対応済）	最低年1回見直しを行っている。
C)	**情報セキュリティ対策に関わる責任者と担当者を明示する**			
	1	責任者として情報セキュリティ及び経営を理解する立場の人を任命していますか	✔（対応済）	情報セキュリティ委員長を任命している。
	2	責任者は、各セキュリティ対策について（社内外を含め）、責任者及び担当者それぞれの役割を具体化し、役割を徹底していますか	✔（対応済）	情報セキュリティ委員会を組織し、その中で各メンバーの役割を具体化している。
	3	利用者向けの問い合わせ窓口を整備していますか	✔（対応済）	問い合わせ窓口は設けている。
D)	**管理すべき重要な情報資産を区分する**			
	1	管理すべき健診等情報を他の情報資産と区分していますか	✔（対応済）	DBの項目にて区分している。
	2	情報資産の管理者を定めていますか	✔（対応済）	情報セキュリティ規程にて定められている。
	3	重要度に応じた情報資産の取扱指針を定めていますか	✔（対応済）	情報セキュリティ規程にて定められている。
	4	健診等情報を取り扱う人の範囲を定めていますか	✔（対応済）	システム管理者の任命について、情報セキュリティ規程にて定められている。
	5	健診等情報を複数の部署で取り扱う場合には、各部署の役割分担及び責任を明確化していますか	✔（対応済）	各部署の役割分担及び責任者を明確化している。
E)	**情報資産区分に基づいて、リスク管理をする**			
	1	保有する情報資産に対する脅威を想定しリスクを洗い出していますか	✔（対応済）	保有する情報資産に関して想定される脅威を把握し、リスクの洗い出しを実施している。
	2	情報資産に対するリスクを評価していますか	✔（対応済）	洗い出したリスクについて評価を行っている。
	3	情報資産のリスク評価に応じた方針を決定し、その方針を実現するための対策を講じていますか	✔（対応済）	情報資産のリスク評価に基づき、リスクの水準に応じた方針を策定し、その方針を実現するために必要な対策を講じている。
	4	情報資産に対するリスク管理を行い、定期的にリスク対策を見直していますか	✔（対応済）	情報資産に対して適切なリスク管理を行っており、定期的にリスク対策を見直し、必要に応じて改善を実施している。
F)	**個人情報の取扱状況を確認する手段を整備する**			
	1	例えば次のような項目をあらかじめ明確化しておくことにより、個人情報の取扱状況を把握可能にしていますか 個人情報データベース等の種類、名称及び個人データの項目 / 責任者、取扱部署 / 利用目的 / アクセス権を有する者　等	✔（対応済）	DB定義書にて定義している。サービス毎に責任者が決まっている。 利用目的は利用規約にて明確にしている。 アクセス権を有するものはAWSの管理者権限一覧で管理している。
G)	**健診等情報については、入手、作成、利用、保管、交換、提供、消去及び破棄における取扱手順を定める**			
	1	各プロセスにおける作業手順を明確化していますか	✔（対応済）	各プロセスにおける作業手順の明確化の対応を現在行っております。
	2	決められた担当者が、手順に基づいて作業を行っていますか	✔（対応済）	明確化した手順の中で、決められた担当者が手順を履行するようにしております。
	3	健診等情報に対して、漏えい及び不正利用を防ぐ保護対策を行っていますか	✔（対応済）	最小権限での特権アクセスを行うよう、情報セキュリティ規程にて定められている。 また、AWS上でのすべての操作ログがCloudWatchに保存されている。登録された情報の消去は個人に紐づく情報を除いてはそもそも行っていない。
H)	**外部の組織と情報をやり取りする際に、情報の取扱いに関する注意事項について合意を取る**			
	1	契約書及び委託（再委託等を含む。以下同じ）業務の際に取り交わす書面等に、情報の取扱いに関する注意事項を含めていますか	✔（対応済）	法人との契約は、基本契約と個別契約を締結しており、作業管理責任者・再委託の事前報告なしには禁止・目的外利用の禁止などを定めている。秘密保持に関する条項において委託先に対する情報の取扱いに関する注意事項を含めている。

I)	**個人データの取扱いを委託する場合は委託先での安全管理措置を確保する**			
	1	自らが講ずべき安全管理措置と同等の措置が講じられるよう、監督を行っていますか	(対象外)	個人データの取扱いの委託は行っていない。
	2	適切な個人データの取扱いを行っている者を委託先として選定していますか	(対象外)	個人データの取扱いの委託は行っていない。
	3	サービス提供を目的として他者が提供するクラウドサービスを利用する場合には、セキュリティ対策等を勘案して、導入するサービスの選定を行っていますか	✔(対応済)	新規サービス導入前に情報セキュリティ部門によるセキュリティ対策のチェック(必要に応じ、併せてリスクアセスメントも実施)を行い、サービスの選定を行なっている。
J)	**取扱状況を把握するとともに、安全管理措置の見直しを行う**			
	1	個人データの取扱状況について、定期的に自ら行う点検又は他部署等による監査を実施していますか	✔(対応済)	資産目録にて月次で取扱い情報の見直しと年次での内部監査、外部監査を行っている。
	2	外部の主体による監査活動と合わせて、監査を実施していますか	✔(対応済)	ISMS活動に合わせ、内部監査・外部監査を行っている。
K)	**従業者(派遣を含む。)に対し、セキュリティに関して就業上何をしなければいけないかを明示する**			
	1	従業者を採用する際に、守秘義務契約又は契約書を交わしていますか	✔(対応済)	入社時に守秘義務契約を締結している。
	2	秘密保持に関する事項を就業規則等に盛り込むなど、従業者が遵守すべき事項を明確にしていますか	✔(対応済)	就業規則に盛り込まれている。
	3	違反した従業員に対する懲戒手続きが整備されていますか	✔(対応済)	就業規則に盛り込まれている。
	4	在職中及び退職後の機密保持義務を明確化するため、プロジェクトへの参加時等、具体的に企業機密に接する際に、退職後の機密保持義務も含む誓約書を取っていますか	✔(対応済)	プロジェクト参加時に退職後の機密保持義務も含む誓約書を取得している。
L)	**情報セキュリティに関するルールの周知及び情報セキュリティに関わる知識習得の機会を与える**			
	1	ポリシー及び関連規程を文書化し、従業員に理解させていますか	✔(対応済)	ポリシー及び関連規程を文書化し、社内ポータルサイトより全従業員が確認可能な状態としている。
	2	従業員に対して、実践するために必要な教育を定期的に行っていますか	✔(対応済)	入社時及び年2回の情報セキュリティ教育において、継続的に理解醸成を図っている。

②物理的セキュリティ

項目番号		内容	チェック	対応内容詳細(公表不要)
A)	**健診等情報を保管したり、扱ったりする場所の入退管理及び施錠管理を行う**			
	1	健診等情報を保管したり、扱ったりする区域を定めていますか	✔(対応済)	利用者様の情報はAWS上のDBに格納されており、物理的対策はAWS側で対策がなされています。またアクセスできる担当者を限定する措置を行っています。
	2	健診等情報を保管している部屋(事務室)又はフロアーへの侵入を防止するための対策を行っていますか	✔(対応済)	同上
	3	健診等情報を保管している部屋(事務室)又はフロアーに入ることができる人を制限していますか	✔(対応済)	同上
	4	健診等情報を保管している部屋(事務室)又はフロアーへの入退の記録を取得していますか	✔(対応済)	同上
B)	**重要なコンピュータ及び記録は地震等の自然災害又はケーブルの引っ掛けなどの人的災害による重大な被害が起こらないように配置又は設置する**			
	1	サービスの提供に用いるサーバ・ストレージ、情報セキュリティ対策機器等のシステムが設置されている建物(情報処理施設)、サーバルーム等(重要なコンピュータ等)については、物理的及び環境上の危険を考慮して、システムが存在する施設の場所を計画していますか	✔(対応済)	同上
	2	重要なコンピュータは許可された人だけが入ることができる安全な場所に設置していますか	✔(対応済)	同上
	3	電源及び通信ケーブルなどは、従業員が容易に接触できないようにしていますか	✔(対応済)	同上
	4	重要なシステムについて、地震等による転倒防止、水漏れ防止及び停電時の代替電源の確保等を行っていますか	✔(対応済)	同上
	5	健診等情報を保管する重要なコンピュータ等の装置については、適切な保護対策を行っていますか	✔(対応済)	同上
C)	**重要な書類及び記憶媒体等について、整理整頓を行うと共に、盗難防止対策、紛失対策、漏えい防止対策及び確実な廃棄・消去を行う**			
	(盗難防止対策・紛失対策)			
	1	健診等情報を記載した書類を保管するキャビネットには、施錠管理を行っていますか	(対象外)	健診等情報を記載した書類の取扱いを行っていない。
	2	健診等情報が存在する机上、書庫及び会議室等は整理整頓を行っていますか	(対象外)	同上
	3	組織内でモバイル PC 及び記憶媒体や備品を施錠保管する等、盗難防止対策を実施していますか	✔(対応済)	リモート勤務等にて利用する業務PCはHDDの暗号化措置を行っており、盗難時にはリモートワイプ処理を実施いたします。またUSBメモリ等の外部記憶媒体の利用は社内規程上、原則禁止しており、本業務において、利用は発生いたしません。
	(漏えい防止対策)			
	4	健診等情報を表示する画面を他人から覗き見されないよう、窃視対策を行っていますか	✔(対応済)	全業務PCについて、窃視対策として、スクリーンロック設定の実施に加え、覗き見防止フィルターを取り付けております。
	5	データの不正な持出しを防止するため、記録媒体の適切な管理について、規則を定めていますか	✔(対応済)	外部記憶媒体の利用は社内規程上、原則禁止しております。
	6	許可なく私有PCを会社に持ち込んだり、私有PCで業務を行わないようにしていますか	✔(対応済)	私用PCの業務利用は、社内規程上、原則禁止しております。
	(健診等情報の確実な廃棄・消去)			
	7	不要になった書類等については、シュレッダー又は焼却等により確実に処分していますか	✔(対応済)	不要になった書類は、外部委託業者に依頼し、確実に処分してる。
	8	使わなくなった健診等情報については、情報システム・記憶媒体から、速やかにデータの消去を行っていますか	✔(対応済)	データ削除後、14日間の猶予期間あり。それを過ぎると完全消去される。

③情報システム及び通信ネットワークの運用管理

項目番号		内容	チェック	対応内容詳細(公表不要)
A)	**情報システムの運用に関して運用ルールを策定する**			
	1	システム運用におけるセキュリティ要求事項を明確にしていますか	✔(対応済)	情報セキュリティ規程、情報システム運用・保守規程にて明確にしている。
	2	情報システムの運用手順書(マニュアル)を整備していますか	✔(対応済)	各システムにて運用手順書を整備している。
	3	システムの運用状況を点検していますか	✔(対応済)	各システムにおいて異常が発生しシステム提供において影響を及ぼさないようにするため、必要と考えられる指標に対し閾値を設け、予め検知可能なようにしております。設定した閾値を超えた場合、専用Slackチャンネルにアラートを発報、通知を行い、日常的な運用状況の点検を行っております。
	4	システムにおいて実施した操作、障害及びセキュリティ関連イベントについてログ(記録)を取得していますか	✔(対応済)	データベースのエラーログと全般ログ(全SQLの記録)、Slow Query等を取得している(詳細は対象システム毎に別途確認が必要)。 監査ログはログシステムにも出力していない。
	5	設備(具体例)の使用状況を記録していますか	✔(対応済)	AWS側設備については、AWSにて使用状況を記録している。 当社側の責任範疇のシステムの利用状況はCloudWatchにて記録している。
	6	重要なコンピュータ等の取得したログ(記録)については、定期的なレビューを行い、不正なアクセス等がないことを確認していますか	✔(対応済)	顧客要望等で一部実施行っている。
	7	重要なコンピュータ等を適切に運用するための管理策を講じていますか	✔(対応済)	ログ監視、バックアップなど適切に運用するための管理策を講じている。
	8	サービス提供に必要な重要なコンピュータ等の環境確保のための対策を実施していますか	✔(対応済)	定期バックアップを実施している
	9	クラウドサービスを利用してサービス提供している場合の運用については、クラウドサービスの性格を踏まえて、運用に関する責任範囲や、報告内容・方法等を取り決めていますか	✔(対応済)	各システムで運用に関する責任範囲と報告内容・方法は事前に取り決めている。
B)	**マルウエア対策ソフトをはじめとしたアプリケーションの運用を適切に行う**			
	1	マルウエア対策ソフトを導入し、製品のバージョンや設定ファイル・定義ファイル等の更新を定期的に行っていますか	✔(対応済)	ディープラーニング型のAI搭載マルウェア対策ソフトを導入しており、検知ロジックの更新があった際にはタイムリーに更新をかけるようシステム運用を行っている。
	2	マルウエア対策ソフトが持っている機能(ファイアウォール機能、スパムメール対策機能及び有害サイト対策機能)を活用していますか	✔(対応済)	同上。メール対策は別途、メールフィルタリングシステムを導入、有害サイト対策は別途、Webフィルタリングシステムを導入しております。
	3	各サーバ及びクライアントPCについて、定期的なマルウエア検査を行っていますか	✔(対応済)	リアルタイムスキャン設定をオンにしており、常時監視している。
	4	組織で許可されていないソフトウェアのインストール及びサービスの利用の禁止又は使用制限を行っていますか	✔(対応済)	許可されていないソフトウェアのインストールは禁止している。
	5	PHRサービスの利用者に対して、適切なセキュリティ対策を利用端末に行うように啓発していますか	✔(対応済)	提供サービスのセキュリティホワイトペーパーにてサービス利用者に対して適切なセキュリティ対策を利用端末に行っていただくよう記載し啓発を行っている。

C)	**導入している情報システムに対して、最新のパッチを適用するなどの脆弱性対策を行う**			
	1	脆弱性の解消（修正プログラムの適用及びWindows update等）を行っていますか	✔(対応済)	サービス基盤及び、社内PCに対して脆弱性対策を適宜実施している。
	2	脆弱性情報及び脅威に関する情報の入手方法を確認し、定期的に収集していますか	✔(対応済)	週次で脆弱性情報及び、脅威情報を入手している。
	3	情報システム導入の際に、不要なサービスの停止等、セキュリティを考慮した設定を実施するなどの対策が施されているかを確認していますか	✔(対応済)	システム導入時に都度確認を実施している。
	4	Webサイトの公開にあたっては、不正アクセス又は改ざんなどを受けないような設定又は対策を行い、脆弱性の解消を行っていますか	✔(対応済)	CMSを最新の状態に保たれるクラウド版を利用しており、適宜、自動更新が行われるようになっている。脆弱性発表時にはアップデート対応がなされたかの確認まで行っている。
	5	Webブラウザ及び電子メールソフトのセキュリティ設定を行っていますか	✔(対応済)	Webブラウザは最新の状態に、電子メールについてはGmailのセキュリティを利用している。
D)	**通信ネットワークを流れる重要なデータに対して、暗号化等の保護策を実施する**			
	1	TLS（version1.3）等を用いて通信データを暗号化していますか。ただし、対応が困難な場合は、Version1.2 によることも可能としますが、その場合は、IPA の「TLS 暗号設定ガイドライン第 3.1.0 版」に規定される最もセキュリティ水準が高い「高セキュリティ型」に準じた適切な設定を行っていますか	(対応予定)	TLS1.3およびTLS1.2を使用しているが、TLS1.2については「高セキュリティ型」の要件を一部満たしておらず、同基準に準じた設定へ変更予定
	2	外部のネットワークから内部のネットワーク又は情報システムにアクセスする場合に、VPN等を用いて暗号化した通信路を使用していますか	✔(対応済)	情報システム管理者による社内ネットワークへの接続時及び顧客提供サービスへの接続における接続元として当社所有のグローバルIPアドレスを利用する必要がある場合のみ、VPN接続を利用している。
	3	電子メールをやり取りする際に、健診等情報については暗号化するなど保護策を講じていますか	(対象外)	健診等情報の電子メールでのやり取りはおこなっていない。
	4	重要なデータやファイルについて、データの漏えいや盗聴、改ざん等を防止するため、暗号化を講じていますか	✔(対応済)	入力されたデータは HTTPS により暗号化されてサーバに送信される。
E)	**モバイルPC、USBメモリなどの記憶媒体又はデータを外部に持ち出す場合、盗難、紛失等に備えて、適切なパスワード設定又は暗号化等の対策を実施する**			
	1	モバイルPC又はUSBメモリ等の使用や外部持ち出しについて、規程を定めていますか	✔(対応済)	情報セキュリティ規程にて定めている。
	2	外部でモバイルPC又はUSBメモリ等を使用する場合の紛失や盗難対策を講じていますか	✔(対応済)	PCについては、HDDの暗号化を実施している。紛失、盗難時には早急な報告をすることとしている。また、USBメモリ等の可搬性媒体については基本的に業務での利用禁止とし、顧客要望等のやむを得ない場合のみ管轄部署責任者と情報セキュリティ委員長へ申請をし、許可を得た上でのみ利用可能とし、利用時には書き込むファイルに暗号化措置を施すことを必須としている。
	3	モバイルPC又はUSBメモリ等を外部に持ち出す、若しくはクラウド上のストレージを取り扱う際は、その使用者の認証（ID及びパスワード設定並びにUSBキー、ICカード認証又はバイオメトリクス認証等）を行っていますか	✔(対応済)	基本的にID、PWでの認証を行っている。PCやサービスによって機能が搭載されていないことから、二要素認証については必須にはしていない。
	4	保存されているデータを、重要度に応じてHDD暗号化又はBIOSパスワード設定等の技術的対策を実施していますか	✔(対応済)	PCのHDD暗号化を行っている。
	5	モバイルPC又はUSBメモリ等を持ち出す場合の持出者並びに持出及び返却の管理を実施していますか	✔(対応済)	リモートワーク環境下のため、PCは常に持ち出しを行う可能性があるのが前提で、誰に該当のPCを貸し出しているかの管理は行っている。
	6	盗難又は紛失時に情報漏えいの脅威にさらされた情報が何かを正確に把握するため、持ち出し情報の一覧及び内容の管理を行っていますか	✔(対応済)	ファイルサーバ及び、Google Driveに情報は保存することとなっており、PCのHDD内に業務情報を保存しないルールとなっているため、持ち出しはできない。
F)	**システム外部から受け取るファイルに対して、マルウエア対策ソフト等によるチェックを実施する**			
	1	システム外部からのファイルを受け取る際には、マルウエア対策ソフト等によるチェックを実施していますか	✔(対応済)	導入済の各種セキュリティ機構により多重でのマルウェアチェックを実施している。

④情報システムのアクセス制御並びに情報システムの開発及び保守におけるセキュリティ対策

項目番号		内容	チェック	対応内容詳細（公表不要）
A)	**情報（データ）及び情報システムへのアクセスを制限するために、組織内利用者（システム管理者を含む）毎のID及びパスワード等による認証情報の管**			
	1	組織内利用者（システム管理者を含む）毎にID及びパスワード等を割当て、当該ID及びパスワード等による識別及び認証を確実に	✔(対応済)	システム管理者毎のID発行とPW設定、認証を行っている。
	2	サービスで取り扱うデータ等の性格やリスク対策の必要性に鑑みて、認証においては多要素認証を実施していますか	✔(対応済)	他要素認証導入済みである。
	3	特に、システム管理者IDの登録及び削除に関する規程を整備、運用していますか	✔(対応済)	情報セキュリティ規程にて規定されている。
	4	組織内利用者（システム管理者を含む）のパスワードの管理を適切に行うとともに、パスワードに関するルールを策定していますか	✔(対応済)	情報セキュリティ規程にて規定されている。
	5	パスワードによる認証を採用する場合、その定期的な見直しを求めていますか	✔(対応済)	パスワード有効期限を設定可能がシステムは設定を実施している。
	6	パスワードによる認証を採用する場合、容易に類推できないパスワードとし、極端に短い文字列を使用しない等の対応を求めていますか	✔(対応済)	情報セキュリティ規程にて規定されている。
	7	離席する際は、パスワード等で保護されたスクリーンセーバーでパソコンを保護していますか	✔(対応済)	スクリーンセーバーの設定を必須としている。
B)	**健診等情報に対するアクセス権限の設定を行う**			
	1	健診等情報に対するアクセス管理方針を定め、組織内利用者（システム管理者を含む）毎にアクセス可能な情報、情報システム、業務アプリケーション及びサービス等を設定していますか	✔(対応済)	AWSのDBへのアクセス権は運用上必要な方に限り、権限を付与している。
	2	職務の変更又は異動に際して、組織内利用者（システム管理者を含む）のアクセス権限を見直していますか	✔(対応済)	異動及び、退職に伴い、権限が不要となった際にはタイムリーに削除している。また、月次での特権IDの棚卸を実施している。
	3	システム管理者のアクセス権限を適切に管理していますか	✔(対応済)	アクセス権限一覧で管理した上で適切に管理している
C)	**インターネット接続に関わる不正アクセス対策（ファイアウォール機能、パケットフィルタリング及びIPSサービス 等）を行う**			
	1	外部との情報・データの転送に関するルールを整備していますか	✔(対応済)	ルールを整備している。
	（外部から内部への不正アクセス対策）			
	2	ネットワークの通信の処理や監視を行い、不正な通信の制御と管理を行うことで対策を確実に実施していますか	✔(対応済)	WAFによる対応を行なっている。
	3	外部から内部のシステムにアクセスする際、なりすまし等の不正アクセスを防止するため、確確実な認証を実施していますか	✔(対応済)	IAMには多要素認証、SSH接続では証明書認証を行っている。 社内ファイルサーバへのアクセスはVPN認証を行っている。
	4	保護すべき健診等情報のデータベースは、サービス利用者が利用する機能（閲覧等）及び保守点検時のリモート管理機能を除き、外部接続しているネットワークから物理的に遮断する又はセグメント分割することによりアクセスできないようにしていますか	✔(対応済)	サービス毎にDBを分割管理しており、アプリを介したアクセス以外では保守目的でしかアクセスできないようにしている。
	（内部から外部への不正アクセス対策）			
	5	不正なプログラムをダウンロードさせるおそれのあるサイトへのアクセスを遮断するような仕組み（フィルタリングソフトの導入等）を	✔(対応済)	Webフィルタリングサービスの適用完了。
	6	サービスが提供するセッションを適切に管理し、不正アクセスやアクセス制御における脆弱性への対応を図っていますか	✔(対応済)	アクセストークンやリフレッシュトークンは適切に管理され、HTTPS 通信により安全にやり取りされ、有効期限の制御や失効処理を行うことで、不正利用やセッションハイジャックを防止している。
D)	**無線LANのセキュリティ対策（WPA3等の導入等）を行う**			
	1	無線LANにおいて健診等情報の通信を行う場合は、暗号化通信（WPA3等）の設定を行っていますか	✔(対応済)	WPA3の設定を行なっている
	2	WPA2 を用いる場合には、パスワードを定期的に変更する等、パスワードの漏えいに伴うリスクへの対応をしていますか	(対象外)	WPA3の設定を行なっているため対象外
	3	無線LANの使用を許可する端末（MAC認証等）及びその使用者の認証を行っていますか	✔(対応済)	ステルスモードでのWifi運用を行っており、情報システム管理者のみ設定内容を把握している状況にしている。
E)	**ソフトウェアの選定及び購入、情報システムの開発及び保守並びにサービス利用に際して、情報セキュリティを前提とした管理を行う**			
	1	情報システムの設計時に安全性を確保し、継続的に見直していますか（情報システムの脆弱性を突いた攻撃への対策を講ずることを含む。）	✔(対応済)	設計時に予め保護されたネットワーク内での構築、AWSのマネージドサービスを利用することで安全性の確保を行っている。継続的な見直しについては、脆弱性情報の定期チェックと必要に応じたシステムへのアップデートを実施している。
	2	サービスを提供するためのシステム（ソフトウェア及びクラウド等の他者が提供するサービス）の導入及び変更に関する手順を整備し、本指針のセキュリティ対策の遵守を確認していますか	✔(対応済)	新規サービス導入前に情報セキュリティ部門によるセキュリティ対策のチェック（必要に応じ、併せてリスクアセスメントも実施）を行い、サービスの選定を行なっている。併せて、本指針のセキュリティ対策の遵守を確認している。
	3	サービスを提供するためのシステム（ソフトウエア及びクラウド等の他者が提供するサービス）を構成するプログラム及びサービス等に	✔(対応済)	社内ルールに従って管理し、導入・変更行なった場合更新を行なっている
	4	システム開発において、レビューを実施し、その記録を残していますか	✔(対応済)	開発全体（工程ごと、リリース判定会等）及び、詳細の設計内容（Backlog）のレビューを実施し、それぞれ記録を残している。
	5	外部委託によるソフトウェア開発を行う場合、使用許諾及び知的財産等について取り決めていますか	✔(対応済)	基本的には帰属は当社に権利がある旨、記載する方針で運用している。
	6	サービスを提供するためのシステム（ソフトウエア及びクラウド等の他者が提供するサービス）に関する保守について、あらかじめ手順	✔(対応済)	保守については手順策定及び実施を行なっている
	7	開発又は保守を外部委託する場合に、セキュリティ管理の実施状況を把握できていますか	✔(対応済)	委託先審査票にて発注前、及び、年次での対策状況の確認を行っている。

⑤情報セキュリティ上の事故対応

項目番号		内容	チェック	対応内容詳細（公表不要）
A)	**情報システムに障害等が発生した場合、業務を再開するための対応手順を整理する**			
	1	情報システムに障害等が発生した場合に、最低限運用に必要な時間及び許容停止時間を明確にしていますか	✔(対応済)	SLA定義書にて明確にしている。
	2	障害等対策の仕組みが組織として効果的に機能するよう、よく検討していますか	✔(対応済)	インシデント発生時には対応フローに基づき、対応を行うこととなっており、運用に関しては保守運用Tが組織化されており、適宜対応にあたるようにコントロールされている。
	3	システムの切り離し（即応処理）、必要なサービスを提供できるような機能（縮退機能）、情報の回復及び情報システムの復旧に必要となる機能等が、障害等発生時に円滑に機能するよう確認していますか	✔(対応済)	サーバ開発導入ガイドラインにバックアップと復旧について明記している。
	4	日常システム運用の中で、バックアップデータ及び運用の記録等を確保していますか	✔(対応済)	バックアップデータはAWS上に35世代保管、運用の記録は最低3ヶ月はシステムログとして保持している。
	5	情報システムに障害等が発生によるシステム停止等を避けるため、必要な冗長化対策を講じていますか	✔(対応済)	当サービスは AWS 上で提供しており、基盤リソースはアベイラビリティゾーンにより冗長化されている。アプリケーションサーバは Amazon ECS 上でステートレスに構成され、常時複数コンテナを起動しているため、個別の障害が発生してもサービス提供に影響を及ぼさず、ダウンタイムを最小化している。
	6	障害等発生時に必要な対応として、障害等発生時の報告要領（電話連絡先の認知等）、障害等対策の責任者と対応体制、システム切り替え及び復旧手順並びに障害等発生時の業務実施要領等の準備を整えてありますか	✔(対応済)	インシデント対応フローにて一連の対応方法と責任者、対応体制が定義されており、そちらに則った対応を行っている。
	7	関係者への障害等対応要領の周知、必要なスキルに関する教育及び訓練等の実施を行っていますか	✔(対応済)	全社へのインシデント対応フローの説明会実施、及び、年次でのBCP訓練を行っている。 また、経営陣向けに半期に一度のインシデント対応訓練を行っている。
B)	**情報セキュリティに関連する事件又は事故等（マルウェア感染、情報漏えい等）の緊急時の対応手順を整理する**			
	1	マルウェア感染又は情報漏えい等の発生時の組織内の関係者への報告、緊急処置の適用基準及び実行手順、被害状況の把握、原因の把握、対策の実施、被害者ほか影響を受ける可能性のある本人への通知、外部への周知方法、個人情報保護委員会への報告、通常システムへの復旧手順並びに業務再開手順等を整えていますか	✔(対応済)	インシデント対応フローにて定義されている。
	2	事実を確認したら速やかに責任者に報告し、対応体制を取ることとしていますか	✔(対応済)	インシデント対応フローにて定義されている。
	3	対応方針についての判断を行うため5W1Hの観点で調査し情報を整理していますか	✔(対応済)	インシデント対応フローにて定義されている。
	4	上記3の整理を踏まえて、対策本部で対応方針を決定することとしていますか	✔(対応済)	インシデント対応フローにて定義されている。
	5	上記3の整理を踏まえて、被害の拡大防止と復旧・再発防止のための措置を行うこととしていますか	✔(対応済)	インシデント対応フローにて定義されている。
	6	漏えいした個人情報の本人及び取引先等への通知、個人情報保護委員会及び監督官庁等への報告並びにホームページ又はマスコミ等による公表についても検討していますか	✔(対応済)	インシデント対応フローにて定義されている。
	7	情報セキュリティに関して、業務上の関係者等との日常的な情報共有や最新情報の収集を行っていますか	✔(対応済)	最新情報の収集は行っている。

⑥外的環境の把握

項目番号		内容	チェック	対応内容詳細（公表不要）
A)	**外国において個人データを取り扱う場合、当該外国の個人情報の保護に関する制度等を把握した上で、個人データの安全管理のために必要かつ適切な措置を講じる**			
	1	外国において個人データを取り扱う場合、当該外国の個人情報の保護に関する制度等を把握した上で、個人データの安全管理のために必要かつ適切な措置を講じていますか	（対象外）	外国において個人データを取り扱っていない。

2．2．第三者認証の取得

項目番号		内容	チェック	対応内容詳細（公表不要）
①	**第三者認証の取得**			
	1	リスクマネジメントシステムを構築するに際して、本指針の対策例に加えて、標準規格（ISO又はJIS）等に準拠した対策の追加及び第三者認証（ISMS又はプライバシーマーク等）を取得するよう努めていますか（マイナポータルAPI経由で健診等情報を入手する場合は、第三者認証を取得していますか）	✔(対応済)	ISMS及び、ISO27017CSCを取得、マイカルテに関してはISO27017のCSPを取得している。

3. 個人情報の適切な取扱い
3. 1. 情報の公表
3. 1. 1. 利用目的の特定
(1)法規制に基づく遵守すべき事項

項目番号		内容	チェック	対応内容詳細(公表不要)
①	**利用目的の特定**			
	1	健診等情報を取り扱うに当たっては、その利用目的をできる限り特定していますか	✔(対応済)	弊社サービスに係る利用規約及びプライバシーポリシーにおいてできる限り特定している。
	2	利用目的を単に抽象的又は一般的に特定するのではなく、個人情報が最終的にどのような事業の用に供されるのか、どのような目的で個人情報を利用されるのかが、本人にとって一般的かつ合理的に想定できる程度に具体的に特定するように努めていますか	✔(対応済)	同上
②	**利用目的の変更**			
	1	変更前の利用目的と関連性を有すると合理的に認められる範囲で、利用目的を変更する場合、変更後の利用目的を本人に通知するか、又は公表していますか	✔(対応済)	ウェブサイト上に公表している。
	2	変更前の利用目的と関連性を有すると合理的に認められる範囲を超えて、利用目的を変更する場合、改めて本人の同意を取得していますか	✔(対応済)	これまで左記の範囲を超えた利用目的の変更を行った例はない。このような変更を行う場合には本人の同意を取得する。

3. 1. 2. 利用目的の明示等
(1)法規制に基づく遵守すべき事項

項目番号		内容	チェック	対応内容詳細(公表不要)
①	**利用目的の明示**			
	1	契約書のような書面等への記載又は利用者入力画面等への打ち込みなどにより、直接本人から健診等情報を取得する場合には、あらかじめ、本人に対し、その利用目的を明示していますか	✔(対応済)	アプリの利用規約に利用の目的等の記載を行っている。
	2	事業の性質及び健診等情報の取扱状況に応じて、内容が本人に認識される合理的かつ適切な利用目的の明示方法を採用していますか	✔(対応済)	病歴(個人情報保護法上の要配慮情報)に関する項目である前提で、 利用規約及びプライバシーポリシーの周知及びサービス開始時の同意取得により対応している。
②	**保有する健診等情報等の本人への開示**			
	1	本人からの要求があった場合、保有する当該本人に係る健診等情報(保有個人データ)を開示していますか	✔(対応済)	開示している。

(2)本指針に基づく遵守すべき事項

項目番号		内容	チェック	対応内容詳細(公表不要)
①	**サービス利用規約及びプライバシーポリシー等の公表**			
	1	利用者及び第三者が当該PHRサービス提供者の取組について評価できるよう、プライバシーポリシー及びサービス利用規約をホームページに掲載するなどにより公表していますか	✔(対応済)	ホームページに掲載している。 プライバシーポリシー:https://welby.jp/privacy/ サービス利用規約:https://welby.jp/term_of_mykarte/
	2	サービス利用規約の概要版を必要に応じて作成するとともに、ホームページのアクセスしやすい場所に掲載するなど分かりやすく公表していますか	✔(対応済)	サービス利用規約の概要版を作成し、アクセスしやすいようにアプリメニューとして概要版へのリンクを設けている。 概要版は以下にございます。 https://karte.welby.jp/

3. 2. 同意取得
(1)法規制に基づく遵守すべき事項

項目番号		内容	チェック	対応内容詳細(公表不要)
①	**取得に係る事前の同意取得等**			
	1	健診等情報のうち要配慮個人情報を取得する際、あらかじめ、本人からの同意を取得していますか	✔(対応済)	取得しています。
	2	当初の利用目的の達成に必要な範囲を超えて健診等情報を取り扱う場合(事業の承継後に、承継前の当初の利用目的の達成に必要な範囲を超えて、健診等情報を取り扱う場合を含む)は、あらかじめ本人の同意を得ていますか	✔(対応済)	同意取得画面で承諾いただかない限りは連携できない仕組みにて実装している。
②	**第三者提供に係る事前の同意取得**			
	1	第三者提供の同意の取得に当たっては、事業の規模及び性質並びに個人データの取扱状況(取り扱う個人データの性質及び量を含む。)等に応じ、本人が同意に係る判断を行うために必要と考えられる合理的かつ適切な範囲の内容を明確に示していますか	✔(対応済)	プライバシーポリシー9、利用規約第8条第1項及び第2項 現時点において第三者提供を行ってはいないものの、個別に提供先、提供する個人データの内容及び利用目的を個別の事案ごとに示して同意取得を行い、第三者提供を行う方針としている。
	2	第三者提供に係る同意取得を行わない場合は、以下のいずれかに当てはまりますか 個情法第27条1項各号又は委託、事業承継若しくは共同利用	(対象外)	同意取得なしでの第三者提供は行わない。
	3	共同利用の場合、あらかじめ、次に掲げる事項を本人に通知又は本人が容易に知り得る状態にしていますか 共同利用をする旨 / 共同して利用される個人データの項目 / 共同して利用する者の範囲 / 利用する者の利用目的 / 当該個人データの管理について責任を有する者の氏名又は名称及び住所並びに法人にあっては、その代表者の氏名	✔(対応済)	アプリ内で知り得る状態にしている。
③	**外国における第三者への提供**			
	1	外国にある第三者と連携して我が国内でサービスを提供する場合等に、当該外国にある第三者に健診等情報を提供する際には、原則として、あらかじめ本人から、外国にある第三者への個人データの提供を認める旨の同意を得ていますか	(対象外)	外国における第三者への提供は行っていない。
	2	同意を得ようとする場合には、あらかじめ本人に対して、当該外国の名称、当該外国における個人情報の保護に関する制度に関する情報、当該第三者が講ずる個人情報の保護のための措置に関する情報について、当該本人に提供していますか	(対象外)	外国における第三者への提供は行っていない。

(2) 本指針に基づく遵守すべき事項

項目番号		内容	チェック	対応内容詳細(公表不要)
①	**予防接種歴の取得に係る事前の同意取得等**			
	1	予防接種歴を取得する際、あらかじめ、本人からの同意を取得していますか	✔(対応済)	本人からの同意を取得している。
②	**健診等情報取得に係る同意取得時の利用目的の通知**			
	1	健診等情報の取得に際しては、利用目的をできる限り特定し、利用目的及びその範囲等について、例えば、本指針に関するQ&Aに示されているような方法により、サービス利用規約の概要を提示するなど、分かりやすく通知した上で、本人の同意を得ていますか	✔(対応済)	現時点において当社としては概要版を作成する必要があるほど利用規約が長大ではない。
	2	健診等情報以外の個人情報も取り扱う場合には、当該情報についての利用目的の範囲内であることを確認していますか	✔(対応済)	確認している。
③	**第三者提供に係る事前の同意取得**			
	1	健診等情報の第三者提供に際しては、提供先、その利用目的(必要に応じてその概要を提示する)及び提供される個人情報の内容等を特定し、分かりやすく通知した上で、本人の同意を得ていますか	(対象外)	現在は第三者への提供は行っていない。
	2	第三者提供の同意があった場合でも、本人に不利益が生じないよう配慮していますか	✔(対応済)	提供先により不利益が発生しない等の配慮を行っている。
④	**利用者による同意状況の確認**			
	1	過去の同意状況を利用者が確認できる方策を確保していますか	✔(対応済)	確保している。

3．3．消去及び撤回

(1)法規制に基づく遵守すべき事項

項目番号		内容	チェック	対応内容詳細(公表不要)
①		**利用停止等請求 を受けた場合の対応**		
	1	本人から、当該本人が識別される保有個人データが、本人の同意なく健診等情報が取得された、目的外利用がされている、違法若しくは不当な行為を助長する等の不適正な方法により個人情報が利用されている、偽りその他不正の手段により取得された、利用する必要がなくなった、漏えい等事案が生じた、又は当該本人の権利若しくは正当な利益が害されるおそれがある、という理由によって、当該保有個人データの利用の停止又は消去の請求を受けた場合であって、その請求に理由があることが判明したときは、遅滞なく、利用停止等の措置を行っていますか	✔(対応済)	利用規約に記載している。
②		**利用停止等請求への対応の例外**		
	1	上記1の措置を講じることが困難な場合、本人の権利利益を保護するために代替措置をとっていますか	✔(対応済)	現在まで発生した事例はないが、本人に個別説明を行う等対応を行う。
③		**健診等情報の消去**		
	1	事業終了等により健診等情報の利用の必要がなくなった場合又は本人の求めがあった場合には、管理している健診等情報(管理を委託している場合を含む。)を消去していますか	✔(対応済)	消去している。
	2	上記1の措置を講じることが困難な場合、本人の権利利益を保護するために代替措置をとっていますか	✔(対応済)	過去発生していないが、本人に個別に説明を行う等を検討。

(2) 本指針に基づく遵守すべき事項

項目番号		内容	チェック	対応内容詳細(公表不要)
①		**同意の撤回**		
	1	健診等情報の取得時及び第三者提供時の当該同意の撤回について、同意する際と同程度の容易さで行えるよう、工夫していますか	✔(対応済)	アプリ等で退会等対応することが可能となっている。
②		**長期間利用がない場合の措置**		
	1	一定の期間、利用がない場合に消去等の措置を講じる旨(消去を行う時期等を含む。)を利用者に通知又は公表していますか	✔(対応済)	医療データなので一方的なデータ消去など行っていない。

3．4．その他

3．4．1．健診等情報に含まれる利用者以外の個人情報の取扱い

(1)法規制に基づく遵守すべき事項

項目番号		内容	チェック	対応内容詳細(公表不要)
①				
	1	医師又は薬剤師等の氏名等は、要配慮個人情報には該当しないものの、医師又は薬剤師等の個人情報に該当することに留意し、利用目的の特定、同意の取得等に関して、個人情報保護法に基づき適切に取り扱っていますか	✔(対応済)	個人情報保護法に基づき取り扱いを行っている。

3．4．2．個人関連情報に関する留意事項

(1)法規制に基づく遵守すべき事項

項目番号		内容	チェック	対応内容詳細(公表不要)
①				
	1	第三者が個人関連情報を個人データとして取得することが想定されるときは、当該第三者が個人関連情報の提供を受けて本人が識別される個人データとして取得することを認める旨の本人の同意が得られていることをあらかじめ確認しないで、個人関連情報を当該第三者に提供していませんか	✔(対応済)	現在は同意取得なしでの第三者提供は行わない。
	2	第三者から個人関連情報の提供を受けて個人データとして取得するときは、当該第三者から個人関連情報の提供を受けて本人が識別される個人データとして取得することを認める旨の本人の同意をあらかじめ得ていますか	✔(対応済)	本人同意を予め得た上で同意取得がなされるように実装完了。

3．4．3．仮名加工情報に関する留意事項

(1)法規制に基づく遵守すべき事項

項目番号		内容	チェック	対応内容詳細(公表不要)
①				
	1	仮名加工情報を作成するときは、個人情報保護委員会規則で定める基準に従い当該個人情報を加工し、仮名加工情報の作成に用いた個人情報から削除した記述等及び加工方法の安全管理のための措置を講じ、利用目的を公表していますか	(対象外)	現在は仮名加工情報の作成は行っていない。
	2	当該仮名加工情報は、法令に基づく場合を除くほか、第三者に提供していませんか	(対象外)	現在は仮名加工情報の作成は行っておらず、第三者への提供も行っておりません。

3．4．4．匿名化に関する留意事項

(1)法規制に基づく遵守すべき事項

項目番号		内容	チェック	対応内容詳細(公表不要)
①		**個人情報保護法に基づく適切な取扱い**		
	1	匿名加工情報を作成するときは、個人情報保護委員会規則で定める基準に従い当該個人情報を加工し、匿名加工情報の作成に用いた個人情報から削除した記述等及び加工方法の安全管理のための措置を講じ、当該匿名加工情報に含まれる個人に関する情報の項目を公表していますか	(対象外)	現在は匿名加工情報の作成は行っていない。
	2	当該匿名加工情報を第三者に提供するときは、あらかじめ、第三者に提供される匿名加工情報に含まれる個人に関する情報の項目及びその提供の方法について公表するとともに、第三者に対して、当該提供に係る情報が匿名加工情報である旨を明示していますか	(対象外)	現在は匿名加工情報の作成は行っていない。

4．健診等情報の保存及び管理並びに相互運用性の確保
4．1．健診等情報の保存及び管理
（1）法規制に基づく遵守すべき事項

項目番号		内容	チェック	対応内容詳細（公表不要）
①	**正確性の確保**			
	1	個人情報データベース等への個人情報の入力時の照合及び確認の手続の整備をしていますか	✔（対応済）	認証機能による個人の特定している。
	2	誤り等を発見した場合の訂正等の手続の整備をしていますか	✔（対応済）	入力時バリデーションで対応してる。
	3	記録事項の更新及び保存期間の設定をしていますか	✔（対応済）	保存期間は設定していない。臨床試験など利用期間が定められている場合は、満了時に速やかに消去を実施している。
②	**第三者提供の記録**			
	1	健診等情報を第三者に提供する場合は、提供した年月日及び提供先等に関する記録を作成していますか	（対象外）	現在は同意取得なしでの第三者提供は行わない方針、かつ第三者提供は行っていない。
	2	当該記録について、一定期間保存していますか	（対象外）	現在は同意取得なしでの第三者提供は行わない方針、かつ第三者提供は行っていない。
	3	第三者提供を受けた場合、提供を受けた年月日及び提供元等に関する記録を作成し、一定期間保存していますか	（対象外）	現在、個人データの第三者提供は受け付けていない。
	4	本人からの請求があった場合、保有する健診等情報の第三者提供の記録を開示していますか	（対象外）	現在は同意取得なしでの第三者提供は行わない方針、かつ第三者提供は行っていない。

4．2．相互運用性の確保
（1） 本指針に基づく遵守すべき事項

項目番号		内容	チェック	対応内容詳細（公表不要）
①	**利用者を介した相互運用性の確保**			
	1	マイナポータルAPI等を活用して入手可能な自身の健康診断等の情報については、利用者へのエクスポート機能を具備していますか	✔（対応済）	実装している。
	2	健診等情報のフォーマット等に関しては、マイナポータルAPIから出力される項目及びフォーマットを基本とし、また、データ変換時は互換性を担保するような方式とし、利用者が容易にデータを取り扱うことができるよう努めていますか	✔（対応済）	マイナポータルから取得したファイルをそのまま保管するように実装している。
②	**サービス終了時の措置**			
	1	サービスを終了する場合、利用者への健診等情報のエクスポート及び他のPHRサービス提供者への当該健診等情報のエクスポートが実施可能な期間を十分に確保していますか	✔（対応済）	サービス終了時は猶予期間を設けエクスポートできるように運用する。
③	**データ提供先の適切性の確認**			
	1	PHRサービス提供者で健診等情報のデータの提供を行う場合、データ提供先のPHRサービス提供者が本チェックシートの確認事項に基づき各要件を満たしていることを確認した上でデータ提供を行っていますか	（対応予定）	データ提供時は必ず利用者が介入しての承認後にデータ提供行っていたが、今後は本チェックシートの確認事項に基づき各要件を満たすように確認予定
	2	上記1に加えて、少なくともマイナポータルAPI経由で健診等情報を入手している場合には、本チェックシートの確認事項に基づき各要件を満たしていることを確認することにより、データ提供先のPHRサービス提供者の本指針への遵守状況を定期的に確認していますか	（対応予定）	上記に加え本指針への遵守状況を定期的に確認予定

5．要件遵守の担保
5．1．本指針の規定する要件を遵守していることの確認
（1） 本指針に基づく遵守すべき事項

項目番号		内容	チェック	対応内容詳細（公表不要）
①	**自主的な確認及びその結果の公表**			
	1	本チェックシートの確認事項に従って各要件を満たしているかどうかを定期的に確認していますか	✔（対応済）	確認を行っている。
	2	本チェックシートによる確認結果を、サービス利用規約及びプライバシーポリシー等を公表しているページと同じページ等で公表していますか	✔（対応済）	同じページで公表するように対応完了。当該ページにプライバシーポリシーへのリンクがございます。 https://welby.jp/about/#anchor-privacy
	3	公表する際に、結果の概要を分かりやすい表現で記載していますか	✔（対応済）	概要について分かりやすい表現で記載。

※本チェックシートの「法規制に基づく遵守すべき事項」は個人情報保護法上の主な要求事項を記載したものであり、本チェックシートに記載のない事項及び関連条文については最新版を参照されたい。

要求を満たさない項目について	
項目番号	
2．1．（2） ①I)1	対応が不要な合理的な理由 個人データの取扱いの委託は行っていない。
2．1．（2） ①I)2	対応が不要な合理的な理由 個人データの取扱いの委託は行っていない。
2．1．（2） ②C)1	対応が不要な合理的な理由 健診等情報を記載した書類の取扱いを行っていない。
2．1．（2） ②C)2	対応が不要な合理的な理由 健診等情報を記載した書類の取扱いを行っていない。
2．1．（2） ③D)3	対応が不要な合理的な理由 健診等情報の電子メールでのやり取りはおこなっていない。
2．1．（2） ④D)2	対応が不要な合理的な理由 WPA3の設定を行なっているため対象外
2．1．（2） ⑥A)1	対応が不要な合理的な理由 外国において個人データを取り扱っていない。
3．2．（1） ②2	対応が不要な合理的な理由 同意取得なしでの第三者提供は行わない。
3．2．（1） ③1	対応が不要な合理的な理由 外国における第三者への提供は行っていない。
3．2．（1） ③2	対応が不要な合理的な理由 外国における第三者への提供は行っていない。
3．2．（2） ③1	対応が不要な合理的な理由 現在は第三者への提供は行っていない。
3．4．3． （1）①1	対応が不要な合理的な理由 現在は仮名加工情報の作成は行っていない。
3．4．3． （1）①2	対応が不要な合理的な理由 現在は仮名加工情報の作成は行っておらず、第三者への提供も行っておりません。
3．4．4． （1）①1	対応が不要な合理的な理由 現在は匿名加工情報の作成は行っていない。
3．4．4． （1）①2	対応が不要な合理的な理由 現在は匿名加工情報の作成は行っていない。
4．1．（1） ②1	対応が不要な合理的な理由 現在は同意取得なしでの第三者提供は行わない方針、かつ第三者提供は行っていない。
4．1．（1） ②2	対応が不要な合理的な理由 現在は同意取得なしでの第三者提供は行わない方針、かつ第三者提供は行っていない。
4．1．（1） ②3	対応が不要な合理的な理由 現在、個人データの第三者提供は受け付けていない。
	対応が不要な合理的な理由

4．1．（1） ②4	現在は同意取得なしでの第三者提供は行わない方針、かつ第三者提供は行っていない。