（別紙） 本指針に係るチェックシート

点検日　2023/5/10
点検担当者　（株）Welby 情報セキュリティ責任者

※　業務委託先の遵守状況も含めた点検を行うこと
※　求められる事項を満たしているか、同等以上の対応を行っている場合にチェックを付けること

1. 基本的事項

項目番号		内容	チェック	対応内容詳細（公表不要）
1		本指針の対象とする情報の定義		
	1-1	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るもの、及び予防接種歴（以下「健診等情報」という。）ですか ・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 ・医療機関等から個人に提供され、個人が自ら入力する情報 ・個人が自ら測定又は記録を行うものであって、医療機関等に提供する情報	✔（対応済）	はい。
2		本指針の対象事業者		
	2-1	健診等情報を取り扱うPHRサービスを提供する民間事業者（以下「PHR事業者」という。）ですか	✔（対応済）	はい。

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		
	1-1	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 ※　具体的には（2）の対策の実施有無を確認	✔（対応済）	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）
1		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		
	1-1	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。
	1-2	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。
2		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		
	2-1	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。
	2-2	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		管理すべき重要な情報資産を区分する		
	3-1	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。
	3-2	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。
	3-3	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。
	3-4	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。
4		個人情報の取扱状況を確認する手段を整備する		
	4-1	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 例）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。
5		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		
	5-1	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。
	5-2	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。
	5-3	健診等情報に対して、漏洩及び不正利用を防ぐ保護対策を行っていますか 例）健診等情報を取り扱う人に対してのみ、アクセス可能とすること / 健診等情報の取扱い履歴を残しておくこと / 健診等情報を確実に消去又は廃棄すること	✔（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。
6		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		
	6-1	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 例）システム開発を委託する際の本番データ取扱い時の際の情報管理、例えば管理体制、受託情報の取扱い、受け渡し、返却及び廃棄等について、注意事項を含めること / 関係者のみにデータの取扱いを制限すること / 外部の組織との間で情報を授受する場合、情報受渡書を以ておこなうこと / 契約に基づく作業に遂行することによって新たに発生する情報（例：新たに作製された統計化又は加工された情報等）の取扱いを含めること 等	✔（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。
7		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		
	7-1	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。
8		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		
	8-1	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。
	8-2	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。
9		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		
	9-1	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。
	9-2	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。
	9-3	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。
	9-4	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。
10		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		
	10-1	ポリシー及び関連規程を従業員に理解させていますか	✔（対応済）	規程類の従業員教育は実施できていなかったが、2021Q3のISMS四半期教育よりコンテンツに入れている。プライバシーポリシーの改訂内容も含めて行う。
	10-2	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）	ISMS四半期教育、入社時教育の中で定期的に行っている。

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）
1		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		
	1-1	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。
	1-2	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
	1-3	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
	1-4	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
2		重要なコンピュータ及び配線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		
	2-1	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
	2-2	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
	2-3	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
3		重要な書類、モバイルPC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、紛失対策及び確実な廃棄を行う		
		（健診等情報を記載した書類について）		
	3-1	不要になった場合、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。
	3-2	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）	同上
	3-3	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
	3-4	郵便物、FAX及び印刷物等の放置を禁止したり、重要な書類の裏面を再利用しないようにしていますか	（対象外）	同上
		（モバイルPC及び記憶媒体等について）		
	3-5	クラウド上のデータを含め、保存した情報が不要になった場合、消去ソフトを用いるなど、確実に処分していますか	✔（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。
	3-6	モバイルPC及び記憶媒体については、盗難防止対策及び紛失対策を行っていますか	✔（対応済）	HDDの暗号化を実施している。
	3-7	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）	私有デバイス利用時には申請が必要となっている。

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）
1		情報システムの運用に関して運用ルールを策定する		
	1-1	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。
	1-2	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。
	1-3	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。
	1-4	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 <ログを取得する項目例> 個人情報データベース等の利用又は出力の状況 / 個人データが記載又は記録された書類及び媒体等の持ち運び等の状況 / 個人情報データベース等の削除又は廃棄の状況（委託した場合の消去又は廃棄を証明する記録を含む。）/ 個人情報データベース等を情報システムで取り扱う場合、担当者の情報システムの利用状況（ログイン実績、アクセスログ等）	✔（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。
	1-5	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。
	1-6	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。
2		ウイルス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		
	2-1	ウイルス対策ソフトを導入し、パターンファイルの更新を定期的に行っていますか	✔（対応済）	自動更新設定を行っており、定期的に更新が行われている。
	2-2	ウイルス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）	ファイアウォール機能はWindows Defenderにて、スパムメール対策はGmailにて行っている。
	2-3	各サーバ及びクライアントPCについて、定期的なウイルス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。
	2-4	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。

	2-5	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。
3	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			
	3-1	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。
	3-2	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。
	3-3	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。
	3-4	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。
	3-5	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。
4	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			
	4-1	TLS(version1.2以上)等を用いて通信データを暗号化していますか	✔(対応済)	暗号化する際はAES256を用いている。
	4-2	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)	社内ファイルサーバのみ、外部からのアクセスに利用しており、VPN接続を必須としている。
	4-3	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。
5	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			
	5-1	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。
	5-2	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。
	5-3	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。
	5-4	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。
	5-5	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。
	5-6	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。
6	外部から受け取るファイルに対して、無害化を実施する			
	6-1	ファイル無害化機器、無害化ソフトウェア又は無害化サービス等を導入し、外部からのファイルを受け取る際に、無害化を実施していますか	✔(対応済)	無害化サービスの適用完了。 OPSWAT社の「MetaDefender Core Deep CDR」を採用(すべてのファイルに悪意があるものとみなし、潜在的に悪意のあるコンテンツを削除・無効化することで非武装化 し、ユーザビリティを維持したまま安全なコンテンツで再構築。)

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)
1	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、システム管理者のIDの管理(パスワード等認証情報の管理等)を行			
	1-1	システム管理者毎に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行っていますか	✔(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。
	1-2	システム管理者IDの登録及び削除に関する規程を整備していますか	✔(対応済)	情報セキュリティ規程にて規定されている。
	1-3	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(ただし、2要素認証を採用している場合等を除く。)	✔(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。
	1-4	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(英数、記号を混在させた8文字以上の文字列とすることが望ましい)ようシステム管理者に求めていますか	✔(対応済)	情報セキュリティ規程にて規定されている。
	1-5	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。
	1-6	不要になったシステム管理者のIDを削除していますか	✔(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。
2	健診等情報に対するアクセス権限の設定を行う			
	2-1	健診等情報に対するアクセス管理方針を定め、システム管理者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。
	2-2	職務の変更又は異動に際して、システム管理者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	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			
	(外部から内部への不正アクセス対策)			
	3-1	外部から内部のシステムにアクセスする際、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。
	3-2	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)			
	3-3	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)を行っていますか	✔(対応済)	Webフィルタリングサービスの適用完了。
4	無線LANのセキュリティ対策(WPA2の導入等)を行う			
	4-1	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(WPA2等)の設定を行っていますか	✔(対応済)	WPA2／AES設定を行っている。
	4-2	無線LANの仕様を許可する端末(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。
5	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			
	5-1	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(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。)ていますか	✔(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。
	5-2	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)	技術的な対応は実施済み。(社内への教育・浸透対応中)
	5-3	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。
	5-4	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。
	5-5	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)
1	情報システムに障害が発生した場合、業務を再開するための対応手順を整理する			
	1-1	情報システムに障害が発生した場合に、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。
	1-2	障害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。
	1-3	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。
	1-4	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。
	1-5	障害発生時に必要な対応として、障害発生時の報告要領(電話連絡先の認知等)、障害対策の責任者と対応体制、システム切替え及び復旧手順並びに障害発生時の業務実施要領等の準備を整えてありますか 例)大容量データの復元には時間を要するため、復元に要する時間の事前見積りの実施	✔(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。
	1-6	関係者への障害対応要領の周知、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。
2	情報セキュリティに関連する事件又は事故等(ウイルス感染、情報漏えい等)の緊急時の対応手順を整理する			
	2-1	ウイルス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 例)ウイルス感染の場合、ウイルス定義ファイルを最新の状態にしたワクチンソフトにより、コンピュータの検査を実施し、ワクチンソフトのベンダのWebサイト等の情報を基に、検出されたウイルスの駆除方法等を試すことが必要となる	✔(対応済)	インシデント対応フローにて定義されている。
	2-2	情報漏えいの場合、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。
	2-3	情報漏えいの場合、対応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た上で、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。
	2-4	情報漏えいの場合、被害の拡大防止と復旧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。
	2-5	情報漏えいの場合、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。

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)
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			
	1-1	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			
	1-1	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		

	1-1	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。
	1-2	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、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			
	2-1	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。
	2-2	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			
	1-1	契約書のような書面等への記載又はユーザー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。
	1-2	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			
	2-1	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			
	1-1	利用者及び第三者が当該PHR事業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/uploads/2022/03/040f8e3d3d873f913e2d6a6b512490126e989cfb.pdf
	1-2	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			
	1-1	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。
	1-2	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			
	2-1	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。
	2-2	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。
	2-3	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			
	3-1	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。
	3-2	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、当該本人に情報提供していますか	(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			
	1-1	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			
	2-1	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。
	2-2	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			
	3-1	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。
	3-2	第三者提供の同意があった場合でも、本人の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			
	4-1	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			
	1-1	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、又は偽りその他不正の手段により取得された、事業者が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			
	2-1	上記1-1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。

(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			
	1-1	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	健診等情報の消去			
	2-1	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、自社が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。
	2-2	上記2-1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。
3	長期間利用がない場合の措置			
	3-1	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				
	1-1	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				
	1-1	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。
	1-2	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				

	1-1	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。
	1-2	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			
	1-1	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。
	1-2	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			
	1-1	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。
	1-2	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。
	1-3	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			
	2-1	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。
	2-2	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。
	2-3	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。
	2-4	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			
	1-1	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、利用者へのエクスポート機能及び利用者からのインポート機能を具備していますか	✔（対応済）	実装している。
	1-2	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、互換性の高い汎用的なデータファイル（例えば、HL7CDA等）としていますか	✔（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			
	2-1	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事業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	データ連携先事業者の適切性の確認			
	3-1	PHR事業者間で健診等情報を利用者を介さず直接的にデータ連携する場合、データ連携先事業者が本指針に規定する対策を行っていることを、当該データ連携先事業者のホームページ等での公表内容又は第三者認証の取得状況等により確認していますか	（対象外）	データ連携は必ず利用者が介入して承認後に実施。

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			
	1-1	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。
	1-2	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
	1-3	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）①	個人データの取扱いの委託は行っていないため対象外となります。
2．1．（2）②	健診等情報を記載した書類の取扱いを行っていないため対象外となります。
2．1．（2）③	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ため対象外となります。
2．1．（2）⑥	外国において個人データを取り扱っていないため対象外となります。
3．2．（1）	同意取得なしでの第三者提供は行わないため対象外となります。
3．2．（1）	外国における第三者提供は行っていないため対象外となります。
3．2．（1）	外国における第三者提供は行っていないため対象外となります。
3．2．（2）	現在は予防接種歴の取得を行っていないため対象外となりますが今後取得する際は利用規約等の変更を行います。
3．2．（2）	現在は健診等情報の第三者提供を行っていないため対象外となります。
3．4．3（1）	現在は仮名加工情報の提供は行っていないため対象外となります。
3．4．3（1）	現在は仮名加工情報の提供は行っていないため対象外となります。
3．4．4（1）	現在は匿名加工情報の提供は行っていないため対象外となります。
4．1．（1）	現在、個人データの第三者提供は行っていないため対象外となります。
4．2．（1）	データ連携は必ず利用者が介入して承認後に実施するため対象外となります。