資料６

※赤字：修正点

（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（案）

確 認 日	
組織名	
担当者名	※ 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. 本指針の対象者」に該当する場合は、以下の「2. 情報セキュリティ対策」から「5. 要件遵守の担保」までの各項目について、求められる事項を満たしている、もしくは、同等以上の対応を行っていることを確認し、チェックをつけて下さい。
なお、「2. 情報セキュリティ対策」の項目については、本指針の「対策例」（（例）以下に記載の内容）を参考に、ご確認願います。

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るもの、及び予防接種歴（以下「健診等情報」という。）を取り扱うこと

・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可能性がある情報

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。
※個人の健康管理ではなく、専ら研究開発の推進等を目的として利用される健診等情報又は匿名加工情報若しくは仮名加工情報のみを取り扱う者は、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
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	
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	

（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
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	
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	
	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	
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	
	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	
	3	利用者向けの問い合わせ窓口を整備していますか	
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	
	2	情報資産の管理者を定めていますか	
	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	
	4	健診等情報を取り扱う人の範囲を定めていますか	
	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	
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	
	2	情報資産に対するリスクを評価していますか	
	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	
	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	
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	
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	
	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	
	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	
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	

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	
	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	
	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	
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	
	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	
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	
	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	
	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	
	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	
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	
	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	

②物理的セキュリティ

項目番号		内容	チェック
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	
	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	
	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	
	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	
B)	**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	
	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	
	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	
	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	
	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	
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	
	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	
	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	
	（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	
	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	
	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	
	（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	
	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	

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
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	
	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	
	3	システムの運用状況を点検していますか	
	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	
	5	設備（具体例）の使用状況を記録していますか	
	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	
	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	
	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	
	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	
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	
	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	
	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	
	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	
	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	

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	
	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	
	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	
	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	
	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	
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	
	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	
	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	
	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	
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	
	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	
	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	
	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	
	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	
	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	
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	

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
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理等を行う**		
	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行っていますか	
	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	
	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	
	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	
	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	
	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	
	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	
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	
	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	
	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	
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	
	（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	
	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	
	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	
	（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）を行っていますか	
	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	
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	
	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	
	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	
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。）	
	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	
	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ついて、規程等に基づいて管理し、導入や変更の都度更新していますか	
	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	
	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	
	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、あらかじめ手順を策定し、実施していますか	
	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	

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
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	
	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	
	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	
	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	
	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	
	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	
	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	
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	
	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	
	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	
	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	
	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	
	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	
	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	

⑥外的環境の把握

項目番号		内容	チェック
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	

2．2．第三者認証の取得

項目番号		内容	チェック
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）	

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
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	
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	
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	
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	

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
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	
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	
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	

(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
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	
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	

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
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	
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	
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	
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	
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	
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	
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	

(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
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	
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	
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	
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	
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	
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	

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
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	
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	
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	
	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	

(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
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	
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	

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
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	

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
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	
	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	

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
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	
	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	

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
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	
	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	

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
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	
	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	
	3	記録事項の更新及び保存期間の設定をしていますか	
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	
	2	当該記録について、一定期間保存していますか	
	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	
	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	

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
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	
	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	
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	
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	
	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、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	

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
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	
	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	
	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	

※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	
	対応が不要な合理的な理由
	対応が不要な合理的な理由
	対応が不要な合理的な理由

※合理的な理由があって要求を満たさない事項が発生する場合は「(対象外)」を選択し、上記「要求を満たさない事項について」欄に対応が不要な合理的な理由を記載すること

※必要に応じて上記をコピーして追加・記入すること