参考資料１

民間ＰＨＲ事業者による健診等情報の取扱いに関する制度上の要求事項

【制度上の要求事項】

- 法令及び法令に基づくガイドライン等を踏まえた要求事項を記載。

【考え方】

- 【制度上の要求事項】を踏まえた原則的な対策について記載。

【構成】

１．情報セキュリティ対策

２．個人情報の適切な取扱い

３．健診等情報の保存・管理、相互運用性の確保

４．その他（要件遵守の担保方法）

【制度上の要求事項／考え方（１）】

制度上の要求事項		考え方
リスクに応じた安全管理措置		
個人情報保護法 第20条	個人情報取扱事業者は、個人データの漏えい、滅失又はき損の防止その他の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なければならない。	対象事業者は、健診等情報について、個人データが漏えい等をした場合に本人が被る権利利益の侵害の大きさを考慮し、事業の規模及び性質、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。）、個人データを記録した媒体の性質等に起因するリスクに応じて、必要かつ適切な安全管理措置を講じなければならない。
個人情報保護法GL （通則編） 第20条関係	個人情報取扱事業者による安全管理措置は、個人データが漏えい等をした場合に本人が被る権利利益の侵害の大きさを考慮し、事業の規模及び性質、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。）、個人データを記録した媒体の性質等に起因するリスクに応じて、必要かつ適切な内容としなければならない。	
個人情報保護法GL （通則編） 「8 別添 講ずべき安全管理措置の内容」	法第20条に定める安全管理措置として、個人情報取扱事業者が具体的に講じなければならない措置や当該措置を実践するための「手法の例示」が示されている。 なお、中小規模事業者（※）については、取り扱う個人データの数量及び個人データを取り扱う従業者数が一定程度にとどまること等を踏まえ、円滑にその業務を履行し得るような「中小規模事業者における手法の例示」が示されている。	健診等情報について、対象事業者がその規模に応じて具体的に講じなければならない措置や当該措置を実践するための「手法の例示」又は「中小規模事業者における手法の例示」が示されている。

※「中小規模事業者」：従業員の数が100人以下の個人情報取扱事業者。ただし、次に掲げる者を除く。
- その事業の用に供する個人情報データベース等を構成する個人情報によって識別される特定の個人の数の合計が過去６月以内のいずれかの日において5,000を超える者
- 委託を受けて個人データを取り扱う者

【制度上の要求事項／考え方（２）】

制度上の要求事項		考え方
リスクに応じた安全管理措置		
個人情報保護法GL（通則編） 8-1　基本方針の策定	個人情報取扱事業者は、個人データの適正な取扱いの確保について組織として取り組むために、基本方針を策定することが重要である。	対象事業者は、健診等情報について、個人データの適正な取扱いの確保について組織として取り組むために、基本方針を策定することが重要である。
個人情報保護法GL（通則編） 8-2　個人データの取扱いに係る規律の整備	個人情報取扱事業者は、その取り扱う個人データの漏えい等の防止その他の個人データの安全管理のために、個人データの具体的な取扱いに係る規律を整備しなければならない。	対象事業者は、健診等情報について、その取り扱う個人データの漏えい等の防止その他の個人データの安全管理のために、個人データの具体的な取扱いに係る規律を整備しなければならない。
個人情報保護法GL（通則編） 8-3　組織的安全管理措置	個人情報取扱事業者は、組織的安全管理措置として、次に掲げる措置を講じなければならない。 （1）組織体制の整備 （2）個人データの取扱いに係る規律に従った運用 （3）個人データの取扱状況を確認する手段の整備 （4）漏えい等の事案に対応する体制の整備 （5）取扱状況の把握及び安全管理措置の見直し 個人データの取扱状況を把握し、安全管理措置の評価、見直し及び改善に取り組まなければならない。	対象事業者は、健診等情報について、組織的安全管理措置として、個人データの取扱い状況を把握し、安全管理措置の見直し及び改善等に取り組まなければならない。

【制度上の要求事項／考え方（３）】

制度上の要求事項		考え方
リスクに応じた安全管理措置		
個人情報保護法GL（通則編） 8-4　人的安全管理措置	個人情報取扱事業者は、人的安全管理措置として、次に掲げる措置を講じなければならない。また、個人情報取扱事業者は、従業者に個人データを取り扱わせるに当たっては、法第21条に基づき従業者に対する監督をしなければならない。 ○従業者の教育	対象事業者は、健診等情報について、人的安全管理措置を講じなければならない。
個人情報保護法GL（通則編） 8-5　物理的安全管理措置	個人情報取扱事業者は、物理的安全管理措置として、次に掲げる措置を講じなければならない。 （1）個人データを取り扱う区域の管理 （2）機器及び電子媒体等の盗難等の防止 （3）電子媒体等を持ち運ぶ場合の漏えい等の防止 （4）個人データの削除及び機器、電子媒体等の廃棄	対象事業者は、健診等情報について、物理的安全管理措置を講じなければならない。
個人情報保護法GL（通則編） 8-6　技術的安全管理措置	個人情報取扱事業者は、情報システム（パソコン等の機器を含む。）を使用して個人データを取り扱う場合（インターネット等を通じて外部と送受信等する場合を含む。）、技術的安全管理措置として、次に掲げる措置を講じなければならない。 （1）アクセス制御 （2）アクセス者の識別と認証 （3）外部からの不正アクセス等の防止 （4）情報システムの使用に伴う漏えい等の防止	対象事業者は、健診等情報について、技術的安全管理措置を講じなければならない。

【制度上の要求事項／考え方（４）】

制度上の要求事項	考え方
リスクに応じた安全管理措置（マイナポータルAPI利用時）	
マイナポータルAPI利用に当たっては、マイナポータルAPI利用規約に基づき、マイナポータル利用条件確認書記載の要件についてチェックを行うことが必要。 ※マイナポータル利用条件確認書記載の「一般的対策の実施」（「情報セキュリティに対する組織的な取組状況」や「物理的セキュリティ」など）は「中小企業における組織的な情報セキュリティ対策ガイドライン」（IPA（情報処理推進機構））の「４　共通して実施すべき対策」を準拠している。	対象事業者は、マイナポータルAPIを利用する際には、マイナポータル利用条件確認書記載の情報セキュリティ要求事項を遵守しなければならない。

【「中小企業における組織的な情報セキュリティ対策ガイドライン」（IPA（情報処理推進機構））　「４　共通して実施すべき対策」 抜粋】

4.1 情報セキュリティに対する組織的な取り組み

4.1.1 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
4.1.2 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
4.1.3 管理すべき重要な情報資産を区分する
4.1.4 重要な情報については、入手、作成、利用、保管、交換、提供、消去、破棄における取り扱い手順を定める
4.1.5 外部の組織と情報をやり取りする際に、情報の取り扱いに関する注意事項について合意を取る
4.1.6 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
4.1.7 情報セキュリティに関するルールの周知と、情報セキュリティに関わる知識習得の機会を与える

4.2 物理的セキュリティ

4.2.1 重要な情報を保管したり、扱ったりする場所の入退管理と施錠管理を行う
4.2.2 重要なコンピュータや配線は地震などの自然災害や、ケーブルの引っ掛けなどの人的災害が起こらないように配置・設置する
4.2.3 重要な書類、モバイル PC、記憶媒体などについて、整理整頓を行うと共に、盗難防止対策や確実な廃棄を行う

4.3 情報システム及び通信ネットワークの運用管理

4.3.1 情報システムの運用に関して運用ルールを策定する
4.3.2 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
4.3.3 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
4.3.4 通信ネットワークを流れる重要なデータに対して、暗号化などの保護策を実施する
4.3.5 モバイル PC や USB メモリなどの記憶媒体やデータを外部に持ち出す場合、盗難、紛失などに備えて、適切なパスワード設定や暗号化などの対策を実施する

4.4 情報システムのアクセス制御の状況及び情報システムの開発、保守におけるセキュリティ対策

4.4.1 情報（データ）や情報システムへのアクセスを制限するために、利用者 ID の管理（パスワードの管理など）を行う
4.4.2 重要な情報に対するアクセス権限の設定を行う
4.4.3 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、ISP サービス 等）を行う
4.4.4 無線 LAN のセキュリティ対策（WPA2 の導入等）を行う
4.4.5 ソフトウェアの選定や購入、情報システムの開発や保守に際して、情報セキュリティを前提とした管理を行う

4.5 情報セキュリティ上の事故対応

4.5.1 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に何をすべきかを把握する
4.5.2 情報セキュリティに関連する事件や事故等（ウイルス感染、情報漏えい等）の緊急時に、何をすべきかを把握する

【制度上の要求事項／考え方（１）】

制度上の要求事項		考え方
要配慮個人情報の取得に関する同意		
個人情報保護法 第17条第２項	個人情報取扱事業者は、法令に基づく場合等を除くほか、あらかじめ本人の同意を得ないで、要配慮個人情報を取得してはならない。	対象事業者は、あらかじめ本人の同意を得てから、要配慮個人情報である健診等情報を取得しなければならない。
要配慮個人情報の第三者提供に関する同意		
個人情報保護法 第23条第１項	個人情報取扱事業者は、あらかじめ本人の同意を得ないで、個人データを第三者に提供してはならない。	対象事業者は、要配慮個人情報である健診等情報を第三者提供する際には、あらかじめ本人の同意を得なければならず、オプトアウトによる第三者提供をしてはならない。
個人情報保護法 第23条第２項	個人情報取扱事業者は、オプトアウトによる要配慮個人情報の第三者提供は認められない。	
個人情報保護法 第23条第５項	委託（※１）、合併等による承継（※２）、共同利用（※３）は第三者提供にあたらない。	－

※１　例えば、保険者が被保険者に対してPHRアプリを保険者のサービスの一環として提供する際にPHRアプリの管理運営会社に個人データを提供する場合など

※２　例えば、PHR事業を別の企業に譲渡し、譲渡先企業に個人データを提供する場合など

※３　例えば、PHRサービスを行っている企業が、同グループに属する企業と共に総合的な健康サービスを提供するために取得時の利用目的の範囲内で個人データを利用する場合など

【制度上の要求事項／考え方（２）】

制度上の要求事項			考え方
利用目的の特定・制限・変更の場合の取扱い			
特定	個人情報保護法 第15条第１項	個人情報取扱事業者は、個人情報を取り扱うに当たっては、その利用の目的をできる限り特定しなければならない。	対象事業者は、健診等情報の利用目的をできる限り特定し、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ってはならず、範囲を超えて健診等情報を取り扱う場合は、あらかじめ本人の同意を得なければならない。
	個人情報保護法GL （通則編） 第15条第１項関係	個人情報取扱事業者は、利用目的の特定に当たっては、利用目的を単に抽象的、一般的に特定するのではなく、個人情報が個人情報取扱事業者において、最終的にどのような事業の用に供され、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ことが望ましい。	
制限	個人情報保護法 第16条第１項	個人情報取扱事業者は、あらかじめ本人の同意を得ないで、利用目的の達成に必要な範囲を超えて、個人情報を取り扱ってはならない。	
	個人情報保護法GL （通則編） 第16条第１項関係	個人情報取扱事業者は、利用目的の達成に必要な範囲を超えて、個人情報を取り扱う場合は、あらかじめ本人の同意を得なければならない。	
変更	個人情報保護法 第15条第２項	個人情報取扱事業者は、利用目的を変更する場合には、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行ってはならない。	
	個人情報保護法GL （通則編） 第15条第２項関係	個人情報取扱事業者は、特定された利用目的の達成に必要な範囲を超えて、個人情報を取り扱う場合は、本人の同意を得なければならない。	

【制度上の要求事項／考え方（３）】

制度上の要求事項		考え方
利用目的の通知、公表、明示		
個人情報保護法 第18条第１項	個人情報取扱事業者は、個人情報を取得した場合は、あらかじめその利用目的を公表している場合を除き、その利用目的を本人に通知又は公表しなければならない。	対象事業者は、要配慮個人情報である健診等情報を、取得する際は、あらかじめその利用目的を公表している場合を除き、その利用目的を、本人に通知するか、又は公表しなければならず、書面で取得する際は、あらかじめ本人にその利用目的を明示しなければならない。その際、社会通念上、本人が認識できる場所及び文字の大きさで記載する等、本人が実際に利用目的を確認できるよう留意することが望ましく、プライバシーポリシー、プライバシーステートメント等を公表し、あらかじめ、対外的に分かりやすく説明することも重要である。
個人情報保護法 第18条第２項	個人情報取扱事業者は、書面（電磁的記録を含む）に記載された個人情報を取得する場合は、あらかじめ本人にその利用目的を明示しなければならない。	
個人情報保護法GL （通則編） 第18条第２項関係	個人情報取扱事業者は、（利用目的条項を記載する場合は）社会通念上、本人が認識できる場所及び文字の大きさで記載する等、本人が実際に利用目的を確認できるよう留意することが望ましい。	
個人情報保護法 第35条第１項・第２項	個人情報取扱事業者は、個人情報の取扱いに関する苦情の適切かつ迅速な処理に努めなければならず、その目的を達成するために必要な体制の整備に努めなければならない。	
個人情報保護法GL （通則編） 第35条関係	個人情報取扱事業者は、消費者等本人との信頼関係を構築し事業活動に対する社会の信頼を確保するためには、「個人情報保護を推進する上での考え方や方針（いわゆる、プライバシーポリシー、プライバシーステートメント等）」を策定し、それをホームページへの掲載又は店舗の見やすい場所への掲示等により公表し、あらかじめ、対外的に分かりやすく説明することや、委託の有無、委託する事務の内容を明らかにする等、委託処理の透明化を進めることも重要である。	

【制度上の要求事項／考え方（４）】

制度上の要求事項		考え方
データの消去		
個人情報保護法 第19条	個人情報取扱事業者は、利用する必要がなくなったときは、当該個人データを遅滞なく消去するよう努めなければならない。	対象事業者は、事業終了、その他の健診等情報の利用が必要なくなった場合又は本人の求めがあった場合、健診等情報を消去することが望ましい。
個人情報保護法 第35条第１項	個人情報取扱事業者は、個人情報の取扱いに関する苦情の適切かつ迅速な処理に努めなければならない。	
個人情報保護法GL Q＆A A3-12-2	令和２年改正法（※）において利用の停止又は消去の請求の要件が緩和されたことにより将来的には対応が必要になる場合があることも踏まえ、適切に利用停止又は消去の請求に応じることが望ましい。	
データの消去（目的外利用等）		
個人情報保護法 第30条第１項	本人は、目的外利用又は不正取得にされた保有個人データについて、利用停止又は消去（以下、この頁において「利用停止等」という）を請求できる。	（健診等情報の消去に関する条件が緩和され、消去義務化の範囲が広がることが想定される。 （消去義務について詳しく記述される令和２年改正個人情報保護法GLは令和３年６月以降に公表予定（第144回個人情報保護委員会資料より）））
個人情報保護法 第30条第２項	個人情報取扱事業者は、利用停止等の請求を受けた場合、保有個人データの利用停止等を行わなければならない。ただし、当該保有個人データの利用停止等に多額の費用を要する場合その他の利用停止等を行うことが困難な場合であって、本人の権利利益を保護するため必要なこれに代わるべき措置をとるときは、この限りでない。	
令和２年改正 個人情報保護法（※） 第30条第５項	本人は、個人情報取扱事業者が保有個人データを利用する必要がなくなった場合、個人情報の漏えい等が発生した場合、本人の権利又は正当な利益が害されるおそれがある場合には、利用停止等を請求できる。	
令和２年改正 個人情報保護法（※） 第30条第６項	個人情報取扱事業者は、利用停止等の請求を受けた場合、保有個人データの利用停止等を行わなければならない。	

※　（施行日：令和２年６月12日から起算して２年を超えない範囲内において政令で定める日）

【制度上の要求事項／考え方（５）】

制度上の要求事項		考え方
第三者提供の同意取得に際しての明示		
個人情報保護法 第23条第１項	個人情報取扱事業者は、あらかじめ本人の同意を得ないで、個人データを第三者に提供してはならない。	対象事業者は、健診等情報を民間事業者に対して提供・連携する場合、本人に対して、事業の規模及び性質、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。）等に応じて合理的かつ適切な範囲の内容を明確に示さなければならない。なお、提供先を個別に明示することまでが求められるわけではないが、想定される提供先の範囲や属性を示すことは望ましい。
個人情報保護法GL （通則編） 第23条第１項関係	個人情報取扱事業者は、同意の取得に当たっては、事業の規模及び性質、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さなければならない。	
個人情報保護法GL Q&A A5-9	個人情報取扱事業者は、提供先を個別に明示することまでが求められるわけではない。もっとも、想定される提供先の範囲や属性を示すことは望ましいと考えられる。	

【制度上の要求事項／考え方】

制度上の要求事項		考え方
データ内容の正確性の確保と適切な保存		
個人情報保護法 第19条	個人情報取扱事業者は、利用目的の達成に必要な範囲内において、個人データを正確かつ最新の内容に保つとともに、利用する必要がなくなったときは、当該個人データを遅滞なく消去するよう努めなければならない。	対象事業者は、利用目的の達成に必要な範囲内で、設定された保存期間、事業終了又は利用者が利用を終えるまで、健診等情報を適切に維持・保存、管理しなければならない。
個人情報保護法GL （通則編） 第19条関係	個人情報取扱事業者は、利用目的の達成に必要な範囲内において、個人情報データベース等への個人情報の入力時の照合・確認の手続の整備、誤り等を発見した場合の訂正等の手続の整備、記録事項の更新、保存期間の設定等を行うことにより、個人データを正確かつ最新の内容に保つよう努めなければならない。	
個人情報保護法 第20条	個人情報取扱事業者は、個人データの漏えい、滅失又はき損の防止その他の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なければならない。	
個人情報保護法 第28条第１項	本人は、個人情報取扱事業者に対し、当該本人が識別される保有個人データの開示を請求することができる。	対象事業者は、健診等情報の開示請求を受けたときは、当該情報を開示しなければならない。 （個人情報保護法は、本人が個人情報取扱事業者に対して提供した自己と関係する個人情報について、利用可能な形式で本人が受け取る権利や他事業者へのポータビリティの権利については定めていない。）
個人情報保護法 第28条第２項	個人情報取扱事業者は、前項の規定による請求を受けたときは、本人に対し、政令で定める方法により、遅滞なく、当該保有個人データを開示しなければならない。	

【制度上の要求事項／考え方】

制度上の要求事項		考え方
要配慮個人情報を取り扱う事業者の適格性		
個人情報保護法 第４章第１節（個人情報取扱事業者の責務）	－	対象事業者は、個人情報保護法に基づく各種義務を負う。
マイナポータルAPIを利用する者の適格性		
マイナポータルAPI利用規約 第３条第２項	マイナポータルAPIを利用する者は、以下に掲げる事項を満たすこと又は行うことを明らかにする。 １：役員若しくは担当部署責任者に行政手続における特定の個人を識別するための番号の利用等に関する法律（平成25年法律第27号）の規定若しくは暴力団員による不当な行為の防止等に関する法律（平成３年法律第77号）の規定若しくはこれらに相当する外国の法令の規定に違反し、又は刑法（明治40年法律第45号）若しくは暴力行為等処罰に関する法律（大正15年法律第60号）の罪を犯し、罰金の刑（これに相当する外国の法令による刑を含む。）に処せられ、その刑の執行を終わり、又はその執行を受けることがなくなった日から５年を経過しない者がないこと。 ２：取得しようとする自己情報について、本人同意を得た期間に限り保持し、及び本人同意を得た目的に限り利用し、並びにその機密性を維持すること。 ３：内閣府大臣官房番号制度担当室が定める情報セキュリティ要求事項を遵守すること。	マイナポータルAPIを利用する者は、役員若しくは担当部署責任者における過去に一定の刑事罰を受けたことがないこととといった社会的信用、取得しようとする自己情報についての適切な取扱い、一定のセキュリティ要求事項の遵守といった適格性の証明が求められる。