資料４

# 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（案）

令和３年４月

（令和●年●月改定）

（総務省、厚生労働省、経済産業省）

## 改定履歴

| | |
|---|---|
| 令和３年４月 23 日 | 「民間 PHR 事業者による健診等情報の 取扱いに関する基本的指針」を策定 |
| 令和４年４月１日 | 個人情報の保護に関する法律の一部改正にあわせて、「民間 PHR 事業者による健診等情報の 取扱いに関する基本的指針」を一部改定 |

## 目次

## はじめに

※赤字：内容的な修正、青字：形式的な修正

近年、民間事業者によって、健康診断結果をはじめとする、体重、血圧、血糖値等の情報等の個人の保健医療情報いわゆる Personal Health Record（以下「PHR」という。）を用いて、個人の健康維持や生活改善の支援をはじめとした多種多様なサービスが提供されている。さらに、我が国では、平成 29 年６月にマイナポータルを通じた予防接種歴の提供を開始し、その後、乳幼児健診結果、特定健診結果、レセプトの薬剤情報等、提供する情報を順次拡大することを通じ、国民の予防、健康づくりの推進等を進めている。

このような背景から、本指針は、安全、安心な PHR（Personal Health Record）サービスの利活用の促進に向けて、PHR ~~を取り扱う~~サービスを提供する者による PHR の適正な利活用が効率的かつ効果的に実施されることを目的として、PHR サービスを提供する者が遵守すべき事項を示すために策定するものである。

本指針では、１．１で定義する健診等情報を取り扱うサービス提供者が法規制により遵守を求められている事項に加えて、適正な PHR の利活用を促進するために遵守することが必要と考えられる事項について提示する。

**コメントの追加 [A1]:** 第１５回民間利活用作業班でのご意見を受け、後続の「PHR サービス提供者」と平仄を合わせるため修正。

## １．本指針の基本的事項

### １．１．本指針の対象とする情報の定義

本指針が対象として想定する PHR サービスにおいて活用される情報としては、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[1]。以下「個人情報保護法」という。）上の要配慮個人情報[2]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。）とする。

・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のある情報

※健診等情報の具体例として、乳幼児健診、診療情報（なお、薬剤情報、検査情報等も含む）、特定健診等が挙げられる。
※「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」は、健康保険組合等から入手する場合又は個人が自らアプリ等に入力する場合も含む。

**コメントの追加 [A2]:** 関係省庁からのコメントを踏まえ、「感染症情報やアレルギー情報等も含まれることが想定されることから」、「等」を追記。

### １．２．本指針の対象者

本指針の対象者は、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。）とする。

※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。

---

[1] 個人情報の保護に関する法律等の一部を改正する法律（令和２年法律第４４号）を参照
[2] 個人情報保護法 第２条第３項及び個人情報の保護に関する法律施行令（平成 15 年政令第 507 号。以下「個人情報保護法施行令」という。）第２条（詳細は用語集に記載）

※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。

**１．３．本指針に記載のない事項の取扱い**

本指針は、個人情報保護法を踏まえ、「個人情報の保護に関する法律についてのガイドライン（通則編）」（平成 28 年個人情報保護委員会告示第６号。以下「個人情報保護法についてのガイドライン（通則編）」という。）並びにマイナポータル API 連携に際して遵守が求められる「マイナポータル API 利用規約」（令和２年内閣府大臣官房番号制度担当室）、「マイナポータル自己情報取得 API 利用ガイドライン」（令和元年内閣府大臣官房番号制度担当室）及び「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」（独立行政法人情報処理推進機構（以下「IPA」という。））の「４．共通して実施すべき対策」を基礎とし、最近の技術動向等を反映すべく、IPA の中小企業の情報セキュリティ対策ガイドライン第 3.1 版、総務省のクラウドサービス提供における情報セキュリティ対策ガイドライン第３版及び内閣サイバーセキュリティセンター（以下「NISC」という。）のインターネットの安心・安全ハンドブックを踏まえ、PHR サービス提供者が行う健診等情報の適正な取扱いの確保に関する活動を支援するために、具体的な遵守すべき事項を示すものである。

なお、本指針は、個人情報保護法上の主な要求事項を記載しており、本指針に記載のない事項及び関係条文については、上記法令等に加え、「個人情報の保護に関する法律についてのガイドライン（外国にある第三者への提供編）」（平成 28 年個人情報保護委員会告示第７号）、「個人情報の保護に関する法律についてのガイドライン（第三者提供時の確認・記録義務編）」（平成 28 年個人情報保護委員会告示第８号）、「個人情報の保護に関する法律についてのガイドライン（仮名加工情報・匿名加工情報編）」（平成 28 年個人情報保護委員会告示第９号）、「個人情報の保護に関する法律についてのガイドライン（認定個人情報保護団体編）」（令和年個人情報保護委員会告示第７号）及び「「個人情報の保護に関する法律についてのガイドライン」に関する Q&A」（平成 29 年個人情報保護委員会）の最新版をそれぞれ参照されたい。

さらに、自治体は、「個人情報の保護に関する法律についてのガイドライン（行政機関等編）」（令和４年１月、個人情報保護委員会）、健康保険組合又は国民健康保険組合は、「健康保険組合等における個人情報の適切な取扱いのためのガイダンス」（平成 29 年４月 14 日、個人情報保護委員会、厚生労働省）又は「国民健康保険組合における個人情報の適切な取扱いのためのガイダンス」（平成 29 年４月 14 日、個人情報保護委員会、厚生労働省）についても適用対象となる。

また、個人が保有する医療情報（医療に関する患者情報を含む情報）[3]を利活用した PHR サービスの提供にあたっては、「健康寿命延伸産業分野における新事業活動のガイドライン（平成 26 年 3 月 31 日、厚生労働省、経済産業省）」に記載されているとおり、医師法第 17 条に規定する「医業」又は保健師助産師看護師法第 5 条に規定する「診療の補助」のいずれにも該当しない範囲とすることに加え、健康保険法第 63 条第 3 項に規定する患者が自らの意思により自由に医療機関等を選定できること等、関連法令等への遵守することが求められる。加えて、患者等の指示に基づいて医療機関等から医療情報を受領する場合は、「医療情報を取り扱う情

[3] 医療情報システムの安全管理に関するガイドライン第 6.0 版（概説編）2.2

報システム・サービスの提供事業者における安全管理ガイドライン」（令和２年８月、総務省、経済産業省）の遵守が求められる。

## 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

**① 個人情報保護法に基づく遵守すべき事項**

PHR サービス提供者は、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なければならない[4]。

具体的に講じるべき対策の内容に関しては、下記（２）に掲げる対策の例を参照し、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。）並びに、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対策を講じなければならない[5]。

**② その他の法令等に基づく遵守すべき事項**

上記①によるほか、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、必要な措置を講じなければならない。

#### （２） 本指針に基づく遵守すべき事項

PHR サービス提供者が情報セキュリティ対策を講じるに当たっては、サービスの提供に必要なリスクアセスメント（リスクの特定・評価・分析）を行い、これらを踏まえたリスク対策を行う一連のプロセス、すなわち、リスクマネジメントの実施が求められる。

さらに、PHR サービス提供者が講じる情報セキュリティ対策を含め、サービス提供上、必要と考えられる規定やルール等は文書（例えば、個人情報取扱規程、開発・調達管理規程、運用管理規程、各種手順書、マニュアル類等）を作成し、これに基づく運用を実施することが求められる[6]。

以下では、「PHR サービス提供者が情報セキュリティを確保する上で講じるべき対策」について示す。各項目においては、実施すべき「対策」を記載し、その下に当該対策を実現する上での具体的な「対策のポイント」を示し、更に、分かりやすさの観点から、必要に応じて、より細かな「対策の例」を追加している。

PHR サービス提供者において具体的な対策を検討する上では、このうち、対策のポイントの部分を参照し、当該部分に規定される内容又はそれと同等程度以上の対策を講じることが求められる。

~~さらに、PHR サービス提供者が講じる情報セキュリティ対策を含め、サービス提供上、必要と考えられる規定やルール等は文書（例えば、個人情報取扱規程、開発・調達管理規程、運用管理規程、各種手順書、マニュアル類等）を作成し、これに基づく運用を実施することが求められる[7]。~~

**コメントの追加 [A3]:** 第１５回民間利活用作業班でのご意見を受け、見やすさの観点から、遵守すべき事項と講じるべき事項の記載をそれぞれまとめるべく、移動させた。

**コメントの追加 [A4]:** 対策の例の位置づけについてはこちらにまとめて記載。
また、第１５回民間利活用作業班での、「意図を踏まえた例示が望ましい」というご意見に関連して、チェックシートの項目番号の修正を実施し、チェックシートから本指針の内容を参照しやすく工夫した。

[4] 個人情報保護法 第 23 条
[5] 個人情報保護法についてのガイドライン（通則編） 3-4-2 安全管理措置
[6] 個人情報保護法についてのガイドライン（通則編） 10-1 基本方針の策定及び 10-2 個人データの取扱いに係る規律の整備
~~[7] 個人情報保護法についてのガイドライン（通則編） 10-1 基本方針の策定及び 10-2 個人データの取扱いに係る規律の整備~~

【凡例】

A） 対策

➢ 対策のポイント

（例）

・ 対策の例

## ①情報セキュリティに対する組織的な取り組み

### 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こと

➢ 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すること。

### 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

➢ 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つこと。

（例）

・ 情報セキュリティ対策は経営者のリーダーシップで IT 活用を推進する中で、情報セキュリティ対策の重要性を認識し、自らリーダーシップを発揮して対策を推進する。

・ 情報セキュリティ対策は、経営者が判断して意思決定し、サービスに求められる情報セキュリティ対策を主導する。

・ 情報セキュリティ対策（事故が起きてしまった場合の被害の拡大防止や、復旧対応も含む）を実施するために、必要な体制を構築する。

・ 経営者が定めた情報セキュリティに関する基本方針を作成し、従業員、関係者に周知する。　等

➢ 情報セキュリティポリシーを定期的に見直しすること。

（例）

・ 基本方針なども適宜見直しを行い、対策の追加や改善などを行うように、責任者・担当者に指示する。

・ 情報セキュリティ対策について、実施状況を点検させ、方針に沿って進んでいるか評価する。　等

### 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[8]

➢ 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すること。

（例）

・ 経営者は、組織全体にわたる情報セキュリティに責任を持つ情報セキュリティ責任者を任命する。　等

➢ 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、役割を徹底すること。

（例）

・ 懸念される事態に関連する情報や業務を整理し、損害を受ける可能性（リスク）へ対応できるよう、責任者・担当者を任命し、対策を検討させる。

・ 情報セキュリティ責任者は、組織が保有、提供するシステム、アプリケーション及びクラウドサービスの一覧を作成し、全ての責任者を定め、セキュリティとプライバシーに関する役割と責任を示す。

[8] 個人情報保護法についてのガイドライン（通則編）10-3　組織的安全管理措置（1）組織体制の整備

・ 情報セキュリティ責任者から部門責任者を通じて従業員への情報の伝達経路を確立する。
・ 緊急時の対応体制（被害原因を速やかに追究して被害の拡大を防ぐ体制整備、復旧手順の作成、緊急時の適切な指示）を整備する。　等

➢ **利用者向けの問い合わせ窓口を整備すること。**

（例）
・ 提供しているサービスに対し、利用者からの苦情、懸念又は質問を受け取り、対応するためのプロセスを構築する。
・ 利用者が、同意する際と同等の容易さで、健診等情報の取得時及び第三者提供時の同意の撤回を行えるように工夫する。
・ 個人情報保護管理体制として個人情報に係る苦情申出先を示す。　等

**D) 管理すべき重要な情報資産を区分する[9]**

➢ 管理すべき健診等情報を他の情報資産と区分すること。

（例）
・ 業務で利用する電子データや書類を以下の要領で、情報資産管理台帳を整備する。
  ✓ 情報資産管理台帳の作成
  ✓ 情報資産管理台帳にある健診等情報（サービス提供上、これに関連する情報）又はその他の要配慮個人情報、サービスに用いるその他の個人情報（決済情報等）、上記以外の個人情報保護法に規定される情報（個人関連情報、匿名加工情報、仮名加工情報等）等について区分するほか、これらの情報とその他の情報との区分
  ✓ 区分に応じた情報資産台帳上の明確化
  ✓ 情報資産台帳に基づく各情報の所在管理　等

➢ 情報資産の管理者を定めること。

（例）
・ 情報資産台帳上の区分に従い、取り扱う各情報資産について管理責任者を定める。　等

➢ 重要度に応じた情報資産の取扱指針を定めること。

（例）
・ 各情報資産の許容範囲(利用可能者、利用目的、利用方法、返却方法等)を明確にした上で管理するとともに、文書化する。
・ 組織が採用した情報分類体系に従って情報資産の取扱いに関する手順を策定し、実施する。　等

➢ 健診等情報を取り扱う人の範囲を定めること。**また、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すること。**

**E) 情報資産区分に基づいて、リスク管理をすること**

➢ **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すこと。**

（例）

[9] 個人情報保護法についてのガイドライン（通則編）10-3　組織的安全管理措置（1）組織体制の整備

・ 保有する情報資産について、情報セキュリティの３要素である「機密性（Confidentiality）」、「完全性（Integrity）」、「可用性（Availability）」の観点から、情報資産に対する脅威を抽出し、これによるリスクを洗い出す。
・ 対応すべきリスクを把握する際には、以下の観点が参考となる。
  ✓ 関連する業務や情報に係る外部状況（法律や規制、情報セキュリティ事故の傾向、取引先からの情報セキュリティに関する要求事項など）
  ✓ 内部状況（経営方針・情報セキュリティ方針、管理体制、情報システムの利用状況など） 等

➢ **情報資産に対するリスクを評価すること。**

（例）
・ 洗い出した情報資産について、対策の優先度を決めるため、リスク値（リスクの大きさ）を算定する。 等

➢ **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ること。**

（例）
・ リスクの大きな情報資産に対して、以下内容を踏まえ、必要な方針を決定する。
  ✓ リスクを回避する（リスク発生の根源となる事業や行為を取りやめる）
  ✓ リスクを低減する（リスクを低減するための対策を講じる）
  ✓ リスクを移転する（発生したリスクを、保険等により移転する）
  ✓ リスクを受容する（リスクが実際に生じることを想定した上での対応を検討する）
  等

➢ **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すこと**

（例）
・ 決定したリスク対策を文書化し、規程を作成する。
・ サービス提供上、委託を行う者が提供するシステムやクラウドサービスについて、当事者間で合意された情報セキュリティリスク対策及びサービスレベルを文書化するとともに、これらの PHR サービス提供者によって確実に実施されることを担保するための措置を講じる。
・ 内部状況、外部状況の変化に応じて、リスクを評価し、レビューするなど、適宜リスク対策を見直す。 等

**F）個人情報の取扱状況を確認する手段を整備する[10]**

➢ **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としておく。**

（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

[10] 個人情報保護法についてのガイドライン（通則編）10-3 組織的安全管理措置（3）個人データの取扱状況を確認する手段の整備

**G) 健診等情報については、入手、作成、利用、保管、交換、提供、消去及び廃棄における取扱手順を定める**

- 各プロセスにおける作業手順を明確化し、決められた担当者が、手順に基づいて作業を行っていること。
- 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ること。

（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。
- 健診等情報の取扱い履歴を残しておく。
- 健診等情報を確実に消去又は廃棄する。　等

**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**

- 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ること。

（例）

- サービス提供を行うための委託先において、自社と同等のセキュリティ対策が講じられることを確認し、その実施を契約等により求める。
- 委託等の性格上、個別に契約や覚書を交わすことができない場合は、委託先のサービス規約や情報セキュリティに関わる対応方針を確認したうえで選定する。
- 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、受渡し、返却及び廃棄等について、注意事項を含める。
- サービス提供目的でクラウドサービスを導入する場合に、クラウドサービスの特性を踏まえたデータおよびシステム管理を行う。例えば管理体制、サービス導入における設定等への対応、受託情報の取扱い、受渡し、返却及び廃棄等について、クラウドサービスの特性を踏まえた注意事項を含める。
- 関係者のみにデータの取扱いを制限すること。
- 取決めに基づいて外部の組織との間で情報を授受する場合、情報の受け渡しの証跡が残せる形で行う（情報受渡書の授受、データのアップロード又はダウンロードを行った記録等）。
- 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。
- 自身の責任範囲をサービスレベル合意書（SLA）等により文書化し、クラウド利用者に明確に示す。　等

**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[11]**

- 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、監督を行うこと。

（例）

- 個人情報保護法では、個人データの取扱いを委託する場合は、委託先にも情報セキュリティ対策を実施してもらう必要がある旨、委託先の理解を促す。
- 重要な情報や個人情報などセキュリティ事故の影響が大きい情報の授受が行われる場合には、委託先にセキュリティ対策についての要望を伝え、取扱い上の対応に関する理解を促す。
- 委託先の健診等情報の取扱状況を把握し、対策が確実に実施される措置を講じる。　等

- 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すること。

（例）

[11] 個人情報保護法第 24 条及び個人情報保護法についてのガイドライン（通則編）3-4-4 委託先の監督

・ 自社が提供するサービスのセキュリティリスクを勘案して、状況に応じて最も適した委託先の選定・契約方法を採用する。
・ 委託先や調達する製品について、過去にセキュリティ対応上のトラブルを起こしていないか、適切な改善措置が講じられているかを確認する。
・ 外部にプログラムや IT 機器の開発を委託する場合、情報の取扱いが厳密でない外国に対して、「オフショア開発」で業務が再委託する際には、国内での保護と同等の情報の保護がなされることを確認する。
・ 必要に応じて ISMS、プライバシーマーク等の第三者認証を取得している企業から委託先を選定する。　等

➢ **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うこと。**

（例）
・ 自社のサービス提供に必要とされるクラウドサービスのセキュリティ対策をあらかじめ検討し、それらを備えたクラウドサービスを選定する。
・ サービス提供に用いるクラウドサービスの範囲と情報を検討し、利用サービスの切り分けや運用ルールを明確にする。
・ サービス提供に用いるクラウドサービスで取り扱う情報が漏えい、改ざん、消失したり、サービスが停止したりした場合の影響を確認し、対策を講じる。
・ サービスの稼働率、障害発生頻度、障害時の回復目標時間などのサービス品質保証の提示・確認するとともに、クラウドサービス提供事業者の信頼性を確認する。

＜その他の確認内容の例＞
✓ サービスに付帯するセキュリティ対策の公開
✓ 利用者サポートの体制の確認
✓ 利用終了時のデータの確保
✓ 適用法令や契約条件の確認
✓ データ保存先の地理的所在地の確認

・ 利用するクラウドサービスにおけるセキュリティが、自社のルールと矛盾がないことを確認する。　等

**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[12]**

➢ 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すること。

（例）
・ 計画した情報セキュリティ対策が、本当に実行されているか、見落としている対策はないか、対策がセキュリティ事故防止のために役に立っているか、を確認する。
・ 点検の結果を経営者に報告し、経営者の意図するセキュリティ対策が実現できているかの確認と評価をする。　等

➢ 外部の主体による監査活動と合わせて、監査を実施すること。

（例）
・ 営業秘密や個人情報等の特に十分な対策が必要な場合には、第三者による情報セキュリティ監査を実施する。　等

**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[13]**

[12] 個人情報保護法についてのガイドライン（通則編） 10-5　物理的安全管理措置（5）取扱状況の把握及び安全管理措置の見直し
[13] 個人情報保護法についてのガイドライン（通則編）10-4　人的安全管理措置

- 従業者を採用する際に、守秘義務契約又は誓約書を交わしていること。
- 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ること。
- 違反した従業員に対する懲戒手続きが整備されていること。

（例）
- 従業員が、情報セキュリティポリシー又はクラウドサービス提供上の契約に違反した場合の対応手続を備える。　等

- 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ること。

**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[14]**

- ポリシー及び関連規程を文書化し、従業員に理解させること。

- 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ること。

（例）
- 全ての従業員に対して、情報セキュリティポリシーに関する意識向上のための適切な教育・訓練を実施すること。
- 組織のトレーニング結果を情報セキュリティ責任者にフィードバックすること。
- 従業員が、情報セキュリティポリシー又はクラウドサービス提供上の契約に違反した場合の対応手続を備える。　等

**② 物理的セキュリティ**

**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 [15]**

- 健診等情報を保管したり、扱ったりする区域を定めていること。

（例）
- 健診等情報を保管する区域を定めるとともに、その区域でのセキュリティを保つため、当該区域での作業に関する手順を設計し、適用する。　等

- 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ること。

（例）
- オフィス、部屋及び施設に対する物理的セキュリティを設計し、適用する。
- 重要な物理的セキュリティ境界の出入口に破壊対策ドアを設置する。
- 重要な物理的セキュリティ境界に警備員を常駐させる。
- 不正な侵入者であることが判別できるよう、健診等情報を保管している部屋への入出が許可されている者に名札、入出許可証の着用を求める。　等

- 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、入退の記録を取得していること。

[14] 個人情報保護法についてのガイドライン（通則編）10-4　人的安全管理措置
[15] 個人情報保護法についてのガイドライン（通則編） 10-5　物理的安全管理措置(1) 個人データを取り扱う区域の管理

**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**

- 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すること。

  （例）
  - 地震・水害、その他の自然災害や火災、気象による環境変化（高温、多湿等）に対する対策を行う。
  - 重要なコンピュータ等を設置する場所では、設置されている機器等による発熱や結露等を抑えるのに十分な容量の空調を提供する。
  - 重要なコンピュータ等について、放水等の消火設備の使用に伴う汚損に対する対策（システム対応の消火器の設置等）を講じる。
  - 重要なコンピュータ等を設置するサーバルームには火災検知・通報システム及び消火設備を備える。
  - 情報処理施設に雷が直撃した場合及び誘導雷が発生した場合を想定した対策を講じる。
  - 重要なコンピュータ等の作業に伴う静電気対策を講じる。　等

- 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すること。

  （例）
  - サーバルームやラックの鍵管理を行う。
  - 暗証番号による入室管理を行う場合には、暗証番号は関係者のみが知りうる状態に置き、定期的に変更を行う。　等

- 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すること。

  （例）
  - データを伝送する又は情報サービスをサポートする通信ケーブル及び電源ケーブルの配線は、傍受、妨害又は損傷から保護する。
  - 装置は、サポートユーティリティの不具合による、停電、その他の故障から保護する。
    等

- 重要なシステムについて、地震等による転倒防止、水濡れ防止及び停電時の代替電源の確保等を行っていること。

  （例）
  - 重要なコンピュータ等を設置する場所には、停電や電力障害が生じた場合に電源を確保するための対策を講じる。　等

- 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ること。

  （例）
  - 装置は、可用性及び完全性を継続的に維持することを確実にするために、正しく保守する。
  - 装置、情報又はソフトウエアは、事前の認可なしでは、構外に持ち出さないようにする。

・ 構外にある情報資産に対しては、構外での作業に伴った、構内での作業とは異なるリスクを考慮に入れて、セキュリティを適用する。
・ 無人状態にある装置が適切な保護対策を備えていることを確実にする。　等

**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）**[16]

- 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、施錠管理を行うこと。
- 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うこと。

（例）
・ 書類及び取外し可能な記憶媒体に対するクリアデスク方針、並びに情報処理設備に対するクリアスクリーン方針を適用する。
・ 郵便物、FAX 及び印刷物等を放置しない。また、重要な書類の裏面を再利用しない。
等

- 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、盗難防止対策の実施すること。

（例）
・ 施錠忘れ対策を実施する。　等

**（漏えい防止対策）**[17]

- 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、窃視対策を行うこと。

（例）
・ 離席時に画面の覗き見等の防止するために、待ち受け画面にロックをするなどの方策を行う。
・ 臨席等から画面の覗き見等の防止するために窃視防止スクリーンなどの対策を行う。
等

- 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、規則を定めること。

（例）
・ 紙、磁気テープ、光メディア等の媒体の保管・在庫状況や利用状況の管理を適切に行う。
・ 磁気テープ、光メディア等の媒体へ書き込みを行える機器について、必要な範囲に制限し、適切に管理する。
・ 情報を格納した媒体は、輸送の途中における、認可されていないアクセス、不正使用又は破損から保護する。　等

- 許可なく私有 PC を会社に持ち込んだり、私有 PC で業務を行ったりしないこと。

（例）
・ BYOD の実施にあたっては、想定されるセキュリティ上のリスクを事前に把握し、判断する。

[16] 個人情報保護法についてのガイドライン（通則編） 10-5　物理的安全管理措置（2）機器及び電子媒体等の盗難等の防止
[17] 個人情報保護法についてのガイドライン（通則編） 10-5　物理的安全管理措置（3）電子媒体等を持ち運ぶ場合の漏えい等の防止

・ 業務で利用するデータ等が BYOD を行う端末、その他許可されていない領域に保存されないための対策を行う。
・ BYOD の実施には企業が運用のルールを設定する。 等

**（健診等情報の確実な廃棄・消去）**[18]

➢ 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すること。

➢ 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うこと。

（例）
・ 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、確実な方法により消去する。
・ 機器及び媒体を正式な手順に基づいて廃棄する。
・ 装置、情報又はソフトウエアは、事前の認可なしでは、構外に持ち出さないようにする。
・ 記憶媒体を内蔵した全ての装置は、処分又は再利用する前に、取扱いに慎重を要するデータ及びライセンス供与されたソフトウエアを全て消去していること、若しくはセキュリティを保って上書きしていることを検証する。 等

**③ 情報システム及び通信ネットワークの運用管理**

**A) 情報システムの運用に関して運用ルールを策定する**

➢ 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ること。
➢ 情報システムの運用手順書（マニュアル）を整備していること。
➢ システムの運用状況を点検していること。

（例）
・ 各情報資産の管理責任者は、自らの責任範囲における全ての情報セキュリティ対策が、情報セキュリティポリシーに則り正しく確実に実施されるように、定期的にレビュー及び見直しを行う。
・ 組織の情報セキュリティのための方針等及び規程類に関し、システムや提供するサービスが、定めに従って技術的に遵守されて いることをレビューする。
・ サービスの提供に用いるシステム等が、情報セキュリティポリシー上の要求を遵守していることを確認するため、定期的に検証・監査する。
・ システムの検証を伴う監査要求事項及び監査活動は、業務プロセスの中断を最小限に抑えるために、慎重に計画し、実施する。 等

➢ 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）を取得していること。[19]

（例）
・ 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

[18] 個人情報保護法についてのガイドライン（通則編） 10-5 物理的安全管理措置（4）個人データの削除及び機器、電子媒体等の廃棄
[19] 個人情報保護法についてのガイドライン（通則編）10-3 組織的安全管理措置（2）個人データの取扱いに係る規律に従った運用

- 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）

・ ログファイルをどのように管理するかの方針を、組織として定めておく。
・ 利用者の活動、例外処理、過失及び情報セキュリティ事象を記録したイベントログを取得し、保持し、定期的にレビューする。また、PHR サービス提供者は、クラウドサービス提供者に、ログ取得機能を提供するよう求める。
・ 取得したログ機能及びログ情報は、安全に管理する。　等

➢ **設備（具体例）の使用状況を記録していること。**

（例）
・ 他者が提供するクラウドサービス等を定常的に監視・レビューし、運用に関する記録及び報告を常に実施するよう求める。
・ 定期的に監査を実施することについて、当該提供先と合意し文書化する。　等

➢ **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すること。**

（例）
・ システムの実務管理者及び運用担当者の作業は、記録し、そのログを保護し、定期的にレビューする。　等

➢ **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ること。**

（例）
・ 情報セキュリティ監視(稼働監視、障害監視、パフォーマンス監視等)の実施基準・手順等を定める。
・ サービスの提供に用いるアプリケーションの運用・管理に関する手順書を作成する。またサービスの提供に用いるプラットフォーム、サーバ・ストレージ、情報セキュリティ対策機器、通信機器の運用・管理に関する手順書を作成する。
・ システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラム(データベースの中身を強制的に書き換えることができる機能や一時的にポートを開放する機能等)の使用は、制限し、厳しく管理する。PHR サービス提供者は、サービス内で利用される全てのユーティリティプログラムのための要求事項を特定する。
・ 運用管理端末に、許可されていないプログラム等はインストールしない。
・ サービスの稼働監視、障害監視、パフォーマンス監視及びセキュリティインシデント監視を行う。
・ 稼働停止や異常、障害、パフォーマンス低下等を検知した場合は、利用者に速報する。
等

➢ **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すること**

（例）
・ パソコンやサーバなどのハードウエアやソフトウエアに関するサービス提供に必要な保有状況情報・構成情報を取りまとめて管理する。
・ 重要なコンピュータ等における情報セキュリティに影響を与える情報処理設備及びシステムの変更を管理する。
・ 運用システムに関わるソフトウエアの導入を管理するための手順を実施する。
等

- 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・方法等を取り決めること。

（例）

・ セキュリティ対策を実施するために、クラウドサービス提供に用いるサーバやネットワークのセキュリティ対策はクラウドサービス提供事業者側の責任であるが、クラウドサービス利用者側のネットワークや端末に対するセキュリティ対策は、原則としてクラウドサービス利用者側の責任とするなど、クラウドサービス提供事業者はクラウドサービス利用者との運用上の責任の範囲を明確に取り決め（責任共有モデル）。

・ クラウドサービス利用者が適切なセキュリティ対応を講じられるように、クラウドサービス提供事業者はセキュリティ対策上可能な範囲で、セキュリティ対策の状況をクラウドサービス利用者に提供する。

- サービスに付帯するセキュリティ対策の公開
- 利用者サポートの体制の確認
- 利用終了時のデータの確保
- 適用法令や契約条件の確認
- データ保存先の地理的所在地の確認

等

**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**

- 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ること。

（例）

・ サービスの提供に用いるプラットフォーム、サーバ・ストレージについてマルウエア等に対する対策を講じる。

・ マルウエアから保護するために、検出、予防及び回復のための対策を実施すること。

・ 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・マルウエア定義ファイル（パターンファイル）は、稼働確認を行った上で、なるべく最新の状態にする。

・ プログラム実行や電子メール送受信、ウェブ閲覧などを、その内容（コンテンツ）によって制御することでマルウエア対策を実施する。　等

- 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）を活用すること。
- 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ること。
- 組織で許可されていないソフトウエ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ること。
- 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すること。

**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**

- 脆弱性の解消（修正プログラムの適用及び Windows update 等）を行っていること。

（例）

・ OS やソフトウエアには、稼働確認を行った上で、修正プログラムを適用する、もしくは最新版を利用する。

・ サーバやアプリケーションに対してスキャニングを行い、脆弱性などを検出する。　等

- 脆弱性情報及び脅威に関する情報の入手方法を確認し、定期的に収集すること。

（例）
- 利用中のシステムの技術的脆弱性に関する情報は、時機を失せずに獲得する。
- 外部の情報セキュリティサービスを利用することで、有効な対策を実施する。
- PHR サービス提供者は、提供するサービスに影響し得る技術的脆弱性の管理に関する情報を利用者が利用できるようにする。　等

- 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すること。

（例）
- 脆弱性に組織がさらされている状況を評価する。さらに、それらと関連するリスクに対処するために、適切な手段をとる。
- 許可されていない不正なコード実行からシステムメモリを保護するために、セキュリティ対策を実施する。　等

- 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、脆弱性の解消を行うこと。

（例）
- Web サイトの安全の維持するためには、サーバ OS やソフトウエアに対して脆弱性修正パッチの適用や安全な設定などを維持する。
- Web サイトの安全を維持するために、開発段階において、可能な限り脆弱性を解消する。また、開発を委託して脆弱性が原因で事故が発生した場合には、脆弱性対策については要求仕様に盛り込む。
- 電子データの原本性確保を行う。　等

- 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うこと。

**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**

- TLS（version1.3）等を用いて通信データを暗号化すること。ただし、対応が困難な場合は、Version1.2 によることも可能とするが、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うこと。

（例）
- 外部ネットワークを利用した情報交換において、情報を盗聴、改ざん、誤った経路での通信、破壊等から保護するため、通信の暗号化を行う。　等

- 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ること。
- 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ること。
- 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、暗号化を講じること。

（例）
- 情報を保護するための暗号利用に関する方針を策定し、実施する。

・ 組織が定めた方針に従って、システム内で使用する暗号鍵を生成・配布・保管・アクセス・廃棄する。
・ PHR サービス提供者は、クラウドサービス提供者に対し、PHR サービス提供者が処理する情報を保護するために、暗号を利用する対象やクラウドサービス提供者の対応範囲について情報提供を求める。　等

**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**

- 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、規程を定めていること。

（例）
・ モバイル機器を業務で用いることによって生じるリスクを管理するために、モバイル機器の利用方針を策定し、その方針を実施するために必要な情報セキュリティ対策を講じる。等

- 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ること。

（例）
・ モバイル機器を業務で用いることによって生じるリスクを管理するために、モバイル機器の利用方針を策定し、その方針を実施するために必要な情報セキュリティ対策を講じる。　等

- 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）を行うこと。
- 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すること。
- 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すること。
- 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うこと。

**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**

- 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すること。

**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**

**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** [20]

- 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うこと。

  （例）
  - パスワード管理システムは、対話式とすること、また、良質なパスワードを確実にする。
  - パスワードの認証に際して、通信内容を暗号化する。
  - パスワード再設定の通知がメールなどで送られて来た場合、それが本当にサービス側から送られてきたものかどうか、事実の確認することを周知する。　等

- 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すること。

  （例）
  - 利用者がサービス利用時に行う利用者認証を、３つの要素（「知識情報」、「所持情報」、「生体情報」）のうち、２つ以上の要素を用いて行う。　等

- 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し、運用すること。

  （例）
  - 情報システムの特権（コンピュータを管理するために与えられた最上位の権限）の利用申請、操作ログなどを管理すること。
  - 不要になったシステム管理者の ID を削除する。　等

- 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すること。

- 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ること。また、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すること。

  （例）
  - 英大文字小文字＋数字＋記号混じりで 10 桁以上を安全圏として推奨する。　等

- 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すること。

**B) 健診等情報に対するアクセス権限の設定を行う** [21]

- 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すること。

  （例）

[20] 個人情報保護法についてのガイドライン（通則編）10-6　技術的安全管理措置（1）アクセス制御及び（2）アクセス者の識別と認証

[21] 個人情報保護法についてのガイドライン（通則編）10-6　技術的安全管理措置（1）アクセス制御

・ アクセス制御方針は、業務及び情報セキュリティの要求事項に基づいて確立し、文書化し、レビューする。また、情報及びシステム機能へのアクセスは、アクセス制御方針に従って、制限する。
・ PHR サービス提供者は、サービスへのアクセス、クラウドサービス機能へのアクセス及び利用者データへのアクセスを制限できるようにクラウドサービス提供者にアクセス制御を提供するよう求める。
等

➢ 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すこと。

（例）
・ 従業員の雇用が終了又は変更となった場合のアクセス権や情報資産等の扱いについて、実施すべき事項や手続、確認項目等を明確にする。 等

➢ システム管理者のアクセス権限を適切に管理すること。

（例）
・ 情報システムの特権の権限付与を管理する。
・ 情報セキュリティ責任者は、システム管理者及びネットワーク管理者の権限の割当及び使用を制限する。 等

**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[22]**

➢ 外部との情報・データの転送に関するルールを整備すること。

（例）
・ あらゆる形式の通信設備を利用した情報転送を保護するために、正式な転送方針、手順及び対策を備える。
・ 外部ネットワークを利用した情報交換において、情報を盗聴、改ざん、誤った経路での通信、破壊等から保護するため、情報交換の実施基準・手順等を備える。
・ 組織と外部関係者との間で、業務情報のセキュリティを保った転送について、合意する。
・ 情報保護に対する組織の要件を反映する秘密保持契約又は守秘義務契約のための要求事項は、特定し、定めに従ってレビューし、文書化する。 等

**（外部から内部への不正アクセス対策）**

➢ 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すること。

（例）
・ セキュリティ侵害に関する通知について手順を確立し、文書化する。
・ 利用する全ての外部ネットワーク接続について、情報セキュリティ特性、サービスレベル(特に、通信容量とトラヒック変動が重要)及び管理上の要求事項を特定する。
・ 外部ネットワークの障害等を監視し、障害等を検知した場合は管理責任者に通報する。
・ システム又はシステムコンポーネントにデータ又は機能を埋め込み、データが盗み出されたり、不適切に変更、削除されたりしたかを検知する。
・ 攻撃者が目標を達成する能力を妨げるために、センサー又は監視機能等を配置する。

＜不正アクセス対策の例＞

[22] 個人情報保護法についてのガイドライン（通則編）10-6 技術的安全管理措置（3）外部からの不正アクセス等の防止

- EDR（Endpoint Detection and Response）
- IDS（Intrusion Detection System：侵入検知システム）
- IPS（Intrusion Prevention System：侵入防御システム）
- UTM（Unified Threat Management：統合脅威管理）

等

- 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、確実な認証を実施すること。

（例）
- 第三者が当該 PHR サービス提供者のサーバになりすますこと(フィッシング等)を防止するため、サーバ証明書の取得等の必要な対策を実施する。
- 多要素認証などで容易に不正アクセスできないように設定するなど、認証情報を適切に管理する。
- 外部及び内部からの不正アクセスを防止する措置(ファイアウォール、リバースプロキシの導入等)を講じる。　等

- 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すること。

（例）
- IT 機器などが乗っ取られたり、DDoS 攻撃に利用されたりする場合は、利用停止、ネット切断、通報の判断、周りを含めマルウエアの駆除、バックアップからの復旧などが図れる措置を講じる。　等

**（内部から外部への不正アクセス対策）**

- 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）を行っていること。

（例）
- 電子メールの添付ファイルや本文中の URL リンクを介したウイルス感染等への対応を周知するとともに、対策を実装する。
- 外部から配信されるアプリケーションを格納する場合には、組織が定めた方法により実施するよう手順によるものとし、承認されていないサイトからのダウンロードは行わない。　等

- 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ること。

（例）
- サービスの提供に用いるセッションのライフサイクルの制御(生成、破棄、タイムアウト検知)を行う。
- 通信セッションの真正性を保護する。
- 定められたアイドル時間を経過した場合、又は利用者から要求された場合、システムがセッションをロックすることによって以降のアクセスを遮断する。　等

**D) 無線 LAN のセキュリティ対策（WPA3 等の導入等）を行う**

- 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）の設定を行うこと。 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図ること。
- 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うこと。

**E) ソフトウエアの選定及び購入、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 [23]**

- 情報システムの設計時に安全性を確保し、継続的に見直すこと（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。）。

  （例）
  - 開発プロセスの種類にかかわらず、プロジェクトマネジメントにおいては、情報セキュリティに取り組む。　等

- 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）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すること。

  （例）
  - ソフトウエアまたはクラウド等のサービス提供事業者により提供されるシステム等について、目的・適用範囲・役割・責任・経営コミットメント・組織間の調整・コンプライアンスを取り扱う構成管理ポリシー及び構成管理ポリシーと関連する対応策の実施手順を策定・文書化する。
  - ソフトウエアまたはクラウド等のサービス提供事業者により提供されるシステム等の導入又は変更を管理することについて、当該サービス提供事業者と合意し文書化する。

  等

- 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すること。

  （例）
  - システムの最新のベースライン構成、システムコンポーネント一覧を把握・文書化する。
  - 構成管理の対象となるシステムに対する変更内容をレビューし、セキュリティへの影響を考慮した上で変更を許可する。また、変更に関する関連の活動を監査し、レビューする。
  - システムに対する変更に関して、物理的／論理的なアクセス制限を定義・文書化・承認の上、実施する。
  - プログラムソースコードへのアクセスは、制限する。　等

- 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ること。

  （例）
  - 開発プロセスの種類にかかわらず、システム開発時のプロジェクトマネジメントにおいては、情報セキュリティ対策に取り組む。　等

[23] 個人情報保護法についてのガイドライン（通則編）10-6　技術的安全管理措置（3）外部からの不正アクセス等の防止及び（4）情報システムの使用に伴う漏えい等の防止

- 外部委託によるソフトウエア開発を行う場合、使用許諾及び知的財産等について取り決めていること。

- 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、実施すること。

（例）
  - システム保守の目的、適用範囲、役割、責任等を策定、文書化し、関係する組織に配布する。
  - 保守契約、保守仕様書及び要求事項に従って、保守・修理を計画、実施、文書化し、記録をレビューする。
  - 保守要員の認可手順を確立し、認可された保守組織又は要員の一覧を維持する。
  - システムの保守ツールを承認・管理し、モニタリングするとともに、以前の保守ツール使用状況レビューする。
  - リモートによる保守及び診断が適切であることを確認の上、承認を行い、必要に応じてモニタリングする。リモート保守及び診断用ツールは、組織のポリシーに沿い、かつシステムのセキュリティ計画に記載されている通りである場合のみ、使用を許可する。
  - システムコンポーネントに障害が発生した場合、保守サポート契約に基づき、保守サポートを行う。　等

- 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ること。

**⑤ 情報セキュリティ上の事故対応**

**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**

- 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おくこと。
- 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、よく検討していること。

（例）
  - 大規模災害等における情報セキュリティ及び情報セキュリティマネジメントの継続のための要求事項を決定するとともに、プロセス・手順・対策を確立、文書化し、実施、維持する。
  - 情報セキュリティ継続のための対策が、大規模災害等の下で妥当かつ有効であることを確認するために、定められた間隔でこれらの対策を検証する。
  - 目的・適用範囲・役割・責任・経営コミットメント、組織間の調整及びコンプライアンスを取り扱う緊急時対応計画を策定するとともに、「緊急時対応計画」の実施手順を策定・文書化する。　等

- 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おくこと。

（例）
  - 緊急時に、システム又は個々のシステムコンポーネントの電源を遮断できる機能を提供するとともに、緊急時に電源を遮断する機能が、不正に起動されないようにする。　等

- 日常の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おくこと。

(例)

- 情報、ソフトウエア及びシステムのバックアップは、バックアップ方針に従って、定期的に実施し、バックアップ内容を検査する。
- PHR サービス提供者は、利用者にバックアップ機能の仕様を提供する。
- 利用者のデータ、アプリケーションの管理情報及びシステム構成情報の定期的なバックアップを実施する。
- バックアップされた情報が正常に記録され、正しく読み出すことができるかどうかについて定期的に確認する。
- バックアップは脅威の性格などを踏まえて、取得計画を作成する。例えばランサムウエア等による攻撃に備え、常時接続しない媒体でのバックアップも取得する。　等

- 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ること。

(例)

- 一次電源が失われた場合に、長期間使用可能な代替電源への切り替えを支援する、もしくは、短期無停電電源装置を用意する。
- 停電が発生した場合や電力が途絶えた場合に作動し、施設内の非常口と避難経路を照らす自動非常用照明をシステムに導入し、維持する。
- 提供するサービスの重要性や性格に応じて、代替通信サービスを確立する。　等

- 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おくこと。

(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を実施する。　等

- 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ること。

(例)

- 緊急時対応計画の有効性を判断して計画の欠陥を特定するために、緊急時対応計画のテストを実施する。
- 要員に対して、役割と責任に応じた緊急時対応トレーニングを実施する。　等

**B) 情報セキュリティに関連する事件又は事故等（マルウエア感染、情報漏えい等）の緊急時の対応手順を整理する[24]**

- マルウエ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おくこと。

(例)

[24] 個人情報保護法についてのガイドライン（通則編）10-3　組織的安全管理措置（1）組織体制の整備及び（4）漏えい等事案に対応する体制の整備

- マルウエア感染の場合、ウイルス定義ファイルを最新の状態にしたマルウエア対策ソフトにより、コンピュータの検査を実施し、マルウエア対策ソフトのベンダの Web サイト等の情報を基に、検出されたマルウエアの駆除方法等を試すことが必要となる。
- 全ての要員に対し、業務において発見あるいは疑いをもったシステムの脆弱性や情報セキュリティインシデント(サービス停止、情報の漏えい・改ざん・破壊・紛失、マルウエア感染等)について、どのようなものでも記録し、できるだけ速やかに管理責任者に報告できるよう手続を定め、実施を要求する。報告を受けた後に、迅速に効果的な対応ができるよう、責任体制及び手順を確立する。
- 利用者が情報セキュリティ事象を PHR サービス提供者に報告する仕組み及び PHR サービス提供者が情報セキュリティ事象を利用者に報告する仕組みを提供する。　等

➢ **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。**

(例)

- 大きな影響があるインシデントが発生した場合等の緊急時に迅速に対応するために体制を整備する。
- 組織内外の緊急連絡先・伝達ルートを整備・周知する。
- 緊急時対応に関する話し合いや訓練等を実施する。
- 関係者や IT 製品のメーカー、保守ベンダ等への連絡先を整理する。　等

➢ **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すること。**

(例)

- インシデントが疑われる兆候や実際の発生を検知する。
- 外部からの通報を受けたりした場合は、速やかに情報セキュリティ責任者に報告する。
- 情報セキュリティ責任者による、対応すべきインシデントの判断実施と報告する。
- インシデントが事業や利用者に与える影響を踏まえ、速やかにインシデント対応のための体制を立ち上げ、対応方針を指示する。　等

➢ **対策本部で対応方針を決定すること及び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。**

(例)

- インシデントからの復旧にあたって、原因を調査し、対応を検討する際は、発覚・発生日時や表面化している事象・被害・影響、発覚から現時点までの時系列での対応経過、現時点で想定される原因などの情報を整理する。
- IT 製品のメーカー、保守ベンダなどの外部専門組織や公的機関の相談窓口などに支援や助言を依頼する。
- 調査において事実関係を裏付ける情報や証拠を保全し、必要に応じてフォレンジック調査（パソコンのハードディスク、メモリ内データ、サーバやネットワーク機器のログ等の調査）を実施する。
- インシデント対応後は、停止したシステムやサービスを復旧し、経営者に対応結果を報告する。
- インシデントを再発させないために根本原因を分析し、新たな技術的対策の導入、ルールの策定、教育の徹底、体制整備、運用の改善など、抜本的な再発防止策を検討する。
等

➢ **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。**

(例)

- インシデントの被害拡大を防ぐために、二次的な被害が想定される場合などは、本人にその事実を報告する。

・ 本人への報告が困難な場合や、インシデントの影響が広く一般に及ぶ場合は、状況をウェブサイトやメディアを通じて公表する。
・ 受付専用の問い合わせ窓口を開設するなどして、その動向を速やかに把握し対応する。
・ インシデント対応完了後は、被害者や、影響を及ぼした取引先や顧客など関係者に対して、インシデントの対応状況や再発防止策などについて報告する。　等

➢ **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うこと。**

（例）
・ 普段から自社の情報セキュリティ対策や、事故が起きたときの対応について、業務上の関係者（顧客、取引先、委託先など）に明確に説明できるように経営者自身が理解し、情報セキュリティに関する取組方針を日常的により関係者に伝達する。
・ コミュニティへの参加で情報交換を積極的に行い、得られた情報について、業界団体、委託先などと共有する。
・ サイバー攻撃の脅威や攻撃の手口を知り、対策を講じる。
・ 情報セキュリティに関する最新動向を発信している公的機関などを把握し、常時参照することで備えるように情報セキュリティ担当者に指示する。
・ 大規模なサイバー攻撃の兆候や脆弱性の発覚をいち早く察知するため、IPA や NISC などの政府機関等による情報収集を行う。　等

**⑥ 外的環境の把握[25]**

**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**

## ２．２．第三者認証の取得

### （１）本指針に基づく遵守すべき事項

PHR サービス提供者は、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）を取得することで、客観的に安全管理措置を担保するよう努めなければならない。

ただし、マイナポータル API 経由で健診等情報を入手する PHR サービス提供者においては、第三者認証を取得しなければならない。

[25] 個人情報保護法についてのガイドライン（通則編）10-7 外的環境の把握

## 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**

**① 利用目的の特定[26]**

PHR サービス提供者は、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なければならない。また、PHR サービス提供者は、上記によって特定した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、仮に当該範囲を超える利用目的のために健診等情報を取り扱う場合は、後述するとおり、あらかじめ本人の同意を得なければならない。

また、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 PHR サービス提供者において、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なければならない。

**② 利用目的の変更[27]**

PHR サービス提供者は、健診等情報を取得する当初に公表又は通知していた利用目的を変更する場合について、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。この場合は、変更された利用目的を本人に通知するか、又は公表しなければならない。

なお、この「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」に関しては、変更後の利用目的が変更前の利用目的からみて、社会通念上、本人が通常予期し得る限度と客観的に認められる範囲となることが必要であり、それを超える範囲で変更する場合は、後述するとおり、改めての本人の同意取得が必要となる。

#### 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**

**① 利用目的の明示[28]**

PHR サービス提供者は、例えば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なければならない。

この場合、本人に対して、その利用目的を明確に示すことが必要であり、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方法による必要がある。

---

[26] 個人情報保護法 第 17 条第 1 項及び第 18 条第 1 項並びに個人情報保護法についてのガイドライン（通則編）3-1-1 利用目的の特定

[27] 個人情報保護法 第 17 条第 2 項及び第 21 条第 3 項並びに個人情報保護法についてのガイドライン（通則編）3-1-2 利用目的の変更

[28] 個人情報保護法 第 21 条第 2 項及び個人情報保護法についてのガイドライン（通則編）3-3-4 直接書面等による取得

**② 保有する健診等情報等の本人への開示**[29]

PHR サービス提供者は、本人からの請求があった場合、保有する当該本人に係る健診等情報（保有個人データ）を開示しなければならない。

具体的な開示の手続きに関しては各 PHR サービス提供者において定めることが必要であるが、例えば同一の本人から、複雑な対応を要する同一内容について繰り返し開示の請求があり、事実上問い合わせ窓口が占有されることによって他の問い合わせ対応業務が立ち行かなくなるなど、業務上著しい支障を及ぼすおそれがある場合等には、開示をしないことが認められている。

**（２） 本指針に基づく遵守すべき事項**

**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**[30]

PHR サービス提供者は、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なければならない。その際、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なければならない。

**３．２．同意取得**

**（１） 法規制に基づく遵守すべき事項**

**① 取得に係る事前の同意取得等**[31]

健診等情報のうち要配慮個人情報に該当するものは、その取得に際して、あらかじめ、本人からの同意取得が必要であり、原則、オプトアウト手続きによる取得は認められていない[32]。

また、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は、あらかじめ本人の同意を得なければならない。また、下記②に記載する事業の承継後に、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にも、あらかじめ本人の同意を得なければならない。

**② 第三者提供に係る事前の同意取得**

健診等情報の第三者提供には、個人情報保護法に基づき同意が不要となる場合を除き、原則として、あらかじめ、本人の同意が必要である。また、健診等情報のうち要配慮個人情報に該当するものについては、オプトアウト手続きによる第三者提供は認められていない[33]。

---

[29] 個人情報保護法 第 33 条第 1 項及び第 2 項並びに個人情報保護法についてのガイドライン（通則編）3-8-2 保有個人データの開示

[30] 個人情報保護法第 21 条第 1 項及び個人情報保護法についてのガイドライン（通則編）2-15「公表」

[31] 個人情報保護法第 18 条第 1 項及び第 18 条第 2 項及び第 20 条第 2 項並びに個人情報保護法についてのガイドライン（通則編）3-3-2 要配慮個人情報の取得

[32] 個人情報保護法第 22 条第 2 項

[33] 個人情報保護法第 27 条第 1 項及び第 27 条第 2 項並びに個人情報保護法についてのガイドライン（通則編）3-6-1 第三者提供の制限の原則及び 3-6-2-1 オプトアウトに関する原則

また、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さなければならない[34]。

ただし、PHR サービス提供者が、委託、事業承継又は共同利用により当該情報を提供する場合は、第三者提供に該当せず、例えば以下の場合に関しては、あらかじめ本人の同意を得る必要はない。[35]

なお、要配慮個人情報を第三者提供の方法により取得する場合、上記①及び②に従って、提供元が本人から必要な同意（要配慮個人情報の取得及び第三者提供に関する同意）を取得していることが前提となるため、提供を受けた PHR サービス提供者が、改めて本人から要配慮個人情報の取得に関する同意を得る必要はない。[36]

他方、健診等情報を第三者提供の方法により取得する場合、当該提供者について、その氏名又は名称及び住所及び法人にあってはその代表者の氏名、並びに当該提供者が提供された健診等情報を取得した経緯を確認しなければならない。[37]

**（健診等情報の第三者提供に係る同意取得が不要な場合の例）**

**【個人情報保護法に列挙される例外に該当する場合】[38]**

- 法令に基づく場合
- 人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき
- 公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき
- 国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。

**【第三者提供に該当しない場合の例】**

- 委託：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。
- 事業承継：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。
- 共同利用（※）：PHR サービスを行っている企業が、例えば同グループに属する企業等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共同利用する。

[34] 個人情報保護法についてのガイドライン（通則編）3-6-1 第三者提供の制限の原則
[35] 個人情報保護法第 27 条第 5 項
[36] 個人情報保護法についてのガイドライン（通則編）3-3-2 要配慮個人情報の取得
[37] 個人情報保護法第 30 条第 1 項
[38] 個人情報保護法第 27 条第 1 項

（※）ただし、上記のうち共同利用に関しては、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置いておくことが必要である。[39]

- 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[40]**

PHR サービス提供者は、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なければならない。

なお、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、当該第三者が構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、当該本人に提供しなければならない。

**（２） 本指針に基づく遵守すべき事項**

**① 予防接種歴の取得に係る事前の同意取得等**

PHR サービス提供者は、予防接種歴の取得に際しては、あらかじめ、本人からの同意を取得しなければならない。

また、オプトアウト手続きによる予防接種歴の取得及び第三者提供は行わないこと。

**② 健診等情報取得に係る同意取得時の利用目的の通知**

PHR サービス提供者は、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、本人の同意を得なければならない。

なお、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すること。

**③ 第三者提供に係る同意取得**

PHR サービス提供者は、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、本人の同意を得なければならない。また、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なければならない。

**④ 利用者による同意状況の確認**

[39] 個人情報保護法についてのガイドライン（通則編）3-6-3 第三者に該当しない場合
[40] 個人情報保護法第 28 条及び個人情報の保護に関する法律施行規則第 17 条第 2 項

過去の同意内容を確認又は見直すことを希望する利用者が一定程度発生することも想定される。PHR サービス提供者は、そうした利用者のため、過去の同意状況を利用者が確認できる方策を確保しなければならない。

### ３．３．消去及び撤回

#### （１） 法規制に基づく遵守すべき事項

**① 利用停止等請求を受けた場合の対応[41]**

PHR サービス提供者は、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（以下「利用停止等」という。）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、原則として、遅滞なく、利用停止等の措置を行わなければならない。

**② 利用停止等請求への対応の例外[42]**

PHR サービス提供者は、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措置をとるときは、当該代替措置によることもできる。

**③ 健診等情報の消去[43]**

PHR サービス提供者は、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、当該 PHR サービス提供者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。）を消去しなければならない。ただし、多額の費用を要する場合その他の消去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措置をとるときは、当該代替措置によることもできる。

#### （２） 本指針に基づく遵守すべき事項

**① 同意の撤回**

PHR サービス提供者は、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、工夫しなければならない。

具体的には、本人が同意の撤回を希望した場合、同意撤回のための情報及び受付窓口が Web サイトの深層にありアクセスしにくいのは望ましくないため、同意の設定変更を容易にできる機能を提供するなど、工夫に努めなければならない。

---

41 個人情報保護法第 35 条第 1 項及び第 5 項

42 個人情報保護法第 35 第 2 項及び個人情報保護法についてのガイドライン（通則編）3-8-5 保有個人データの利用停止等

43 個人情報保護法第 22 条及び第 35 条第 5 項及び第 6 項並びに個人情報保護法についてのガイドライン（通則編）3-4-1 データ内容の正確性の確保等及び 3-8-5 保有個人データの利用停止等

**② 長期間利用がない場合の措置**

利用者によるアクセスがなく、長期間利用されない健診等情報について、本人が認知しないままに、当該情報が削除されることは望ましくないため、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なければならない。

## 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[44]**

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わなければならない。

### 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[45]**

PHR サービス提供者は、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はならない。

また、PHR サービス提供者は、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なければならない。

### 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[46]**

PHR サービス提供者は、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、利用目的を公表しなければならない。

また、当該仮名加工情報は、法令に基づく場合を除くほか、第三者に提供してはならない。

### ３．４．４．匿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[47]**

PHR サービス提供者は、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なければならない。

また、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

[44] 個人情報保護法 第 17 条第 1 項及び第 21 条第 1 項
[45] 個人情報保護法 第 31 条
[46] 個人情報保護法 第 41 条及び 42 条
[47] 個人情報保護法 第 43 条及び 44 条

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なければならない。

## 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

**① 正確性の確保[48]**

PHR サービス提供者は、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、誤り等を発見した場合の訂正等の手続の整備、並びに記録事項の更新及び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。

**② 第三者提供の記録**

PHR サービス提供者は、健診等情報を第三者に提供したときは、原則として、提供した年月日及び提供先等に関する記録を作成し、一定期間保存しなければならない[49]。また、第三者提供を受けた PHR サービス提供者は、原則として、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、一定期間保存しなければならない[50]。

さらに、PHR サービス提供者は、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なければならない。ただし、業務上著しい支障を及ぼすおそれがある場合等には、開示をしないことが認められている[51]。

### 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

**① 利用者を介した相互運用性の確保**

健診等情報を取り扱う PHR サービス提供者においては、利用者を介したデータの相互運用性確保の観点から、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することが望ましい。少なくともマイナポータル 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なければならない。

その際、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することで、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なければならない。

**② サービス終了時の措置**

PHR サービス提供者が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なければならない。

**③ データ提供先の適切性の確認**

PHR サービス提供者間で健診等情報をデータの提供を行う場合、データ提供元の PHR サービス提供者は、データ提供先の PHR サービス提供者が本指針の別紙チェックシートの確認事項に

[48] 個人情報保護法 第 22 条
[49] 個人情報保護法 第 29 条第 1 項及び第 2 項
[50] 個人情報保護法 第 30 条第 3 項及び第 4 項
[51] 個人情報保護法 第 33 条第 5 項

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う。加えて、少なくともデータ提供元のPHRサービス提供者がマイナポータル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なければならない。

## 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

**① 自主的な確認及びその結果の公表**

PHRサービス提供者は、本指針の別紙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、結果を自社のホームページ等で公表しなければならない。ホームページに掲載する際は、本指針３．１．２．（２）①の「サービス利用規約及びプライバシーポリシー等の公表」における公表と同じページ等に、その結果を掲示するとともに、当該結果の概要を理解しやすいように分かりやすい表現にて記載するよう努めなければならない。

## ６．本指針の見直し

PHR サービスを含め、社会における個人情報の利活用のあり方及び保護に関する考え方は、社会情勢及び個人の意識の変化等に対応して変化して行くものと考えられ、関連する法令等も、当該変化に対応して改正等が行われることが見込まれる。

そこで、本指針に関しても、個人情報保護法等の法令又はガイドラインの改正、本指針の運用状況及び PHR サービス又はセキュリティ技術等の拡大等の状況の変化を踏まえて、必要に応じて検討及び見直しを行うものとする。

**用語集**

アルファベット順・50 音順

| | |
|---|---|
| BIOS | パソコンなどの主基板等に格納されたコンピュータプログラムの一種で、起動時の OS の読み込み並びに接続された装置及び機器に対する基本的な入出力制御等を行うもの。 |
| BYOD | Bring Your Own Device の略語。個人が私物として所有しているパソコンやスマートフォンなどデバイスを業務に使う利用形態のこと。 |
| DDoS 攻撃 | Distributed Denial of Service 攻撃の略称。攻撃対象となる Web サーバ等に対して、複数のコンピュータ等から大量の通信を発生させることで正常なサービス提供を妨げる攻撃のこと。 |
| EDR | Endpoint Detection and Response の略語。ユーザーが利用するパソコンやサーバ（エンドポイント）において未知のマルウエアなどの不審な挙動を検知し、迅速な対応を支援する仕組みのこと。 |
| | |
| IDS | Intrusion Detection System の略語。サーバやネットワークの外部との通信を監視し、侵入の試みなど不正なアクセスを検知するシステム。 |
| IPS | Intrusion Prevention System の略語。サーバやネットワークの外部との通信を監視し、侵入の試みなど不正なアクセスを検知して、不正な通信の遮断を行うシステム。 |
| ISMS | Information Security Management System の略語。個別の問題毎の技術対策の他に、組織のマネジメントとして、自らのリスクアセスメントにより必要なセキュリティレベルを決め、プランを持ち、資源配分して、システムを運用すること。 |
| ISO | スイスのジュネーブに本部を置く非政府機関 International Organization for Standardization（国際標準化機構）の略語。ISO の主な活動は国際的に通用する規格を制定することであり、ISO が制定した規格（ISO 規格）を指して用いられることも多い。 |
| JIS | Japanese Industrial Standards の略語。我が国の産業標準化の促進を目的とする産業標準化法（昭和 24 年法律第 185 号）に基づき制定される任意の国家規格。 |
| LAN | Local Area Network の略語。主として同一組織内で用いられる情報通信ネットワーク。 |
| MAC アドレス | Media Access Control（メディア・アクセス・コントロール）アドレス。LAN カードの中で、イーサネット（特に普及している LAN 規格）を使って通信を行うカードに割り振られた一意の番号のこと。インターネットでは、IP アドレス以外にも、この MAC アドレスを使用して通信を行っている。LAN カードは、製造会社が出荷製品に対して MAC アドレスを管理しているため、原則同一の MAC アドレスを持つ LAN カードが 2 つ以上存在することはない。 |
| PHR | Personal Health Record の略語。一般的には、生涯にわたる個人の保健医療情報（健診（検診）情報、予防接種歴、薬剤情報、検査結果等診療関連情報及び個人が自ら日々測定するバイタル等）である。電子記録として本人等が正確に把握し、自身の健康増進等に活用することが期待される。本指針の対象となる情報については、１．１．に規定。 |
| PHR サービス | 利用者が、予防又は健康づくり等に活用すること並びに医療及び介護現場 |

| | |
|---|---|
| | で役立てること等を目的として、PHR を保存及び管理並びにリコメンド等を行うサービス。 |
| TLS | Transport Layer Security の略語。インターネットなどのネットワークでデータを暗号化して送受信するプロトコル（通信手順）の一つ。データを送受信する一対の機器間で通信を暗号化し、中継装置などネットワーク上の他の機器による成りすましやデータの盗み見、改竄などを防ぐことができる。SSL の後継規格。 |
| UTM | Unified Threat Management の略語。日本語で「統合脅威管理」あるいは「統合型脅威管理」と呼ばれるコンピュータウイルスやハッキングなどの脅威から、コンピューターネットワークを効率的かつ包括的に保護する管理手法のこと。 |
| VPN | 仮想私設網、Virtual Private Network の略語。不特定多数が接続するネットワーク上に構築された、特定の拠点間のみを接続する仮想的な閉域網のこと。 |
| WPA2 | Wi-Fi Protected Access 2 の略語。無線 LAN（Wi-Fi）上で通信を暗号化して保護するための技術規格の一つで、WPA の後継規格。また、通信機器などが同規格に準拠していることを認定する認証制度。業界団体の Wi-Fi Alliance が運用している。 |
| WPA3 | Wi-Fi Protected Access 3 の略語。WPA2 の後継規格。WPA2 に発見された脆弱性を解消する技術（パスワードが漏えいした場合に、通信内容を暗号化し解読不可能にする技術）が導入されている。 |
| 開示 | （本人等からの）開示請求に基づいて、当該請求の対象となっている保有個人情報を、当該請求者に対して閲覧させ、又は写しを交付すること。<br>特に個人情報保護法第 33 条第 2 項に基づく場合は、電磁的記録の提供による方法その他の本人が請求した方法（当該方法による開示に多額の費用を要する場合その他の当該方法による開示が困難である場合にあっては、書面の交付による方法）による。 |
| 経営者 | 企業を経営する人。雇用関係からは使用者に同じ。所有と経営との分離していない企業にあっては、資本家・企業家などと同義。 |
| 公表 | 事業の性質及び個人情報の取扱状況に応じ、合理的かつ適切な方法によって、広く一般に知らせること。不特定多数の人々が知ることができるように発表すること。 |
| 個人情報データベース等 | 個人情報を含む情報の集合物であって、特定の個人情報を電子計算機を用いて検索することができるように体系的に構成したものなどであり、個人情報保護法に規定されている。 |
| 個人データ | 個人情報データベース等を構成する個人情報。 |
| 従業員 | 雇われて、ある業務に従事している人。企業と労働・就労契約を結んで雇用されている人。 |
| 従業者 | 事業所に所属して働いている全ての人のこと。 |
| 情報資産 | 情報そのものと、情報を収集したり処理したり保管したりするための装置。 |
| 脆弱性 | 脅威によって悪用される可能性がある欠陥や仕様上の問題。「セキュリティホール」ともいう。 |
| 責任者 | 代表者によって組織の内部の者から指名された者であって、責任及び権限を持つ人。 |
| 多要素認証 | 本人確認のために、「知識情報」、「所持情報」、「生体情報」のうち、２つ |

| | |
|---|---|
| | 以上の認証要素を組み合わせて認証する方式のこと。 |
| 通知 | 事業の性質及び個人情報の取扱い状況に応じ、内容が認識される合理的かつ適切な方法により、直接知らしめること。開示とは異なり、必ずしも本人等からの請求に基づかない。 |
| パッチ | 一旦完成して配布したコンピュータプログラムを部分的に修正あるいは更新するために用いられる追加分（差分）を抜き出したデータのこと。主に、サービスリリース後に発生した不具合への対応や小規模なサービスのバージョンアップを行う際に適用される。 |
| プライバシーマーク制度 | 日本産業規格「JIS Q 15001 個人情報保護マネジメントシステム―要求事項」に適合して、個人情報について適切な保護措置を講ずる体制を整備している組織等を認定して、その旨を示すプライバシーマークを付与し、事業活動に関してプライバシーマークの使用を認める制度のこと。 |
| マイナポータル | 内閣府大臣官房番号制度担当室が運営する Web システムであり、やりとり履歴、利用者の情報、お知らせの表示や子育てワンストップサービス等の各種情報提供、電子申請等のサービスを提供するもの。 |
| マイナポータル API | 民間や行政機関等の組織が提供する外部サービスからの電子申請をマイナポータルで受け付けることや、システム利用者の同意のもと、行政機関から入手した自らの個人情報を外部サービスに提供することを可能にするもの。<br>マイナポータル利用規約別表に掲げられる、マイナポータルが提供する API であり、外部の Web システム等が利用するもの。 |
| マルウエア | コンピュータの正常な利用を妨げたり、利用者やコンピュータに害を及ぼしたりする不正な動作を行うソフトウエアの総称。代表例として、ウイルス、ワーム、スパイウエア、トロイの木馬、ランサムウエアなどがある。 |
| 無線 LAN | 無線でデータの送受信を行なう LAN のこと。 |
| 明示 | 事業の性質及び個人情報の取扱状況等に応じ、内容が認識される合理的かつ適切な方法によって、明確に示すこと。相手方が内容を理解できるよう、分かりやすく示すことが必要。 |
| 要配慮個人情報 | 本人の人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実その他本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして個人情報保護法施行令で定める記述等が含まれる個人情報をいう。施行令では、(1)身体障害、知的障害、精神障害（発達障害を含む。）その他の個人情報保護委員会規則で定める心身の機能の障害があること、(2)本人に対して医師その他医療に関連する職務に従事する者（次号において「医師等」という。）により行われた疾病の予防及び早期発見のための健康診断その他の検査（同号において「健康診断等」という。）の結果、(3)健康診断等の結果に基づき、又は疾病、負傷その他の心身の変化を理由として、本人に対して医師等により心身の状態の改善のための指導又は診療若しくは調剤が行われたことなどが規定されている。 |