民間事業者の PHR サービスに関わる
ガイドライン（第 3 版）

一般社団法人 PHR 普及推進協議会　　PHR サービス事業協会

（2024 年 6 月）

目次

別添資料

I. 民間 PHR サービスガイドラインの背景と目的

（１）PHR を取り巻く背景

超高齢社会における認知症予防、社会構造の変化に伴うメンタルヘルス対策の重要性など、従来の生活習慣病の枠を超えて、生活習慣の改善による健康増進、疾病予防の重要性が高まっている。国民の健康増進の推進に関する基本的な方向や目標に関する事項等を定めた「健康日本 21」では、「休養・こころの健康」の基本方針の一つとして「日常生活や習慣の重視（全人的なアプローチ）」を掲げており、身体的・精神的・社会的視点を含めた日常生活改善のための取り組みが求められている。この課題の解決の方策の一つとして、個人の健康診断結果や服薬歴、日々の健康データを電子記録として本人や家族が正確に把握し、活用するための仕組みである『Personal Health Record（PHR）』に対する期待が世界的に高まっている。

Information and Communication Technology（ICT）の急速な発展と普及に伴い、これまで測定が難しかった日常的な健康データの測定・記録が可能となり、健康診断結果やお薬手帳等のデータの電子化も進んでいる。マイナポータル経由で「予防接種歴」「乳幼児健診の結果」「薬剤情報」「特定健診情報」「後期高齢者健診情報」といった情報が本人に提供され始め、今後は他の法定健診にも拡大する。PHR サービスの発展により、母子保健、学校健診、特定健診等の「健康診断」、体重、血圧等の生活習慣病に関わるデータや食事・運動・睡眠に関わる「日々の記録」、「服薬記録」等を生涯にわたって活用することが可能となり、人々の健康増進、病気の早期発見や重症化予防、ADL（日常生活動作）・QOL（生活の質）の向上等の幅広い健康課題解決への貢献が期待できる。PHR の利活用が進めば、多くの人々の PHR が集積された健康ビッグデータを構築でき、データに基づく健康増進や QOL の向上に繋がるとともに、医学の発展や新産業の創生にも寄与し得る。

国によるマイナポータルを用いた取り組み等の開始に伴い、PHR サービスへの注目はかつてないほどに高まっている。しかしながら、健康情報の活用に当たっては医学的な妥当性、特別な秘匿性などが求められるためにその他の情報と画一的に扱うことに問題があり、個人情報を伴う健康情報を適切に利活用する仕組みは確立していない。また「PHR」という言葉の定義も統一されておらず、話者によって、「仕組み全体」「IT システム」「サービス」「データそのもの」と指し示す範囲が異なり、混乱を招いている現状がある。

このような背景より、民間 PHR サービスの多様化や国際的な動向を踏まえ、PHR サービスの適切な利活用に関する事業者のためのルール整備が求められている。

（２）民間 PHR サービスガイドラインの目的

PHR の利活用促進による健康増進や QOL の向上、医学の発展や新産業の創生が期待されているが、PHR サービス事業者が踏まえるべきモラルやルール（PHR サービスとしての質・安全性の担保、データの互換性、データの質の担保、本人認証の方法、説明と同意方法等）を整理することが重要である。PHR サービスを社会に根付かせるためには、サービスを利用する個人・家族にとっての有効性・安全性を確保すると同時に、PHR サービス普及の妨げとなるような過度の規制とならないよう、バランスの取れた社会的合意に基づいたルールの整備が重要である。PHR サービス事業者が準拠すべきルールが整理されれば、PHR サービスの質の向上、PHR の適切な取扱いを促すことが可能となり、PHR 業界の活性化、ひいては、人々及び社会の健康増進・病気の予防への寄与が期待できる。

本ガイドラインの目的は、国の示す指針を基本に、PHR サービス事業者が踏まえるべきルールや規範を整理して提示することで、更なる PHR サービスの質、有効性と安全性の向上を図り、健康情報を活用した個人と社会の健康増進に寄与するとともに、国民の健康寿命の延伸や豊かで幸福な生活（Well-being）に貢献することである。

（３）PHR サービスとは

「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」において、PHR サービスとは「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」として定義されている。

例として下記目的での使用が考えられる：

・個人が健康増進等の目的で利用する場合

・保険者、地方公共団体、企業が保健指導や健康経営等の一環として住民や従業員等に利用を促す場合

・医療機関（医療・介護に関連する機関等）が健康管理目的で患者に利用を促す場合

II. PHR に関する国の取り組みと民間 PHR サービスガイドラインの関連法令等

（1）国の取り組み

『経済財政運営と改革の基本方針 2018～少子高齢化の克服による持続的な成長経路の実現～（平成 30 年 6 月 15 日閣議決定）』において、個人の健診・診療・投薬情報が医療機関等の間で共有できる全国的な保健医療情報ネットワークについて 2020 年度からの本格稼働を目指す旨と、PHR について 2020 年度よりマイナポータルを通じて本人等へのデータの本格的な提供を目指す方策が掲げられた。その後、毎年の経済財政運営と改革の基本方針において、PHR の拡充を図る方針が継続的に記載されている。令和 3 年 6 月にはデータヘルス改革に関する工程表が策定され、PHR の拡充が推進されてきた。令和 4 年 10 月には内閣総理大臣を本部長とする医療 DX 推進本部が設置され、令和 5 年 6 月 2 日に「医療 DX の推進に関する工程表」が本部決定された。同工程表では国民の更なる健康増進のため、誕生から現在までの生涯に渡る保健・医療・介護の情報を PHR として自分自身で一元的に把握可能となり、個人の健康増進に寄与することや、ライフログデータの標準化等の環境整備が進むことでのライフログデータ等の活用による疾病予防などが期待されている。具体的な施策として、検査結果等について PHR として本人がマイナポータルを通じ情報を確認できる仕組みを整備するとともに、ライフログデータの標準化や流通基盤の構築等を通じたユースケースの創出支援も行っていく方針が示されている。今後「Society5.0」の実現に向けて、健康分野における ICT 活用が進み、民間企業における健康ビッグデータを活用したサービス提供やイノベーションが加速すると思われる。

医療情報システムの安全管理に関しては、「3 省 2 ガイドライン[1]」が策定されている中で、PHR に関しても、目的や方向性を明確にした上で、自身の健康に関する情報について電子データ等の形での円滑な提供や適切な管理、効果的な利活用が可能となる環境を整備していくために、関係省庁の連携の下、2019 年度（令和元年度）に「国民の健康づくりに向けた PHR の推進に関する検討会」が立ち上げられ、民間 PHR サービスの適切かつ効果的な利活用に向けて、『国民の健康づくりに向けた PHR の推進に関する検討会 民間利活用作業班』の中で検討が進められた。（令和元年度にはそれぞれ「健康・医療・介護情報利活用検討会」及び「健診等情報利活用ワーキンググループ 民間利活用作業班」として再組成）

---

[1] 電子化された医療情報を取り扱う医療情報システムに関連する厚生労働省・経済産業省・総務省の 3 省による以下に示す 2 つのガイドラインを指す。

・厚生労働省「医療情報システムの安全管理に関するガイドライン 」

・総務省・経済産業省「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」

なお「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」（総務省・経済産業省）では「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事業者」も対象事業者としており、このような PHR サービス事業者は 3 省 2 ガイドラインの対象事業者となる。

民間利活用作業班の成果物は「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」（以下、「国の PHR 指針」）として取りまとめられた。本指針は令和 3 年 4 月 23 日公表の後、個人情報保護法改正を受けて一度改正され、総務省・厚生労働省・経済産業省の 3 省から公表されている。特にマイナポータル API 等を活用して入手可能な自身の健康診断等の個人情報保護法上の要配慮個人情報となる保健医療情報や予防接種歴（以下「健診等情報」)を取り扱う PHR 事業者には本指針の遵守が求められるものとなっており、実際にマイナポータル API に接続する事業者には本指針の遵守状況をチェックシートにて確認されるものとなっている。

（２）国の民間 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と民間 PHR サービスガイドラインの位置づけ・対象

＜民間 PHR サービスガイドラインの位置づけ＞

本ガイドラインは、国の PHR 指針を補完するものとして、より高い水準の PHR サービスの提供を実現するためのものである。国レベルでは、健診等情報のマイナポータルを経由した提供において民間 PHR 事業者が遵守すべき事項、特に PHR 利活用に係る「情報セキュリティ対策」「個人情報の適切な取扱い」「健診等情報の保存・管理、相互運用性の確保」「その他（要件遵守の担保方法）」について国の PHR 指針に策定されている。国が定める健診等情報には、個人情報保護法上の要配慮個人情報である乳幼児健診、特定健診、薬剤情報等、及び予防接種歴が含まれる。いわゆるライフログのみを取り扱う事業者は現時点では国の PHR 指針の対象となっていない。また、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事業者も対象となっていない。

本ガイドラインは、国が定める指針に加えて、PHR サービスを提供する民間事業者が踏まえるべきルールや規範を提示することで、更なる PHR サービスの質、有効性と安全性の向上を図ることを目的に、主に下記 3 点を中心に必要と考えられる事項を検討し、提示するものである。

① PHR サービス提供に当たっての具体的な運用（有効性や安全性に配慮したリコメンド機能の運用等）
② ライフログ等（本人が日々計測するバイタル・健康情報等）の健診等情報以外の情報に関する取扱い
③ 国の検討対象となっていない範囲のサービスのあり方

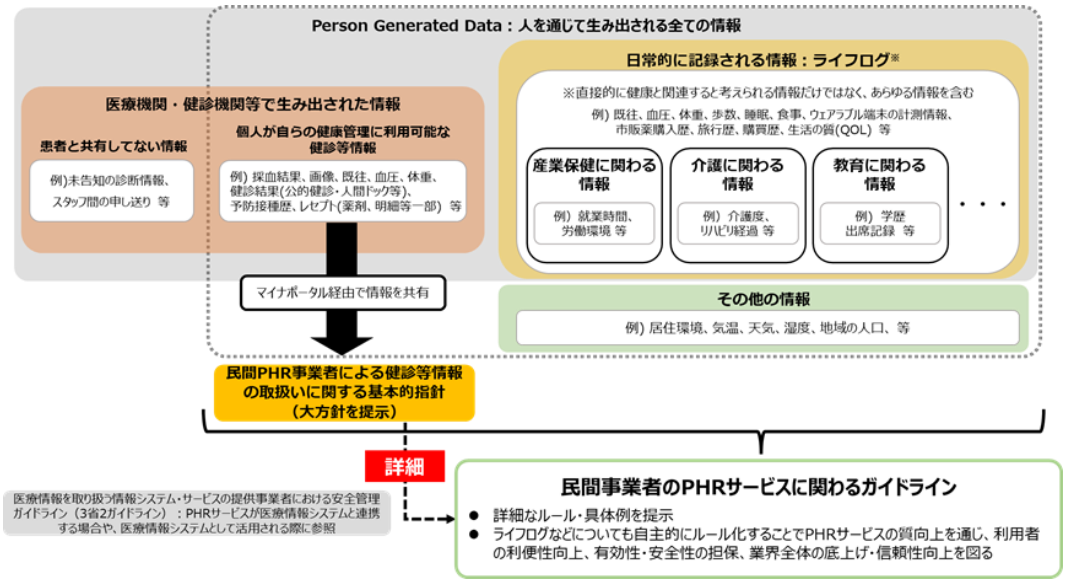
＜民間 PHR サービスガイドラインの対象＞

本ガイドラインの対象は、全ての PHR サービス（医療情報システム[2] として提供されるものを除く）を提供する事業者を想定しており、国の PHR 指針が対象としてないライフログのみを取り扱う PHR サービス事業者等も含む。「健診等情報」を取り扱う PHR 事業者は、国の PHR 指針の参照が求められるが、本ガイドラインを遵守することで更なる PHR サービスの質向上が望まれる。本ガイドライン策定の目的は、PHR サービスの有効性と安全性の向上を図り、個人と社会の健康増進に寄与するとともに PHR 業界の発展に繋げることであり、ここに記載された内容をクリアすることにとどまらず、提供する PHR サービスの質向上に繋げていただくことを期待するものである。

なお、「医療情報システムとの直接連携」を行う場合は、その要件や安全管理に関しては 3 省 2 ガイドラインに準拠する必要があり、遺伝情報の取扱いについては経済産業省「経済産業分野のうち個人遺伝情報を用いた事業分野における個人情報保護ガイドライン」等の遺伝情報に係る各種ガイドラインに準拠する必要がある。

以上を踏まえて、本ガイドラインの対象とする情報と対象者を下記に示す。

- 対象情報： PGD（Person Generated Data：詳細は後述）の考え方に基づき、国の PHR 指針が対象とする「健診等情報[3]」に加え、日常的に記録される情報（ライフログ）を含む個人が活用し得る健康に関連する情報
- 対象者： 日本在住の個人に対し、個人が活用し得る健康に関連する情報を取扱い、PHR サービス（保健医療情報を国民・患者の病気の予防・健康づくり等に活用するサービス）を提供する民間事業者



【図 1 ：Person Generated Data の考え方を基本とした民間 PHR サービスガイドラインの対象】

[2] 医療に関する患者情報（個人識別情報）を含む情報を扱うシステムを指す。
[3] 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個人情報保護法上の要配慮個人情報である乳幼児健診、特定健診、薬剤情報等、及び予防接種歴が含まれる。

（３）民間 PHR サービスガイドラインの策定にあたり参照した法律及びガイドライン等

本ガイドラインの策定にあたり参照した法律及びガイドライン等は以下の通りである。なお、PHR サービスに係る法令等は多岐にわたるものであり、本ガイドラインはその全てを網羅するものではないことにあらかじめご留意いただきたい。

＜関連法規＞

- 医師法（昭和 23 年 7 月 30 日. 最終改正令和 3 年 5 月 28 日）
- 医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律（昭和 35 年 8 月 10 日. 最終改正令和 5 年 12 月 13 日）
- 医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律施行令（昭和 36 年 1 月 26 日. 最終改正令和 4 年 5 月 20 日）
- 医療分野の研究開発に資するための匿名加工医療情報及び仮名加工医療情報に関する法律（平成 29 年 5 月 12 日. 最終改正令和 5 年 5 月 26 日）
- 医療法（昭和 23 年 7 月 30 日. 最終改正令和 5 年 6 月 7 日）
- 健康増進法（平成 14 年 8 月 2 日. 最終改正令和 4 年 6 月 22 日）
- 個人情報の保護に関する法律（平成 15 年 5 月 30 日. 最終改正令和 5 年 11 月 29 日）
- 個人情報の保護に関する法律施行令（平成 15 年 12 月 10 日. 最終改正令和 6 年 1 月 31 日）
- 特定商取引に関する法律（昭和 51 年 6 月 4 日、最終改訂令和 4 年 6 月 1 日）
- 不当景品類及び不当表示防止法（昭和 37 年 5 月 15 日. 最終改正令和 5 年 5 月 17 日）
- 保健師助産師看護師法（昭和 23 年 7 月 30 日. 最終改正令和 5 年 6 月 16 日）

＜公的指針・ガイドライン等＞

- 医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス（個人情報保護委員会、厚生労働省）（平成 29 年 4 月 14 日. 令和 5 年 3 月最終改正）
- 医療機器プログラムの取扱いについて（厚生労働省）（平成 26 年 11 月 21 日. 平成 30 年 12 月 28 日一部改正）
- 医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン第 1.1 版（総務省・経済産業省）（令和 4 年 8 月. 令和 5 年 7 月改定）
- 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（厚生労働省）（令和 5 年 5 月）
- オンライン診療の適切な実施に関する指針（厚生労働省）（平成 30 年 3 月. 令和 5 年

3 月一部改訂）

- 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）（総務省）（令和 3 年 9 月）
- 経済産業分野のうち個人遺伝情報を用いた事業分野における個人情報保護ガイドライン（経済産業省）（令和 3 年 3 月 23 日）
- 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（厚生労働省、経済産業省）（平成 26 年 3 月 31 日）
- 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）（個人情報保護委員会）（平成 28 年 11 月. 令和 5 年 12 月一部改正）
- 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）（個人情報保護委員会）（平成 28 年 11 月. 令和 4 年 9 月一部改正）
- 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）（個人情報保護委員会）（平成 28 年 11 月. 令和 5 年 12 月一部改正）
- 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）（個人情報保護委員会）（平成 28 年 11 月. 令和 5 年 12 月一部改正）
- 「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（個人情報保護委員会）（平成 29 年 2 月 16 日. 令和 6 年 3 月 1 日更新）
- 個人情報の保護に関する基本方針（平成 16 年 4 月 2 日閣議決定、令和 4 年 4 月 1 日一部変更）
- 雇用管理に関する個人情報のうち健康情報を取り扱うに当たっての留意事項（厚生労働省）（平成 29 年 8 月 24 日）
- 情報銀行における健康・医療分野の要配慮個人情報の取扱いに係わる方針（総務省、経済産業省「情報信託機能の認定スキームの在り方に関する検討会」）（令和 5 年 7 月）
- 情報信託機能の認定に係る指針 Ver3.0（総務省、経済産業省「情報信託機能の認定スキームの在り方に関する検討会」）（令和 5 年 7 月）
- 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）
- JIS X8341 シリーズ「高齢者・障害者等配慮設計指針―情報通信における機器，ソフトウェア及びサービス（第 1 部～第 7 部）」
- 認知症の人の日常生活・社会生活における意思決定支援ガイドライン（厚生労働省）（平成 30 年 6 月）
- 不当景品類及び不当表示防止法第 7 条第 2 項の運用指針 ―不実証広告規制に関する指針―(公正取引委員会) (平成 15 年 10 月 28 日)
- プログラムの医療機器該当性に関するガイドライン（厚生労働省）（令和 3 年 3 月 31 日、令和 5 年 3 月 31 日一部改正)
- 労働者の心身の状態に関する情報の適正な取扱いのために事業者が講ずべき措置に関す

る指針（厚生労働省）（令和４年３月 31 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（総務省、厚生労働省、経済産業省））（令和３年４月. 令和 5 年４月最終改正）

＜その他＞

・ 情報システムに係る相互運用性フレームワーク（経済産業省、情報処理推進機構）（平成 19 年６月）

・ ヘルスケアサービスガイドライン等のあり方（経済産業省 商務・サービスグループ ヘルスケア産業課）（平成 31 年４月 12 日. 令和３年６月９日改訂）

・ マイナポータルＡＰＩ利用規約 1.4 版（デジタル庁）（令和 5 年 1 月 26 日）

III.　民間 PHR サービスガイドラインに用いられる用語の定義

用語	定義
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。 （国の PHR 指針より抜粋）
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。 （国の PHR 指針より抜粋）
PHR サービス事業者	日本国内において、PHR サービスを提供、又は製造（OEM 含む。）している、法人（営利を目的としないものを含む。）、個人事業者、団体。
医療・介護関係事業者	「医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス*」で定義される医療・介護関係事業者を意味する。 *当ガイダンスが対象とする事業者の範囲は、下記の通りである ①病院、診療所、助産所、薬局、訪問看護ステーション等の患者に対し直接医療を提供する事業者 ②介護保険法に規定する居宅サービス事業、介護予防サービス事業、地域密着型サービス事業、地域密着型介護予防サービス事業、居宅介護支援事業、介護予防支援事業、及び介護保険施設を経営する事業、老人福祉法に規定する老人居宅生活支援事業及び老人福祉施設を経営する事業その他高齢者福祉サービス事業を行う者
医療情報システム	医療に関する患者情報（個人識別情報）を含む情報を扱うシステム
PHR システム	PHR サービスを提供するために構築された情報システム
Electronic Health Record	①コンピュータで処理可能な形式で保存・管理された診療対象

（EHR）	者の健康状態に関する情報のリポジトリ（保管場所） ②地域の病院や診療所などをネットワークでつないで患者情報等を共有活用する基盤（地域医療連携ネットワーク）
ヘルスケアサービス	健康の保持及び増進、介護予防を通じた 健康寿命の延伸に資する商品の生産若しくは販売又は役務をいう。（ただし、個別法による許認可等が必要な商品や役務等を除く。）
医行為	医療及び保健指導に属する行為のうち、医師が行うのでなければ保健衛生上危害を生ずるおそれのある行為
リコメンドサービス（機能）	スマートフォン等のアプリケーションを介して、記録管理された個人の保健医療情報に基づいて、生活習慣改善等に向けた推奨を行う機能
記録管理・閲覧サービス（機能）	個人の保健医療情報を記録管理・閲覧する機能。記録管理・閲覧機能には、ウェアラブル端末等を通じた健康情報収集を含む。
相互運用性	情報の視点から見て、異なった目的で作られたアプリケーション間で情報の伝達又は共有がなされることを意味する。特に本ガイドラインでは、異なる PHR サービス間で、PHR の伝達又は共有が可能であると担保されている状態を意味する。
薬機法	医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律
個人情報保護法	個人情報の保護に関する法律
通則 GL	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）
要配慮個人情報	不当な差別、偏見その他の不利益が生じないように取扱いに配慮を要する情報として、個人情報保護法に定められた情報である。要配慮個人情報には、（1）人種、（2）信条、（3）社会的身分、（4）病歴、（5）犯罪の経歴、（6）犯罪により害を被った事実、（7）身体障害、知的障害、精神障害等の

	障害があること、（8）健康診断その他の検査の結果、（9）保健指導、診療・調剤情報、（10）本人を被疑者又は被告人として、逮捕、捜索等の刑事事件の手続が行われたこと、（11）本人を非行少年又はその疑いがある者として、保護処分等の少年の保護事件に関する手続が行われたこと、が該当する。

IV.　PHR サービスの提供に当たっての基本理念

（１）PHR と Person-Generated Data（PGD）の考え方

Person-Generated Data（PGD）とは、個人の生活に紐付く医療・介護・健康等を含む全ての情報を意味する。PGD には、病気になってから記録される「医療機関等で患者より生み出された情報」だけでなく、病気の有無にかかわらず日常的に記録される健康関連データや産業保健・介護等に関連する情報のほか、旅行履歴、行動履歴、購買履歴等の情報（ライフログ）も含まれる。PHR サービスの提供に当たっては、PHR として個人の意思で管理・利活用する健康に関わる可能性のある情報の大部分は、PGD であることを前提とすべきである。

（２）日常的な健康データを活用したセルフケアによる健康増進、病気の予防

ICT の発展と普及により、日常的な健康データの測定・記録が容易となり、日々の体重・血圧等の生活習慣病に関わるデータや食事・運動・睡眠に関わる記録、服薬記録等の健康データを生涯にわたって PHR として利活用することが可能となった。今後、人々の健康増進、疾病の早期発見や重症化予防、ADL・QOL の向上にむけたセルフケアに、PHR を活用することが求められる。

（３）周辺データを活用した健康増進、医療の質向上

PHR サービスが取り扱うデータには、現時点で医療や健康に関連すると考えられるデータだけではなく、購買履歴や行動履歴などの医療・健康以外の個人に紐付いたデータや環境等のあらゆるデータが含まれる可能性がある。また将来的にまだ見ぬ新しいデータが活用されるかもしれない。健康・医療に関連する情報とあわせて、環境等の周辺情報も積極的に利用し、健康増進、医療の質向上に繋がるサービスに発展することが望ましい。

（４）PHR サービス利用者の健康、安全、権利の確保

PHR サービスの主な目的は利用者の健康増進であり、PHR を蓄積・可視化することや、それらをもとに実施されるリコメンドが利用者の心身の健康増進に役立つという「有効性」と、危害を及ぼさないという「安全性」の確保がその機能や用途に応じて求められる。PHR を参照して医療が提供される場合もあるため、蓄積される PHR や提供される PHR サービスの目的に応じて、蓄積されるデータやリコメンドの信頼

性が担保されるような仕組みがあることが望ましい。また、PHR には、個人情報、要配慮個人情報、個人関連情報として個人情報保護法が適用される情報も含まれることから、PHR サービス事業者や PHR を扱う者はそのことを十分に認識し、利用者自身が自身のデータをコントロールできる仕組みを構築することが求められるとともに、データの漏洩・改ざん・紛失等の危険への十分な対策が必要となる。さらに、PHR サービスは、高齢者や障害のある人を含め多種多様な背景を持つ人が利用可能なものであることが求められるため、あらゆる人が適切に利用できるようユーザビリティ及びアクセシビリティの確保に配慮したサービス設計とするよう努めなければならない。具体的には、JIS X8341 シリーズ「高齢者・障害者等配慮設計指針―情報通信における機器，ソフトウェア及びサービス（第１部～第７部）」が参考となる。

（５）利用者への説明と同意に基づくサービス提供

PHR サービス提供の際は、サービスの内容等について、利用者に対して、同意に係る判断に必要と考えられる合理的かつ適切な方法を用いて明確に説明した上で、明示的な同意を取得することが求められる。PHR サービス事業者は、PHR サービス利用者に対して、PHR サービスの目的・使用用途等について、文書によって情報を理解することについて特別な配慮が必要な方（例えばこども、高齢者、外国人、障害のある人等）も正しく理解できるような方法で情報提供するよう努めるべきである。また、同意取得においては、利用者の同意の範囲を明らかにし、適切な PHR サービスを選択・利用できるように努めなければならない。認知症や小児・乳幼児等の十分な自己判断能力や責任能力を持たない利用者の PHR を管理・活用できるようなサービスを提供する際には、その親権者やその他の代理人等への適切な説明を行った上で同意を取得することが求められる。さらに、取り扱う情報の機微性と心身の発達に応じ、PHR の管理権限を本人に移譲することに関しても明確に説明した上で、適時において本人の同意を改めて取得することが望ましい。

（６）PHR サービスの質の担保と向上

PHR サービスは利用者の健康や生活に直結するものである。よって PHR サービス事業者は利用者の健康と福祉の増進を第一の関心事とし、利用者の最善の利益のためにサービスの質の担保と向上に努めなければならない。PHR サービス事業者は、良心と最善の知識をもってこの責務を達成すべきであり、間違っても利用者の健康や福祉を阻害するものであってはならない。

サービスの質は、利用者の手間やコストとトレードオフとなる場合があるため、PHR サービス事業者は、提供するサービスごとにその目的に合致した最適な質のレベルを設定し、利用者に不要な負担を掛けてはならない。また、PHR サービスは利用者の生涯に渡り長期的に利用されるものであることから、PHR サービス事業者は、自社の事業が継続できなくなった場合でも、類似の他社サービスに情報を引き継ぐ手段を提供するなど、利用者の健康や福祉の低下につながらないように努めるべきである。

PHR サービスは未だ発展途上であり、今後多くの技術革新が見込まれる。PHR サービス事業者は常に最新の技術に注意を払い、情報セキュリティ、相互運用性を含むサービスの向上に努めなければならない。特に新しい技術を適用する場合、例えばプログラム医療機器や特定保健用食品では承認等の取得のためにエビデンス取得が必要となるところ、PHR サービスにおいても、特に新技術を適用する場合など、PHR サービスの内容に即した適切な健康上のエビデンスの有無に注意を払うべきである。さらに、様々な IoT 機器やモバイルデバイスとの連携を行う場合には、デバイスメーカーごとに規格や仕様が異なるケースも多く、不具合の発生も考えられるため、PHR サービス事業者はサービスの目的に合致した最適なデバイスを提供あるいは利用者が選択できるようにし、デバイスの差異及び不具合、並びにデバイスの非互換性により利用者が不利益を被らないように努めなくてはならない。デバイスメーカーや業界団体等と協議を行い、不具合の解消や新しい仕様を策定しなければならないケースもあるが、その場合も常に利用者の最善の利益を追求すべきである。

（７）PHR サービス事業者間での連携

人生 100 年時代と言われる今日、PHR サービス利用者はライフステージや趣向に応じて複数の PHR サービスを同時又は乗り換えて利用していくことが考えられる。また、PHR サービスが取り扱うデータの種別は、健診等情報からライフログまで多岐にわたるため、一事業者があらゆる利用者に対応した PHR サービスを提供することは現実的ではない。加えて、PHR サービスの終了や PHR サービス事業者の統廃合も生じることが考えられる。そのような状況下において、PHR サービス利用者の権利を保護し、PHR 業界の健全な発展を促すためには、PHR サービス事業者間での相互運用性を向上させる連携（必要最低限のデータの引き継ぎを可能とする、共通項目やデータ流通形式の標準化など）が欠かせない。

（８）市場の拡大による受益者増、社会全体の健康増進、生産性向上

PHR サービス事業者及び社会に対して、PHR サービスの適切な利活用に向けた教育・啓発が行われるべきである。本ガイドラインが広く利用されることで、PHR 業界の健全な育成及び活性化が図れるとともに、適切な PHR サービス市場の拡大により受益者が増え、社会全体の健康増進・生産性向上に繋がることが期待できる。

（９）継続的な改訂が可能な体制の構築

PHR サービス関連事業の継続的な発展のためには、PHR サービス業界の社会的信頼の確保が不可欠である。そのためには、国の PHR 指針のみならず、民間事業者が自ら定める PHR サービスに関連す

るルール・規範を遵守し、PHR サービスの質が維持・向上されることが重要となる。ICT の技術革新は著しく、今後、未知の PHR サービスが創出されることも予想され、PHR に関連する技術やサービスの発展に沿って、PHR サービスに係るルールの改訂やあり方の継続的な検討が必要である。そのためには、PHR に関係する者（産官学民）の間の連携を強化し、継続的な検討ができる体制が構築されるべきである。

（10）国際的な動向を踏まえた PHR サービス提供に係るルールの整備

国際的にも PHR サービスを活用した健康増進・事業化に期待が高まっており、それぞれの地域の特性を生かした取り組みが進められている。医療従事者・患者双方からの医療情報へのアクセスを可能とする公的な EHR プラットフォームの構築が進んでいる国では、そこを起点とした多種多様な PHR サービスが展開されている。欧州では、国際標準規格の採用や欧州内での相互運用性の確保のためのネットワークやルール整備等の、官民一体となったフレームワーク構築が進んでいる国もある。このような国際的な PHR サービスの動向に追走し、日本における PHR サービス事業を発展させるために、日本の個人情報保護法にも対応した上で、国際的な標準化、相互運用性の確保及びデータの保管場所（国内外）、データ連携を実現するための標準化を意識した PHR サービス提供に係るルールの整備が強く求められる。

V.　民間 PHR サービスガイドラインの具体的適用

本章においては、PHR サービス提供における「最低限遵守する事項」及び「推奨される事項」を、その考え方とともに示す。また、本ガイドラインの理解を容易にするため、必要に応じて、PHR サービスとして「望ましい例」及び「不適切な例」を付記する。「最低限遵守すべき事項」として掲げる事項は、PHR サービスの安全性・有効性を担保し、PHR サービス事業者の事業が適切に行われるために必要なものである。

１．PHR サービス提供に関する事項

（１）事業者―利用者の関係/合意（説明と同意）

考え方

PHR サービスに係る契約を締結する際には、明確な説明及び明示的な合意形成が求められる。また、PHR は個人情報（個人情報保護法 2 条 1 項）、要配慮個人情報（同 3 項）、個人データ（同法 16 条 3 項）や個人関連情報（同法 2 条 7 項）に該当し得るものであり、PHR を含む個人情報データベース[4]等を事業の用に供している PHR サービス事業者は、個人情報保護法で定義される個人情報取扱事業者に該当する（同 2 項）。PHR サービス事業者は個人情報保護法及び各種ガイドライン並びに個人情報保護又は守秘義務に関する他の法令等を遵守する必要がある。特に、医療・介護関係事業者は「医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス」を遵守する必要があるため、別途ご参照いただきたい。

事業者―利用者の関係/合意（説明と同意）については、契約締結時と契約期間中に分けて検討するのが有益である。契約締結時においては、①明確な説明及び明示的な合意形成及び②利用目的の通知について留意する必要がある。次に、契約締結時及び契約期間中においては、①個人情報に係る同意の適切な取得、②個人情報の適切な取得及び③一定事項の公表等について留意する必要がある。最後に、契約期間中においては、①契約期間中の同意の確認、②利用目的の遵守及び③利用目的の適切な変更等について留意するとともに、契約内容を遵守する必要がある。

[4]個人情報を含む情報の集合物であって、次に掲げるもの（利用方法からみて個人の権利利益を害するおそれが少ないものとして政令で定めるものを除く。）をいう（個人情報保護法 16 条 1 項）。
一　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
二　前号に掲げるもののほか、特定の個人情報を容易に検索することができるように体系的に構成したものとして政令で定めるもの

最低限遵守する事項

【契約締結時】

① 明確な説明及び明示的な合意形成

PHR サービス事業者は、PHR サービスの内容や契約の目的等について利用者に対し明確に説明した上で、明示的な合意を形成する必要がある。この際には、本人、PHR サービス事業者、医療機関等、利用対象者ごとに説明の方法を検討する。特に、本人については、病気の予防・健康づくり、PHR サービス等に関し、十分な知見を有していない場合も想定されることから、本人に対する説明が分かりやすいものとなるよう、特に配慮が必要である。

② 利用目的の通知等

個人情報取扱事業者に該当するPHRサービス事業者は、個人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（個人情報保護法 17 条 1 項）。特に、第三者提供を予定しているときは、その旨が明確に分かるよう特定する必要がある（通則 GL3-1-1、3-6-1）。

このような個人情報の利用目的は、あらかじめ公表するか、又は個人情報の取得後に速やかに利用目的を本人に通知し、又は公表する必要がある（個人情報保護法 21 条 1 項）。ただし、本人との間で契約を締結することに伴って電磁的記録を含む契約書その他の書面に記載された当該本人の個人情報を取得する場合その他本人から直接当該書面に記載された当該本人の個人情報を取得する場合は、原則として、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(個人情報保護法 21 条 2 項)。利用目的の明示には、ネットワーク上において、利用目的を、本人がアクセスした自社のホームページ上に明示し、又は本人の端末装置上に表示する場合が含まれる（通則 GL3-3-4）。

【契約締結時及び契約期間中】

① 個人情報に係る同意の適切な取得

個人情報取扱事業者が要配慮個人情報の取得や個人データの第三者提供等を行うためには、原則として、事前に本人の同意を取得する必要がある（個人情報保護法 20 条 2 項、27 条）[5]。特に、要配慮個人情報については、基本的にオプトアウト[6]による第三者提供は認められていないことや、外国にある第三者への提供については原則として一定の情報を提供した上で同意を取得する必要があることに留意する必要がある（個人情報保護法 27 条 2 項、28 条）。そのため、個人情報取扱事業者に該当する PHR サービス事業者は、原則として、契約締結時等、当該行為を行う前に本人の同意を取得

[5] なお、第三者提供について、同意が不要な場合が同法 27 条 1 項各号に列挙されており、また第三者提供に該当しない場合が同 5 項各号に列挙されている。詳細は下記(6) 他の事業者・第三者へのデータ提供を参照。法律上有効な同意として認められる程度の明確性があった場合でも、本人の正しい理解が得られないことでレピュテーションリスクを抱えることがあることに留意すること。不安な場合は、第三者等にレビューを受けることが望ましい。

[6] 「オプトアウト」方式とは、個人情報を第三者提供するに当たって、その個人情報を持つ本人が反対をしない限り、個人情報の第三者提供に同意したものとみなし、第三者提供を認めること。

する必要がある。

また、個人関連情報取扱事業者は、第三者が個人関連情報（個人関連情報データベース等を構成するものに限る。）を個人データとして取得することが想定されるときは、原則として、当該第三者が個人関連情報取扱事業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当該本人の同意が得られていることを確認せずに、当該個人関連情報を当該第三者に提供してはならない（個人情報保護法 31 条 1 項）。

個人情報に係る同意の取得の際には、事業の性質及び個人情報の取扱状況に応じ、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方法を用いる必要がある（通則 GL2-16）。この際には、電磁的方法を用いて同意を取得することも可能である。同意の取得方法の具体例として、以下が挙げられる（通則 GL2-16）。

例①：本人からの同意する旨の書面（電磁的記録を含む。）の受領
例②：本人からの同意する旨のメールの受信
例③：本人による同意する旨の確認欄へのチェック
例④：本人による同意する旨のホームページ上のボタンのクリック
例⑤：本人による同意する旨の音声入力、タッチパネルへのタッチ、ボタンやスイッチ等による入力

なお、個人情報の取扱いに関して同意したことによって生ずる結果について、未成年者、成年被後見人、被保佐人及び被補助人が判断できる能力を有していないなどの場合は、親権者や法定代理人等から同意を得る必要がある（通則 GL2-16）。このうち、未成年者については、法定代理人等から同意を得る必要がある具体的な年齢は、対象となる個人情報の項目や事業の性質等によって、個別具体的に判断されるべきだが、一般的には 12 歳から 15 歳までの年齢以下のこどもについて、法定代理人等から同意を得る必要があると考えられている（「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 1-62）。

加えて、第三者提供に当たっての同意の取得の際には、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とされている（通則 GL3-6-1）。認知症の方を含む高齢者においても、医療介護などの生活を支えるために有用なデータの利用が阻害されてしまわないよう、医療や介護といった領域で既に行われている同意取得・意思決定支援方法を参考に、本人の意向等を踏まえつつ、データ活用を進めるべきである。

また、PHR を含む個人関連情報データベース等を事業の用に供している PHR サービス事業者は、個人情報保護法で定義される個人関連情報取扱事業者に該当するところ（個人情報保護法 16 条 7 項）、個人関連情報取扱事業者は、第三者が一定の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、原則として、一定の事項を確認することをしないで、当該個人関連情報を当該第三者に提供してはならない（個人情報保護法 31 条）。

② 個人情報の適切な取得

PHR サービス事業者は、偽りその他不正の手段により個人情報を取得してはならない（個人情報保護法 20 条 1 項）。例えば、以下が不正の手段により個人情報を取得している事例として挙げられる（通則 GL3-3-1）。

例①：個人情報を取得する主体や利用目的等について、意図的に虚偽の情報を示して、本人から個人情報を取得する場合
例②：他の事業者に指示して不正の手段で個人情報を取得させ、当該他の事業者から個人情報を取得する場合
例③：個人情報保護法第 27 条 1 項に規定する第三者提供制限違反がされようとしていることを知り、又は容易に知ることができるにもかかわらず、個人情報を取得する場合
例④：不正の手段で個人情報が取得されたことを知り、又は容易に知ることができるにもかかわらず、当該個人情報を取得する場合

③ 一定事項の公表等

個人情報取扱事業者に該当する PHR サービス事業者は、原則として、以下の事項について（例えばホームページに掲載するなどの方法で）PHR サービス利用者の知り得る状態に置かなければならない（個人情報保護法 32 条 1 項、個人情報の保護に関する法律施行令第 10 条、通則 GL3-8-1）。

①個人情報取扱事業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
②全ての保有個人データの利用目的
③保有個人データの利用目的の通知の求め又は開示等の請求に応じる手続及び保有個人データの利用目的の通知の求め又は開示の請求に係る手数料の額（定めた場合に限る。）
④保有個人データの安全管理のために講じた措置
⑤保有個人データの取扱いに関する苦情の申出先
⑥認定個人情報保護団体の対象事業者である場合には、当該認定個人情報保護団体の名称及び苦情の解決の申出先

※匿名加工情報を第三者提供する場合の推奨については、V.1.（４）PHR サービスにおける個人情報の保護・情報セキュリティ【匿名加工情報等の作成及び利用】を参照のこと

【契約期間中】

① 契約期間中の同意の確認

上記の通り、個人情報取扱事業者が要配慮個人情報の取得や個人データの第三者提供等を行うためには、原則として、事前に本人の同意を取得する必要があるところ、当該同意の確認については、国の PHR 指針と同様の内容による個人情報に係る同意の確認を行う。

② 利用目的の遵守・不適正な利用の禁止

個人情報取扱事業者に該当する PHR サービス事業者は、個人情報保護法の例外に当たる場合を除き、あらかじめ本人の同意なくして、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 18 条 1 項）。

また、個人情報取扱事業者に該当する PHR サービス事業者は、違法又は不当な行為を助長し、又は誘発するおそれがある方法により個人情報を利用してはならない（個人情報保護法 19 条）。

③ 利用目的の適切な変更等

個人情報取扱事業者に該当する PHR サービス事業者は、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 17 条 2 項）[7]。「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」とは、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内をいい、「本人が通常予期し得る限度と客観的に認められる範囲内」とは、本人の主観や事業者の恣意的な判断によるものではなく、一般人の判断において、当初の利用目的と変更後の利用目的を比較して予期できる範囲をいい、当初特定した利用目的とどの程度の関連性を有するかを総合的に勘案して判断される（通則 GL3-1-2）。

個人情報保護法 17 条 2 項に基づき利用目的を変更した場合には、変更された利用目的について本人に通知し、又は公表しなければならない（個人情報保護法 21 条 3 項）。

個人情報取扱事業者に該当する PHR サービス事業者は、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利用目的を変更する場合、PHR サービス利用者から利用目的の変更について本人の同意を取得する必要がある。

【契約終了時】

① サービス終了時の情報の破棄・本人への PHR の返却等

PHR サービス事業者がサービスを終了する場合、利用者への PHR のエクスポート及び他の PHR サービス事業者への当該 PHR のインポートが実施可能な期間を十分に確保すべきである。また PHR サービス事業者は、管理する PHR が利用者の重要な資産であることに留意し、利用者が PHR を引き続き利用可能なように最大限努めるべきである（データベースのダンプファイルの提供や、他の PHR サービス事業者へのデータ引き継ぎ等。データをエクスポートする際のデータ交換規格については、PHR サービス間のデータ連携に関する考え方の項を参照）。その上で、サービス終了後は、契約内容に従って情報の破棄等を確実に行う。手順に則って情報の返却・移管・破棄を適切に実施したことの証跡を取得しておくこと

[7] 「個人情報取扱事業者が、開示、内容の訂正、追加又は削除、利用の停止、消去及び第三者への提供の停止を行うことのできる権限を有する個人データであって、その存否が明らかになることにより公益その他の利益が害されるものとして政令で定めるもの以外のもの」を意味する（個人情報保護法 16 条 4 項）。

も必要である。

最低限遵守する事項

- PHR サービス事業者は、解約の権利を設ける場合にはその旨及び解約後のデータ処理について明示すること。

推奨される事項

- PHR サービス利活用の対象となる利用者は、疾患を抱えている方からそうでない方、こどもから高齢者、日本人から外国人、障害のある人まで幅広いため、PHR サービスの内容や利用者に応じて説明をすることが望ましい。特に、PHR サービスを利用することによって、健康に悪影響を及ぼす可能性について考慮し、契約締結時の説明において、サービスを活用する前にかかりつけ医等の医療者に相談することが望ましい旨を伝えるよう留意する。
- 契約締結時の説明の際には電磁的手段を用いることが考えられるが、電磁的手段を用いて説明を行う場合には、一般に個々人の理解度等に応じて柔軟に説明を変えることが難しい点や、問い合わせ先の掲載等の手段により意図的に質問の機会を作り出さなければ、PHR サービス利用者が当該説明に関して質問をすることが難しい点に留意する。
- 契約締結時に個人情報を取得する可能性があることに鑑み、個人情報取扱事業者に該当する PHR サービス事業者は、個人情報の利用目的をあらかじめ公表し、又は契約締結時に通知することが望ましい。
- 契約締結時、医療機関へ PHR サービスを提供する場合は、関連するガイドラインに準拠して財務諸表や IR 情報等に基づく経営の健全性に関する情報提供を行うことが望ましい。
- 要配慮個人情報に該当する PHR を取得する場合には、個人情報保護法 20 条 2 項各号の例外に該当することが見込まれる場合であっても、個人情報保護法 20 条 2 項各号の例外に該当することが明確な場合を除き、事前に利用者から同意を取得することが望ましい。
- 個人データに該当する PHR を第三者に提供する場合には、個人情報保護法上の例外に当たることが見込まれる場合であっても、個人情報保護法上の例外に当たることが明確な場合を除き、事前に利用者から同意を取得することが望ましい。
- 救急・災害時の治療や支援に有用な個人データに該当する PHR を取り扱う PHR サービス事業者は、救急・災害時に本人に適切な治療や支援を行えるよう、PHR サービス開始時に、「救急・災害時に、迅速に有効な診断・治療を行う目的で本人の PHR を利用し、又は医療機関等の第三者に提供すること」について、あらかじめ利用者の意思を確認する機会を提供することが望ましい。
- 個人情報取扱事業者に該当する PHR サービス事業者は、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、こ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 40 条 2 項）。

（２）本人確認

考え方

特に要配慮個人情報を取り扱う PHR サービスにおいては、サービスの継続的な利用において利用者本人の同意が重要である。また、PHR サービス事業者は、PHR サービス利用者が利用するサービスについて、PHR を本人あるいは代理人等の同意なく第三者に閲覧されることがないようにする「機密性」を守る必要がある。更に PHR を本人以外の医療者や事業者が利用することを想定している PHR サービスにおいては、当該 PHR が確かに PHR サービス利用者本人のデータであることを保証する観点に留意し運用を行う必要がある。以上から、特に個人情報取扱事業者に該当する PHR サービス事業者にとっては、確実な本人確認の実施は PHR サービスの運用において極めて重要である。PHR サービス利用時の本人確認は、オンラインでの本人確認（eKYC：electronic KYC（Know Your Customer）の略で、KYC をオンライン上で実現するための仕組みを指す）だけではなく対面や郵送による本人確認（KYC：Know Your Customer の略で、本人確認を行う手続を指す）、氏名、住所、生年月日、メールアドレス等の情報入力など運用面で実施する方法もある。なお、本人確認の際には、個人情報保護法や医療保険各法等の法令を遵守することも必要である。一方で、PHR サービスは日常的な利用が想定されることから、不必要に煩雑な本人確認を行うことは避けるべきである。

ネットワークを利用するサービスで通信している相手が本人かどうかを確認する「認証」の方法については、技術の発展によりデファクトスタンダードが変わり得るため、その時々の最善のスタンダードを採用することが望ましい。現状では、Fast IDentity Online（FIDO[8]）、マイナンバーカードを用いた公的個人認証サービス（JPKI[9]）などの技術が精度の高い認証の方法として期待されている。PHR サービスは、スマートフォンやタブレット等のモバイル端末上に実装され、モバイル端末自体に機密性を確保する認証の仕組みが組み込まれている場合もあるため、その利用も検討する。

最低限遵守する事項

①　開示等の請求の際の本人確認

個人情報保護法に基づく当該本人が識別される保有個人データの開示等の手続における本人確認については、個人情報保護法 37 条 2 項及び通則 GL3-8-7 に留意する必要がある。個人情報取扱事業者に該当する PHR サービス事業者は、円滑に開示等の手続が行えるよう、本人に対し、開示等の請求等の対象となる当該本人が識別される保有個人データの特定に必要な事項（住所、ID、パスワード、会員番号等）の提示を求めることができる。なお、その際には、本人が容易かつ的確に開示等の請求等をすることができるよう、当該保有個人データの特定に資する情報を提供するなど、本人の利便

[8] FIDO Alliance が定めた新しい認証方式。スマートフォン等のローカル環境での本人認証と、公開鍵認証方式のオンライン認証を並行して行う方法。
[9] 公的個人認証サービス（Japanese Public Key Infrastructure）の略。マイナンバーカードの IC チップに記録された「署名用電子証明書」や「利用者証明用電子証明書」を利用した本人認証手段。

性を考慮しなければならない。その確認の方法は、事業の性質、保有個人データの取扱状況、開示等の請求等の受付方法等に応じて、適切なものでなければならず、本人確認のために事業者が保有している個人データに比して必要以上に多くの情報を求めないようにするなど、本人に過重な負担を課するものとならないよう配慮しなくてはならない（個人情報保護法 37 条 2 項、通則 GL3-8-7）。

② その他

モバイル端末あるいは PHR アプリの機能で本人確認・認証を行える仕組みを設ける。

推奨される事項

- PHR を本人以外の医療者や事業者が利用することを想定している PHR サービスにおいては、当該 PHR が確かに PHR サービス利用者本人の PHR であることを保証するための仕組みを設けることが望ましい。
- 本人確認の実施方法は、取り扱う PHR のリスクに応じた方法（eKYC（electronic Know Your Customer）の利用、対面又は郵送、氏名、住所、生年月日、メールアドレス等の情報入力等）を採用することが望ましい。

（3）PHR の管理・閲覧

考え方

PHR は基本的に利用者自身に由来する PGD であり、権利は利用者自身に帰属する。また、個人情報として個人情報保護法が適用され、あるいは利用者のプライバシー権の対象となり得る。そのため、PHR サービス事業者はできる限り利用者が自身の PHR を自由に取り扱える状態を保証することが望ましい。また、保護者による小児・乳幼児の PHR 管理に代表されるように、十分な責任能力を持たない利用者の PHR を代理の者が管理・活用できる仕組みや、責任能力が認められた後の管理権限の移譲についても対応できていることが望ましい。

PHR は、様々なデバイス・測定者・環境によって測定され、蓄積されていくため、その質は玉石混交となる。また、個人的な健康管理としての利用から医療における利用まで幅広い用途で用いられ、その利用目的によって求められるデータの質が異なる。そのため、PHR サービス事業者は、測定機器、測定日時、測定環境など、PHR の発生源や取得方法、PHR の移動・参照の変遷などをメタ情報（データそのものに付帯する情報のこと）として記録し利用者が参照できるようにする。また、異なる事業者間でデータが連携されることも想定し、データ連携の際にはメタ情報も含んで連携できるようにすることが望ましい。これらを通じてデータ及びサービスの質を可視化することが望ましい。

PHR サービスは、血圧計や活動量計など様々なデータを計測する機器と連携して使用されると考えられる。計測機器の活用に当たっては、目的に合った精度の機器を選定すべきである。医療や健康診断、

治験を含む臨床研究においては、一般に高い精度を求めているが、日常の健康管理で使うようなケースで同レベルの精度の機器を求めることは利用者の負担の増大や結果としての測定機会の減少に繋がる可能性もあり、リスクベースアプローチの観点からも避けるべきである。

なお、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、この場合個人情報取扱事業者は、原則として、遅滞なく本人が請求した方法（電磁的記録の提供による方法、書面の交付による方法その他当該個人情報取扱事業者の定める方法）により当該保有個人データを開示しなければならないとされている（個人情報保護法 33 条、個人情報保護法施行規則 30 条）。

また、本人は、一定の場合に、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訂正、追加、削除、利用停止又は消去を請求でき、一定の場合には、個人情報取扱事業者は訂正等を行わなければならない（個人情報保護法 34 条、35 条）。

最低限遵守する事項

- 利用者が自身の PHR を自由に閲覧できること。
- 利用者の求めに応じて PHR を削除できること。
- 健診等情報を取り扱う場合は、業界で合意された一般的な規格に従った形でのインポート及び PHR サービス内のデータのエクスポートができること。

推奨される事項

- PHR の追加・削除・修正・他サービスへの移動を利用者自身が管理できる機能を有することが望ましい。
- PHR の管理に当たっては、データの利活用時の判断を容易にするため、データの入力者、データの測定者、データを測定したデバイス、データを測定した環境、外部から取得した場合はデータの由来（マイナポータル等）、同意取得の範囲、データの削除や修正が行われたことが分かる情報（データベース上でフラグを立てる等を含む）などをメタ情報として記録することが望ましい。
- 健診等情報以外の情報についても、本人の求めに応じてデータをエクスポートできることが望ましい。
- 代理人等が PHR の管理・活用を行える機能及び、利用者本人へ管理機能を移譲する機能を有することが望ましい。
- 管理・閲覧サービスに対するリスクアセスメントを実施し、求めに応じ開示できる体制を確保しておくことが望ましい。
- 管理・閲覧サービスに対するリスクマネジメントシステム（PDCA サイクルの設定や体制）を確立することが望ましい。さらに、管理・閲覧サービスのための組織体制や責任等に言及した情報を開示するとともに、そのサービスに対する定期的レビューを行うことが望ましい。
- 定期的なレビューの期間は、第三者認証を取得しその基準に従うことが望ましい。

・　管理・閲覧サービスに対する利用者側の利便性についても配慮することが望ましい。

（４）PHR サービスにおける個人情報の保護・情報セキュリティ

考え方

PHR サービス事業者が個人情報取扱事業者に該当する場合[10]は、その取り扱う PHR の漏えい[11]、滅失[12]又は毀損[13]（以下「漏えい等」という。）の防止その他の PHR 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 23 条）。当該措置は、PHR 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、PHR の取扱状況（取り扱う PHR の性質及び量を含む。）、PHR 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（通則 GL3-4-2）。なお法第 23 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等は、通則 GL10 に記載されている。

また、個人情報取扱事業者に該当する PHR サービス事業者は、以下の個人データの漏洩等の事態が生じた場合には、原則として、当該事態が生じた旨を個人情報保護委員会に報告し、かつ本人に通知しなければならない（個人情報保護法 26 条、個人情報の保護に関する法律施行規則 7 条）。

一　要配慮個人情報が含まれる個人データ（高度な暗号化その他の個人の権利利益を保護するために必要な措置を講じたものを除く。以下同じ。）の漏えい等が発生し、又は発生したおそれがある事態
二　不正に利用されることにより財産的被害が生じるおそれがある個人データの漏えい等が発生し、又は発生したおそれがある事態
三　不正の目的をもって行われたおそれがある個人データの漏えい等が発生し、又は発生したおそれがある事態
四　個人データに係る本人の数が千人を超える漏えい等が発生し、又は発生したおそれがある事態

情報セキュリティ対策としては、取り扱う情報の要求レベルに応じて、国が定める関連ガイドラインや既存の法令・ガイドライン（「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」を含む。）との整合性の確保に留意しながら、一定の安全管理水準が確保されるようにする必要がある。病歴や健康診断結果に加え、ライフログや環境・生活情報においても、特に思想や信仰などの利用者の信条に関わる情報が含まれていればそれも要配慮個人情報となる可能性があり、その収集や利活用、情報流通等

[10] PHR サービス事業者が個人情報取扱事業者に該当しない場合としては、PHR サービス事業者が個人を識別できる情報を取得せずに、利用者の端末から送信される利用者 ID 等に紐づく形での PHR の管理等のみを行う場合などが考えられる。
[11] 個人データが外部に流出することをいう（通則 GL3-5-1-1）。
[12] 個人データの内容が失われることをいい、その内容と同じデータが他に保管されている場合や、個人情報取扱事業者が合理的な理由により個人データを削除する場合は、滅失に該当しない。（通則 GL3-5-1-2）。
[13] 個人データの内容が意図しない形で変更されることや、内容を保ちつつも利用不能な状態となることをいう（通則 GL3-5-1-3）。

において注意を要する。

なお、PHR サービス事業者が個人情報を取り扱うか否かにかかわらず、PHR は本人の健康に関する情報であるため、その情報の種別や利用用途を鑑みて、改ざんにより健康被害が生じる懸念が高い場合には、改ざん防止対策を適切に実施する必要がある。

幅広い PHR サービスの特性に応じた必要十分な対策を設計するために、一律に要求事項を定めることはせず、リスクベースアプローチに基づいた対応を推奨する。高リスクな情報を扱う場合や、取り扱う情報量や利用者数が多いなど社会的な影響が大きい場合には、別添 2 を参考にリスクマネジメントを実施することを推奨する。

総務省「情報銀行における健康・医療分野の要配慮個人情報の取扱いに係わる方針（2023年7月）」16頁（総務省、経済産業省「情報信託機能の認定スキームの在り方に関する検討会」）を参考とした情報の分類の一例を以下に示す。なお、本ガイドラインにて追加した部分は太字下線表記とした。定義は用語集を参照されたい。

総務省「情報銀行における健康・医療分野の要配慮個人情報の取扱いに係わる方針（2023年7月）」における「健康・医療分野の情報のレベル区分」			PHR用途におけるその他の情報項目例
取り扱いレベル	情報区分	考え方、情報項目例	
レベル0	利用者個人の同意を必要とせずに取得・提供可能な、個人情報に該当しない情報	・統計データ・匿名加工情報	**居住環境、気温、天気**
レベル1	利用者個人の同意に基づいて取得・提供可能な、要配慮個人情報に該当しない健康・医療分野の個人情報	・利用者個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の結果等ではなく、健康診断、診療等の事業及びそれに関する業務とは関係ない方法により知り得た個人情報※ ※例えば、利用者個人の病歴や個人情報の保護に関する法律施行令第2条第1号から第3号までの事項を内容とする記述等は含まれない ※健診機関や医療機関等において医療専門職が管理する情報を除く 【情報項目例】 歩行測定、体重、体脂肪、体温、血圧、脈拍等のバイタルデータ	**歩数、活動量、身長、食事日誌、睡眠日誌、詳細な位置情報**
レベル2	利用者個人の同意と医療専門職（医師、歯科医師、薬剤師、保健師等）の助言に基づいて情報銀行が取得し、データ倫理審査会において医療専門職の助言と承認に基づいて提供可能な※、健康・医療分野の要配慮個人情報 **※「PHRサービス事業者が取得し、利用者個人の同意に基づいて取得・提供可能な」に読み替え**	・「PHR指針」に定める「健診等情報」※に該当し、利用者個人に明示的に開示・説明されており、利用者個人が十分に理解することができる医療情報 ※「PHR指針」に定める「健診等情報」に該当するもの 個人が自らの健康管理に利用可能な個人情報保護法上の要配慮個人情報で、次に掲げるもの及び予防接種歴 ・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 【情報項目例】 法定健診項目（既往歴含む）、アレルギー、お薬手帳、OTC医薬品等	**健診等情報（特定健診結果、高齢者健診結果、乳幼児健診結果、予防接種歴、レセプト情報）、介護記録**
レベル3	レベル2において取り扱いを保留する情報	・利用者個人に明示的に開示・説明されていない、又は利用者個人が十分に理解することが困難な医療情報 【情報項目例】腸内細菌、口腔内細菌、遺伝子情報等	

※ここに記載した具体例、求められるセキュリティ水準は一つの例であり、具体的なサービス提供時には、その内容と想定されるリスクに応じた対応が求められる。

利便性とセキュリティはトレードオフの関係となることも多いため、他項で記載の通りサービスの運用に際して利用者への明示的な説明と同意を得ることが重要である。セキュリティ対策の妥当性と限界について、利用者が正しい理解と明示的な合意のもと PHR サービスを選択・利用できるよう、PHR サービス事業者からのリスクの明確な提示が重要である。特に健診等情報を取り扱う PHR においては、国の提示する PHR 指針におけるチェックリストを参照することが求められる。健診等情報を取り扱わない PHR サービス事業者においても、国の PHR 指針を参照の上で、対応可能な点については対応することが望ましい。

PHR サービスの利用に当たっては、パソコン・スマートフォンなどの広く普及した端末での利用が想定さ

れる。これらの端末に備わっているセキュリティを用いることができる場合には、PHR サービス側でさらに本人認証などを付加することは利便性を損なうことにもなり得るため、端末の標準的なセキュリティを用いることは合理的である。

PHR サービスの普及・発展においては利便性が極めて重要であることから、過度なセキュリティ対策によって、そのコストが PHR サービス利用者に転嫁されたり、PHR サービス利用者の利便性が損なわれたりすることがないように留意すべきである。

【情報セキュリティ事故等発生時における義務と責任】

1. 危機対応義務

   「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）」を参考に、必要な対策を講ずることが望まれる。

2. 民事責任

   情報漏洩等のセキュリティ事故が発生し、PHR サービス利用者等に被害が生じると、PHR サービス利用者等は PHR サービス事業者に対し、契約責任又は不法行為責任に基づき損害賠償を請求することがある。契約責任の場合、PHR サービス事業者がいかなる債務を負っていたのかという、委託契約(サービス提供契約等)の解釈問題となる。また、不法行為責任の場合、PHR サービス事業者の過失の存否等が問題になる。

3. 情報の提供

   PHR サービス事業者は何らかの情報セキュリティ事故が発生した場合、個人情報保護法に従って個人情報保護委員会に報告し、かつ本人に通知する必要がある場合があり、それ以外の場合でも、発生した情報セキュリティ事故に関する情報と PHR サービス利用者に対する影響を速やかに PHR サービス利用者へ提供すべきである。

4. 善後策・再発防止策

   事業者は、発生した情報セキュリティ事故について、速やかに善後策を講じなければならない。さらに、発生した情報セキュリティ事故自体に対応するための施策を講ずるに留まらず、同様の情報セキュリティ事故が以降発生しないように再発防止策を検討することが求められる。

【第三者認証等の取得】

PHR サービス利用者等が適切な PHR サービスを選択するに当たっては、第三者認証の取得も有効である。情報セキュリティに係る第三者認証として、プライバシーマーク認定又は ISMS 認証、セキュリティ管理に係る内部統制保証報告書などがある。特にマイナポータルに接続する事業者や要配慮個人情報を取り扱う PHR サービス事業者などは、情報セキュリティに係る第三者認証の取得が求められる。

【リスクアセスメントにおける留意事項】

リスクアセスメントにおいては、取扱い情報の種別（健診等情報、その他の要配慮個人情報、個人情報、ライフログ、環境情報等）、取り扱う情報量・利用者数、マイナポータル API との接続の有無、他のシステムとの直接のデータ連携の有無、PHR サービス利用者からの入力の有無などを総合的に判断し、過度なリスク対応のために過剰なコストが PHR サービス利用者に転嫁されることのないように留意すべきである。なお、健診等情報を取り扱う PHR サービス事業者については、国の PHR 指針を参照することとする。

【従業者の監督】

PHR サービス事業者が個人情報取扱事業者に該当する場合は、その従業者に個人データを取り扱わせるに当たっては、当該個人データの安全管理が図られるよう、当該従業者に対する必要かつ適切な監督を行わなければならない（個人情報保護法 24 条、通則 GL3-4-3）。

【個人情報管理への委託】

PHR サービス事業者が個人情報取扱事業者に該当する場合は、個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない（個人情報保護法 25 条）。PHR サービス事業者は、適切な委託先の選定を行うとともに、監督義務を果たすため、上記の委託先と適切な内容の委託契約を締結する（通則 GL3-4-4）。

【クラウドサービスの利用】

PHR サービス事業者は、PHR サービスを提供するに当たって、別の事業者が提供する IaaS、PaaS、BaaS 等のクラウドサービスを利用することが考えられる。適切なクラウドサービスを利用することにより、情報セキュリティの向上とコスト削減が実現される。クラウドサービス利用時の責任分担については、責任共有モデル[14]（共同責任モデル）が一般に採用されている。なお大まかなデータ所在地（分散管理をしている場合にはそのそれぞれについて）や準拠法及び管轄裁判所を利用者に示すことが望ましい[15]。

[14] クラウドサービス事業者がクラウドサービスのセキュリティに対する責任を負い、PHR サービス事業者はクラウドサービス内におけるセキュリティに対する責任を負う、といったクラウドサービスのセキュリティにおける基本的な考え方。
[15] 個人情報保護法及び総務省・経済産業省「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン第 1.1 版」等、関連する法令・ガイドライン等を参照の上で適法に対応すること。

【匿名加工情報等の作成及び利用】

PHR サービス事業者が個人情報取扱事業者に該当する場合は、個人データの第三者提供に当たっては、利用者に対して、同意に係る判断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説明した上で、明示的な同意を取得することが原則である（通則 GL3-6-1）。ただし、PHR サービス事業者が匿名加工情報を作成し、かつ、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し、その他個人情報保護法や関係するガイドライン等を遵守した上で、本人の同意を得ることなくこれらの情報を第三者に提供することも考え得る。また、PHR サービス事業者が匿名加工情報や仮名加工情報を作成した上で利用する場合も考えられる[16]。この際には、個人情報保護法及び同法に関する規制や「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）」等のガイドラインを遵守する必要がある。

推奨される事項

① 個人情報の正確性の担保等

PHR サービス事業者が個人情報取扱事業者に該当する場合は、利用目的の達成に必要な範囲内において、個人データに該当する PHR 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 PHR を遅滞なく消去するよう努めるものとする（個人情報保護法 22 条）。その際には、データを単に削除するだけでは第三者へ漏洩し悪用される可能性があることから、復元不可能な手段で削除することが望ましい。復元不可能な削除方式については、総務省「地方公共団体における情報セキュリティポリシーに関するガイドライン」等を参照いただきたい。

なお、消去とは当該データを個人データとして使えなくすることであり、当該データを削除することのほか、当該データから特定の個人を識別できないようにすること等が含まれる（通則 GL3-4-1）。

② 個人情報に係る規定の整備

PHR サービス事業者は、PHR の安全管理に係る基本方針として、以下の事項を運用管理規程に含めることが望ましい。

- 本ガイドライン、提供事業者指針及び医療情報安全管理指針の遵守
- 個人情報保護法やその他最新の関連法令等の遵守
- 個人情報に関して他の情報と区別した適切な管理
- 情報セキュリティに関する基本方針等の情報セキュリティポリシーの策定と公開
- 情報セキュリティポリシーの遵守を担保する組織体制の構築

[16] なお、仮名加工情報（個人情報保護法 2 条 5 項）については、第三者提供が基本的に禁止されている（個人情報保護法 41 条 6 項、42 条 1 項）

③ 委託契約の締結

委託契約には、当該個人データの取扱いに関する、必要かつ適切な安全管理措置として、委託元、委託先双方が同意した内容とともに、委託先における委託された個人データの取扱状況を委託元が合理的に把握することを盛り込むことが望ましい（通則 GL3-4-4）。また、PHR サービス事業者と委託先は、障害が生じた場合等の責任分担について、契約で規定することが望ましい。

④ 定期的な情報セキュリティ対策の見直し

PHR サービス事業者は、情報保護に関する技術が日々進歩していることを踏まえ、定期的に情報セキュリティ対策を見直して改善することが望ましい。なお適切なクラウドサービスを利用することで、クラウドサービス側にて最新の情報セキュリティ対策を実施するなど、見直しのコストが低減することも期待される。

（５）リコメンドの方法（有効性・安全性の確保）

考え方

PHR サービスにおけるリコメンドとは、スマートフォン等のアプリケーションを介して、記録管理された個人の保健医療情報に基づいて、生活習慣改善等に向けた推奨を行うことである。

医行為が誤って提供されると、有効でないばかりか、健康を害する危険もある。医師法 17 条は、「医師でなければ、医業をなしてはならない」と定めている。「医業」とは、医行為を、反復継続する意思をもって行うことであると解されており、医師でない PHR サービス事業者が医業をなした場合には違法となる。また、保健師助産師看護師法に基づき、看護師でない者は傷病者若しくはじよく婦に対する療養上の世話又は診療の補助を行うことを業としてはならないとされている（保健師助産師看護師法 31 条、5 条）。そのため、PHR サービスを提供する際には、それが医行為や診療の補助に該当しないよう注意する必要がある。

医行為や診療の補助の具体例としては、「利用者の身体機能やバイタルデータ等に基づき、個別の疾病であるとの診断を行うことや治療法の決定等を行うこと」や「傷病や障害を有する者に対し、傷病の治療のような医学的判断及び技術を伴う運動／栄養指導サービスを行うこと」が挙げられる（厚生労働省、経済産業省「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」2 頁）。

医師以外の者は、診断を行うことはできないため、検査（測定）後のサービス提供については、検査（測定）結果の事実や検査（測定）項目の一般的な基準値を通知することに留めなければならない。また、検査（測定）項目が基準値内にあることをもって、利用者が健康な状態であることを断定することは行ってはならない（厚生労働省、経済産業省「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」、5 頁）。

PHR サービス事業者は、医師が民間事業者による運動や栄養指導サービスの提供を受けても問題ないと判断した者に対し、自ら診断等の医学的判断を行わず、医師が利用者の身体機能やバイタルデータ等に基づき診断し、発出した運動や栄養に関する指導・助言に従い、医学的判断及び技術が伴わない範囲内で運動や栄養指導に関するサービスを提供できる（厚生労働省、経済産業省「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」、2 頁。）。なお、PHR サービスは、運動や栄養指導に関するものに限定されない。また、①遠隔医療のうち、医師又は医師以外の者－相談者間において、情報通信機器を活用して得られた情報のやりとりを行うが、一般的な医学的な情報の提供や、一般的な受診勧奨に留まり、相談者の個別的な状態を踏まえた疾患のり患可能性の提示・診断等の医学的判断を伴わない行為、②社会通念上明らかに医療機関を受診するほどではない症状の者に対する経過観察や非受診の指示、及び③患者の個別的な状態に応じた医学的な判断を伴わない一般的な受診勧奨については、遠隔健康医療相談として医師以外の者が行うことができると解されている（厚生労働省「オンライン診療の適切な実施に関する指針」、5-6 頁）。この点、遠隔健康医療相談の該当性について、厚生労働省の「『オンライン診療の適切な実施に関する指針』に関する Q & A 」の QA19 では、①及び②の点について、「あらかじめ医師の監修の下で策定されたマニュアル等に従い、年齢、性別、身長・

体重（BMI）といった相談者の属性や症状（発症時期、痛みの程度等）を踏まえ、一般的に可能性があると考えられる疾病についての情報提供や、採血や血圧等の検査（測定）項目に係る一般的な基準値についての情報を提供することが可能です。また、医学的判断を要さずに社会通念上明らかに医療機関を受診するほどではないと認められる症状の者に対して経過観察や非受診の指示を行うこと、患者の個別的な状態に応じた医学的な判断を伴わない一般的な受診勧奨を行うことが可能です。」と説明されている。加えて、当該 QA19 は、遠隔健康医療相談として医師以外も可能な行為の具体例について、以下のとおり説明している。

【具体例】

（１）腰痛の相談に対し、

① あらかじめ医師の監修の下で策定されたマニュアル等に従い、重篤な疾病を疑うべき患者の属性（高齢者等。以下同じ。）や症状等（発熱、脱力等。以下同じ。）がないかを確認し、発熱と両足に力が入らないと説明する患者に対して、「一般に、腰痛の場合、原因が明らかではない腰痛も多いのですが、発熱と両足の脱力といった神経症状を伴うような腰痛の場合には、感染を伴った腰痛である可能性もあります。」と伝える行為 → 遠隔健康医療相談（医師以外も可能）

② あらかじめ医師の監修の下で策定されたマニュアル等に従い、重篤な疾病を疑うべき患者の属性や症状等がないかを確認し、発熱と両足に力が入らないと説明する患者に対して、①を伝えた上で、「一般に、こういった感染を伴った腰痛である可能性がある場合は、早期に医療機関に受診することをおすすめします。」と伝える行為 → 遠隔健康医療相談（医師以外も可能）

③ あらかじめ医師の監修の下で策定されたマニュアル等に従い、重篤な疾病を疑うべき患者の属性や症状等がないかを確認し、そのような症状等はなく、もともと腰痛持ちであり、歩行は可能であると説明する患者に対して、「かかりつけの整形外科にかかることをおすすめしますが、受診までに湿布や解熱鎮痛剤を使用して様子をみることも考えられます。なお、湿布や解熱鎮痛剤の使用に際しては薬剤師・登録販売者の指示や注意事項等をよく聞いて使用してください。」と伝える行為 → 遠隔健康医療相談（医師以外も可能）

④ 数日前に軽い作業後に腰痛があったが、既に痛みが収まって数日経ち、重篤な疾病を疑うべき属性や症状等がなく、既往歴やその他の異常がない患者に対して、経過観察の指示をすること → 遠隔健康医療相談（医師以外も可能）

⑤ 「あなたは骨折です。」や「あなたは椎間板ヘルニアの可能性があります。」と判断して伝える行為 → 診断（遠隔健康医療相談では実施できない）

（２）高血圧の相談に対し、

① ①「日本高血圧学会の診断基準では収縮期血圧が 140mmHg 以上、または拡張期血圧が 90mmHg 以上の場合を高血圧としています。」と伝える行為 → 遠隔健康医療相談（医師以外も可能）

② ①を伝えた上で、「高血圧が気になる場合には、まずは循環器内科等の内科を受診してくださ

い。」と伝える行為 → 遠隔健康医療相談（医師以外も可能）
③ 日本高血圧学会の診断基準に照らし高血圧に該当せず、その他の異常がない患者に対して、経過観察の指示をすること → 遠隔健康医療相談（医師以外も可能）
④ 「あなたは高血圧症です。」と判断して伝える行為 → 診断（遠隔健康医療相談では実施できない）

PHR サービスの第一義的な目的は利用者の健康増進であり、PHR を蓄積・可視化することや、それらをもとに実施されるリコメンドが、「利用者の心身の健康を改善するものであること」「安全なものであること」が求められる。PHR サービスの適切な普及推進において、「PHR サービスの拡大」とリコメンド機能の安全性・有効性確認のための「医療との連携」の両立が大切となる。そのためには、「安全性を確保できる仕組み」や「医療者との連携が必要な範囲」を提示することが重要である。

PHR サービスにおけるリコメンド機能の提供に当たっては、医療機器はもとより、非医療機器である場合においても、リコメンド機能の裏付けとなった科学的なエビデンスの提示や、医学的な監修の取得などにより、有効性・安全性の確保に努めるべきである。[17]

また、関係法令等を遵守した上で、エビデンス等に基づいた安全性や効果を提示するが、サービスの利用者より、その安全性や効果の根拠となるエビデンス等を問われた場合は開示し、その際には、提供するサービスの安全性や効果における妥当性を分かりやすく利用者へ示すとともに、情報源（一次情報、二次情報）、対象者（属性、人数）、測定方法（実施時期やデータ取得、分析方法等）等を明確に示すことで、安全性や効果の信頼性を確保することが望ましい。また、エビデンスは、関係する法令や規格等の変更、ヘルスケアサービスの安全性や効果の根拠となる新たなデータ、研究成果の公表等に応じて、随時見直しを行っていくことが望まれる。

サービス提供時点で十分なエビデンスを認めないものは、エビデンスが十分でない等の表示や他の根拠表現をし、データを蓄積し、有効性、安全性の検証に努めることが望ましい。なお、プログラム医療機器は、承認取得にエビデンスが必須である。加えて、事業者が自己の供給する役務の取引について、その品質、規格その他の内容について、一般消費者に対し、実際のものよりも著しく優良であると示す表示又は事実に相違して当該事業者と同種若しくは類似の役務を供給している他の事業者に係るものよりも著しく優良であると示す表示は、「不当表示」に該当するものとして禁止されていることに留意する必要がある（不当景品類及び不当表示防止法 5 条）。これ以外にも、不正競争防止法の誤認惹起行為（不正競争防止法 2 条 1 項 20 号）、薬機法上の虚偽誇大広告の禁止（薬機法 66 条 1 項）や承認前の医療機器の広告の禁止（薬機法 68 条）等の表示に関する規制が PHR サービスについての表示に関係し得る。

PHR を用いて国民・社会の適切な健康増進を促すためには、リコメンド機能利用時においても、必要に応じて医療が活用されることも大切である。利用者がすでに医療機関を受診している場合は、医療者（かかりつけ医等）に相談の上での利用を推奨すべきである。多種多様な PHR サービスが創出される

[17] リコメンドについて「医療・健康分野における行動変容を促す医療機器プログラムに関する開発ガイドライン２０２３（手引き）」https://www.meti.go.jp/policy/mono_info_service/healthcare/report_iryou_fukushi.html が参考となる。

中で、PHR に関する情報が過多となり、適切な PHR サービスの選択の妨げになる場合が想定される。そのため、個人にとって望ましいリコメンド機能の選択に際して、必要に応じて医療者（かかりつけ医・歯科医・コメディカル等）のアドバイスを受けながら選択することを促すことも触れておくとよい。また、リコメンド機能利用時に有害事象が起こるリスクを考慮して、必要に応じて受診を促すことが望ましい。

＜リコメンドに対する医師への相談を促す際の表示例＞

・ あなたが医療機関を受診している場合は、本サービスからのアドバイスについて主治医に一度、相談してみましょう。あなたが医療機関を受診していない場合でも、本サービスからのアドバイスについては、一度医師（かかりつけ医等）にその内容を確認してもらうため、受診することをお勧めします。

＜一般的なリコメンドの例＞

・ 本サービスからのアドバイスについて、体調で気になることがありましたら、医療機関の受診や定期的な精密検査の受診をしてください。

＜一般的な通知機能の例＞

・ 本サービスからのアドバイスは、〇〇のデータ及び△△の基準に基づくものです。今後の研究によりアドバイスが修正されることがありますので、あらかじめご了承ください。

医療者側が個々の PHR サービスに対する理解を深めるために、PHR サービス事業者は、医療者に情報共有をすることも検討すべきである。

なお、リコメンド機能の目的が、疾病の診断・治療・予防に使用されること、又は人の身体の構造や機能に影響を及ぼすことである場合は、PHR を扱うプログラムが薬機法上の医療機器（一部の疾病診断用プログラム、一部の疾病治療用プログラム及び一部の疾病予防用プログラム）に該当する可能性がある（薬機法 2 条 4 項、同法施行令 1 条、別表第 1、厚生労働省「プログラムの医療機器該当性に関するガイドライン」）。PHR を扱うプログラムが医療機器に該当する場合には、薬機法の規定を遵守する必要がある。例えば、プログラム医療機器の製造販売については厚生労働省による製造販売承認又は第三者機関による製造販売認証を得なければならない。具体的なプログラムの医療機器の該当性やプログラムの医療機器の取扱いについては、厚生労働省「プログラムの医療機器該当性に関するガイドライン」及び薬食機参発 1121 第 33 号、薬食安発 1121 第 1 号、薬食監麻発 1121 第 29 号「医療機器プログラムの取扱いについて」をご参照いただきたい。

最低限遵守する事項

・ PHR サービスを提供する際には、それが医行為や診療の補助に該当しないよう注意する必要がある（医行為や診療の補助の具体例は、V.1.（５）リコメンドの方法（有効性・安全性の確保）

を参照のこと）。

- PHR サービスに関する表示については、不当景品類及び不当表示防止法 5 条の不当表示の禁止及び薬機法 68 条の広告規制等、各種の法令を順守する必要がある。
- PHR サービスを提供するに当たって、PHR を扱うプログラムを開発・利用する際には、場合によっては当該プログラムが医療機器に該当し得ること、一部の医療機器については製造業の登録や製造販売業に許可が必要となることから（薬機法 23 条の 2 第 1 項、23 条の 2 第 3 項）、当該プログラムの開発前に当該プログラムが医療機器に該当するか否か検討する必要がある。そして、当該プログラムが医療機器に該当する場合には、薬機法上の規定を順守する必要がある。

推奨される事項

- リコメンド機能の提供に際しては、関連学会等によるエビデンスがあるものを提供する。最低限の基準がある項目については、リコメンド機能の質の担保のためにも、その基準を満たしたリコメンドを提供することが望ましい（例：特定保健用食品等）。
- リコメンド機能の提供に当たっては、医療者等の監修を受けるなどして、有効性・安全性の確保に努める。有効性、安全性のエビデンスが十分でない場合には、データを蓄積し、有効性、安全性の検証に努めることが望ましい。
- リコメンドサービスに対するリスクマネジメントシステム（PDCA サイクルの設定や体制）を確立することが望ましい。
- リコメンドサービスのための組織体制や責任等に言及した情報を開示することが望ましい。
- リコメンドサービスのプロセスやリソース、指導内容の根拠を提示すること、及び、リコメンドサービスに対する定期的レビューを行うことが望ましい。

＜望ましい例＞

- 糖尿病など基礎疾患を有するものに対し、運動や栄養の指導に関するリコメンドを提供する場合は、事前にかかりつけ医等に相談することを利用規約に明記しておくこと。

＜不適切な例＞

- 病気や障害のある人に対して、診断等の医学的判断を行うアプリを開発し、医療機器認定を受けることなくサービスを提供すること。
- 病気や障害のある人に対して、医師以外が、医学的判断及び技術を伴う内容についてリコメンドサービスを提供すること。
- 科学的なエビデンスや医学的な監修が十分でないまま、画一的に激しい運動についてリコメンドを提供すること。

【PHR を活用したサービスの具体的な事例】

事例 1　個人が健康増進に向けて活用するケース

スマートフォンアプリやウェアラブル端末等から自動的に記録される歩数や活動量等の情報から、健康増進に向けたリコメンドサービス（運動、食事、睡眠等）を提供する。

【解説】昨今、ICT の普及に伴い、歩数、体重などに加え、血圧や睡眠等、健康に関わる様々な情報が自宅等において測定可能となり、ライフログに基づいた運動や食事、睡眠等の生活習慣改善に繋がるリコメンド機能の普及が期待される。一方で、こうしたデータに基づくリコメンドの有効性が十分に証明されていないものや、データの精度が明らかでないものも多い。リコメンド機能の提供に当たっては、医療機器はもとより、非医療機器である場合においても、リコメンド機能の裏付けとなった科学的なエビデンスの提示や、「医療者等の監修を受ける」「根拠のある文献を参照にする」など有効性・安全性の確保に努めるべきである。サービス提供時点で十分なエビデンスを認めないものは、エビデンスが十分でない等の表現や他の根拠表現をし、データを蓄積し、有効性・安全性の検証に努めることが望ましい。なお、プログラム医療機器は、製造販売承認取得にエビデンスが必須である。

事例 2　生活習慣病患者の生活習慣改善を支援するケース

日々の歩数をはじめとした運動、食事などの生活習慣と体重、血圧、血糖などを自身で記録し、そのデータを元にした運動や食事内容のリコメンドを行う。

【解説】昨今、歩数・体重などに加え、血圧や血糖値等の生活習慣病の指標も自宅等において、自身で測定可能な環境が整ってきた。生活習慣病患者に対し、日々の歩数・体重・食事、血圧・血糖等のデータに基づいた運動や食事等についてのリコメンドは生活習慣改善に繋がる PHR サービスとして期待される。糖尿病などの生活習慣病を有する場合は、安全性・有効性の観点からかかりつけ医等に相談しながらサービスを利用することが望ましい。ただし、PHR サービスが医行為や診療の補助に該当する場合は、医療として医師が行い、又は医師の指導の下で行う必要がある。

目的や利用者の状態に合わせた（パーソナライズした）リコメンドを提供できるサービスの創出も求められている。疾患の有無を含めて PHR サービス利用者は多様な背景を持つことを考慮し、例えば、画一的に激しい運動が推奨されることにより、結果として病気の悪化や怪我のリスクを高めてしまう等、個人の健康が損なわれることがないよう留意すべきである。

糖尿病の管理等の治療を目的として、公的な医療保険を適応してリコメンドサービスを提供する場合には、薬事承認を取得し医療機器認定されているアプリを使用する必要がある。医師が医療機器認定を受けたアプリを用いて行う場合を除き、リコメンドサービスが医行為に該当しないよう留意する。

事例 3　禁煙指導に活用するケース

禁煙外来に通院しながら、保険適用となった禁煙治療用アプリを使用できるようになった。また、一般的な禁煙サポートアプリを個人として使用することも可能である。

【解説】禁煙外来の指導は医行為であり、医師によって行われる。当該指導を公的な医療保険を適用して提供する場合には、薬事承認を取得し医療機器認定されているアプリを使用する必要がある。それ以外の禁煙にむけた工夫やモチベーション向上に関することについては、医療機器認定されていないアプリによるライフログを活用した PHR サービスを使用することが可能である。

事例 4　災害時における治療内容の確認や治療継続の支援に活用するケース

災害時に内服薬がなくなってしまった場合、PHR を参照することで、救護所やかかりつけでない医療機関でも迅速かつ正確に処方を確認し、治療の継続が可能となる。

【解説】災害時の治療内容の確認と継続支援は PHR のメリットの一つである。緊急時に最低限の本人確認が実施される条件で事前の説明と同意があれば、必要な保健医療情報（アレルギー、内服薬、既往歴等）を確認することができ、本人の利益につながる医療を提供することができる。

なお、人の生命、身体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には、本人の同意がなくとも個人データの第三者提供は認められる（個人情報保護法 27 条 1 項 2 号）。しかし、このような個人情報保護法上の例外に該当するか判断に迷う状況も想定されることから、あらかじめ、災害時の情報提供先（救急隊員、医療機関、DMAT 隊員等）や提供する情報の内容等について検討し、具体的に「説明と同意」を得ておくことが望ましい。

事例 5　救急時における治療内容の確認や医療者への情報提供に活用するケース

救急搬送時や救急医療機関へ受診した際、救急隊員や搬送を受け入れた医療者が PHR を確認し、普段のバイタルサイン（血中酸素飽和度、心拍数、血圧、体温など）、既往歴、内服薬、血糖値などを把握することができれば、救急医療の質の向上に繋がり、患者へのメリットとなる。在宅用の医療機器等を普段から使用している場合、その設定も医療者が確認することができる可能性がある。

【解説】救急時は意識がない状態で搬送されることもあるなど本人との意思疎通が難しい場合も多く、また個人情報保護法上の例外に該当するか判断に迷う状況も想定されるため、閲覧権限等は事前に「説明と同意」を得ておくことが望ましい。参照可能なデータの範囲を事前に本人が指定できるようにしておくことも必要である。

事例 6　職場（産業保健領域）で活用するケース

従業員の健康診断結果やメンタルヘルス情報（ストレスチェック等）を本人の同意の下で PHR として活用することで、本人の健康増進、生活習慣病の改善に繋がるほか、産業医が復職判定や就業措置を行う際等にも活用することができる。

【解説】職場での健康情報も PHR として活用が可能である。ただし、PHR としての活用は本人の意思のもとで本人の健康増進や職場の環境改善のために行われることが前提であり、その情報の扱いは慎重に行う必要がある。

原則として、職場における健康情報の保存責任者は事業者（契約関係のある事業主及び健診実施機関等）であり、産業医や産業保健師が責任を持って管理をしなければならず、健診結果等が直接の上司などの第三者に閲覧可能な状態で渡されるようなことがあってはならない。状況に応じて衛生管理者をはじめとする他の産業保健スタッフが健康情報を取扱う場合があるが、この場合、関係する全ての人々に守秘義務があることを認識させるべきである。このことは事業者の責務である。また、当該事業者は、その事業場における心身の状態の情報の適正な取扱いのための規程を策定する必要がある（平成 30 年 9 月 7 日労働者の心身の状態に関する情報の適正な取扱い指針公示第 1 号）。事業場に送られてくる全ての従業員の健康管理情報は、産業医がいる事業場においてはまず産業医に届くようにすべきであり、本人の上司や人事・労務担当者が直接受け取るシステムになっている場合は、これを抜本的に改善しなければならない。

事例 7　睡眠改善に活用するケース

睡眠に関するデータはアンケートなどの個人記録によるものや、ウェアラブルセンサー等によるライフログとして記録されるものがある。それらのデータを基にした PHR サービス事業者からのリコメンドによって自ら睡眠習慣の改善を試みたり、産業医と勤務時間や就業形態などの相談を行なったりできるようにしてもよい。また、睡眠時無呼吸症候群などが疑われるデータの場合、医師による診断や早期治療に繋げるために、医行為に該当しない範囲で受診を勧めてもよい。

【解説】ライフログデータを活用した PHR サービスによって改善が期待されるものの一つに睡眠がある。睡眠パターンなどの記録から、入眠時刻、起床時刻に加えて、入眠前の食事・アルコール摂取や運動等の生活習慣についてのリコメンドがあってもよい。ただし、睡眠障害に対する内服治療が求められる場合や、睡眠時無呼吸症候群の診断が求められる場合は受診を促すにとどめ、診断を含む医行為を行ってはならない。

事例 8　内服薬の管理や服薬支援に活用するケース

PHR に本人の薬剤情報（処方薬、アレルギー歴など）を記録することで、内服薬の重複や併用

禁忌がないかをチェックし、フィードバックすることができる。また、内服記録を行うことで、手持ちの内服薬の残量も把握でき、服薬支援や処方薬の調整を行いやすくなる。

【解説】PHR に本人の薬剤情報が記録されることで、医師、薬剤師、看護師が本人に合わせた処方や服薬指導ができるようになる。他の医療機関に受診・入院する際も、処方内容が把握しやすいため、医療の継続性が担保されるほか、無駄な処方を減らすことができる。そのためには、参照する薬剤データや参照方法は標準化されている必要がある。

事例 9　地域包括ケアで活用するケース

PHR によって本人の日々の状態（体重、食事、排便、体温、血圧等）を記録し、本人・家族が承認した範囲でかかりつけ医、訪問看護ステーション、介護施設の担当者等が参照することができるようにすることで、多職種で共有が必要な情報を見逃さないようなサービスが提供されてもよい。

【解説】ライフログや PHR は本人あるいは法定代理人等の同意のもと、関係者間で閲覧されてもよい。ただし、原則として、個人データを第三者に提供してはならないため、あらかじめ書面で「閲覧する対象者及び内容」について具体的に説明し、同意を得ておく必要がある。

事例 10　母子保健で活用するケース

産後のサポートを行うアプリ等を活用し、産後うつなどの症状が見られた場合に、医行為に該当しない範囲で地域のサポートを得るようにリコメンドを行っても良い。また、本人（未成年者、成年被後見人、被保佐人及び被補助人が判断できる能力を有していないなどの場合は、親権者等）の同意が得られていれば、行政と連携して、早期の支援に繋げてもよいだろう。

【解説】出産前の妊婦検診の結果、出産後の新生児／乳児の発達や母の状態（身体的、精神的な指標）を医療機関や行政（母子保健部門）と共有し、必要な支援が提供されるような取り組みである。乳幼児健診の結果が PHR に反映されるとともに、養育者によってこどもの身体発育や運動発達、精神発達などの指標を記録していくことで、適切な支援（養育サポートや子育て支援、事故予防）を受けられるようにリコメンドをしてもよい。

事例 11 ワクチン接種において活用するケース

かかりつけ医等が提供するワクチンスケジューラーで予約をすると、「問診も PHR 上の過去の記録から転載された上で予約され、ワクチンが予約状況に従って納入される」、「接種当日は、接種記録が PHR に反映されるとともに、定期接種のワクチンであれば実施記録が行政へも報告される」といったサービスも有用と思われる。

【解説】ワクチン接種は、個人のライフステージに合わせて管理されるべきものであり、かつ、接種履歴や副反応の管理など正確な接種情報を行政や医療機関等と共有することが求められるため、PHR サービスの活用が期待される分野の一つである。医療と物流、行政が連動するようなシステムが構築されてもよい。ワクチンスケジューラーのように予定をリコメンドする機能とともに、PHR として接種記録（Lot 番号を含む。）が保存されてもよい。新型コロナウイルス感染症対策として、今後期待されるワクチン接種の普及に当たっても活用が期待される。小児期・学童期のワクチン接種歴を大学入学時や成人後に確認するに当たっても PHR サービスの活用が有効である。

事例 12　PHR サービスの利活用を支援するケース

PHR サービス事業者が利用者に対してマイナポータルからデータを入手して日々の健康増進に役立てることを促したり、健康情報を収集・活用することを助言したりするサービスを提供する。
【解説】PHR サービスとして活用できるデータが数多く存在し、今後も増加すると思われるが、十分に活用しきれていないのが現状である。利用者が活用できるデータの存在を提示し、その活用のためのデータ出力の仕方を助言する等のサービスが提供されてもよい。同時に、そのデータを活用することによって得られる利用者のメリットや活用時の留意点を提示することも望ましい。

事例 13　日常の環境・生活に関係する情報を健康増進に活用するケース

行動歴・購買歴・その他の情報（環境、気温、天気等）を含めた日常の生活情報を、PHR として個人の健康管理・増進に活用するサービスを提供する。
【解説】スマートフォンやウェアラブル端末の普及により、日常の生活情報（行動履歴・旅行歴・購買情報等）や気温・天気を含む環境情報等を用いて、個人の健康管理・増進に向けたリコメンドを行うサービスの提供が想定される。日常の生活情報を活用することで、より個々に最適化されたリコメンドが提供できる可能性があり、さらに新たな医学的エビデンスの創出が期待される。一方で、生活や環境に関する情報には、思想や信仰などの利用者の信条に関わる要配慮個人情報が含まれる可能性があるため、「個人情報」と「プライバシー」の保護に十分に留意したサービスとされるべきである。

事例 14　COVID19 等の新興感染症対策としての健康観察での活用ケース

COVID-19 等の新興感染症対策として、自宅で熱や呼吸器症状・倦怠感等の健康状況を記録し、保護者や保健所職員その他の健康管理者と情報共有するサービスを提供する。
【解説】COVID-19 のクラスター対策においては、自宅やホテル等の病院外での健康観察の効率的な仕組みの構築が喫緊の課題である。感染症対策での観察項目は日常の健康観察の延長線上

にある。PHR に COVID-19 特有の観察項目を収集できるように拡張することで、効率的に COVID-19 に関する病院外での健康観察を実施できる。保健所が実施する積極的疫学調査への協力のみならず、感染症の早期発見や自発的な自宅隔離により、感染蔓延防止に寄与することが可能となる。データの第三者提供を伴う場合は、同意取得と個人情報保護に十分に留意したサービスとする必要がある。

（６）他の事業者・第三者へのデータ提供

考え方

１（１）で論じたように、個人データの第三者提供を行うためには、原則として、事前に本人の同意を取得する必要がある（個人情報保護法 27 条）。しかしながら、以下の場合には、例外的に本人の同意のない個人データの第三者提供が認められる（個人情報保護法 27 条 1 項）。

一　法令に基づく場合
二　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。
三　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。
四　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。
五　当該個人情報取扱事業者が学術研究機関等である場合であって、当該個人データの提供が学術研究の成果の公表又は教授のためやむを得ないとき（個人の権利利益を不当に侵害するおそれがある場合を除く。）。
六　当該個人情報取扱事業者が学術研究機関等である場合であって、当該個人データを学術研究目的で提供する必要があるとき（当該個人データを提供する目的の一部が学術研究目的である場合を含み、個人の権利利益を不当に侵害するおそれがある場合を除く。）（当該個人情報取扱事業者と当該第三者が共同して学術研究を行う場合に限る。）。
七　当該第三者が学術研究機関等である場合であって、当該第三者が当該個人データを学術研究目的で取り扱う必要があるとき（当該個人データを取り扱う目的の一部が学術研究目的である場合を含み、個人の権利利益を不当に侵害するおそれがある場合を除く。）。

また、以下の場合には、「第三者」への個人データの提供に該当しない（個人情報保護法 27 条 5

項）。

一　個人情報取扱事業者が利用目的の達成に必要な範囲内において個人データの取扱いの全部又は一部を委託することに伴って当該個人データが提供される場合 二　合併その他の事由による事業の承継に伴って個人データが提供される場合 三　特定の者との間で共同して利用される個人データが当該特定の者に提供される場合であって、その旨並びに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及び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について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いているとき

それ以外にも、個人データの第三者提供については、①確認・記録義務が存在すること及び②第三者提供停止の請求の制度があることに留意する必要がある。

自らデータは収集せずに、既に収集されたデータの提供（データ複製の発生を認める。）や預託（データ複製の発生を認めない。）を受けて、そのデータに付加価値をつけて利用者に提供する PHR サービスも考えられる。その際、PHR サービス利用者がより自身のデータを活用しやすくなるよう、データ流通についてオープンプラットフォーム化されることが望ましい。データの授受にあたり一定の対価が発生することも考えられるが、PGD の考え方に則り、高額な対価によって個人の意思によるデータの流通が阻害されることのないように留意する必要がある。なお、外国にある第三者に個人データを提供する場合の記録義務等の適用については取扱いが細かく分かれており、外国にある第三者に個人データを提供する場合には、個人情報の保護に関する法律についてのガイドライン（外国にある第三者への提供編）を参照すること。

最低限遵守する事項

【個人情報の第三者提供】

①　同意の取得

1（1）で述べたように、個人情報取扱事業者に該当する PHR サービス事業者は、原則として、個人情報の第三者提供を行う前に本人の同意を取得する必要がある。なお、同意の取得方法等、具体的な内容については 1（1）を参照されたい。

②　確認・記録義務

PHR サービス事業者が個人情報取扱事業者に該当する場合は、個人情報の第三者提供に当たって、個人情報保護法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（第三者提供時の確認・記録義務編）を遵守する必要がある。

例えば、個人データの提供者は、提供年月日・受領者の氏名等を記録し、それを一定期間保存する

義務を有する（個人情報保護法 29 条）。また、受領者は、原則として、提供者の氏名、取得経緯等を確認し、提供を受けた年月日・確認に係る事項等を記録し、一定期間保存する必要がある（個人情報保護法 30 条）。

なお、国の機関等と個人データの授受を行う場合には確認、記録義務は課されないことに留意する必要がある（個人情報保護法 29 条 1 項、16 条 2 項各号）。上記の通り、個人情報取扱事業者が、個人データを第三者に提供したときは、基本的に記録を作成しなければならないが、個人情報取扱事業者が本人からの委託等に基づき当該本人の個人データを第三者提供する場合は、当該個人情報取扱事業者は「本人に代わって」個人データの提供をしているものであって、この場合の第三者提供については、提供者・受領者のいずれに対しても確認・記録義務は適用されない（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）2-2-1-1）。

③　第三者提供停止の請求

PHR サービス事業者が個人情報取扱事業者に該当する場合は、個人情報保護法 35 条 3 項に基づき第三者提供停止の請求を受け、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、当該第三者提供を停止しなければならない（個人情報保護法 35 条 4 項）。

④　医療機関に該当する PHR サービス事業者による PHR の提供

医療機関に該当する PHR サービス事業者[18]が、第三者提供を含めた個人情報の取扱いをする際には、対象とする PHR が要配慮個人情報を含む可能性もあることから、個人情報保護法及び各種ガイドラインに加え、医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンスを参照する必要がある。

※情報銀行の指針については、情報信託機能の認定に係る指針 Ver3.0 を参照のこと

推奨される事項

- 匿名加工情報を第三者提供する場合、提供内容を説明しておくこと、提供先など取扱いを適宜、事業者の Web サイトやパンフレット等で公開すること
- 改正次世代医療基盤法（医療分野の研究開発に資するための匿名加工医療情報及び仮名加工医療情報に関する法律）等の、法令によって定められた方法に従って第三者提供を行うこと

[18] なお、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事業者は「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」（総務省・経済産業省）の対象となることに留意されたい。

２．PHR サービス間のデータ連携に関する考え方

本人が生涯にわたり、自身の意思で自身の健康・医療情報を活用して健康増進を実現するため PHR を継続して利活用することが期待されている。

多様な PHR サービスの全てを単一の PHR サービス事業者が提供し得るとは考えにくく、利用者は様々な PHR サービス事業者が提供するサービスの中から最適なものを組み合わせて使用することが想定される。また一方で、PHR サービス事業者がサービス内容の変更やサービスを終了する可能性もある。こうした可能性を考慮すると、サービス利用者が、PHR を自らの意思で、事業者に捕らわれる事無く保管可能となることが求められる。

しかし現時点では、PHR サービス事業者ごとに個別に作成し運用されているサービスそのものを、組織やビジネスプロセスの壁を越えて連携させることは容易ではない。また PHR サービスによって取り扱うデータは多岐にわたるため、すべてのデータについて PHR サービス間の連携を強要することはサービス事業者に過度な負担を強いることになり、現実的ではない。

これらの背景より、利用者が PHR を有効かつ継続的に活用するために、特に価値が高いと考えられる項目について、共通性が担保されたデータフォーマットで他のサービスへ移動・活用できる「データポータビリティ」を確保することが望ましい。

具体的には利用者が複数 PHR サービスを同時に利用したり、サービス終了時に他事業者にて PHR を継続利用したりできるよう、利用者が使用中の PHR サービスから、ある程度の共通性が担保されたデータフォーマットで本人が必要な時に自身の PHR を出力可能とすること等（具体的な項目や交換規格）が考えられる。

また、PHR サービスによっては、データの変更・追加・削除が可能なサービスも存在するため、データの由来や真正性が確認できる情報や同意取得の範囲に関わる情報をメタデータとして保持すること、エクスポート時にメタデータと合わせて出力することが望ましい。

その際、事業者や関連団体との間でのコンセンサスを得ることで、実効性を持つと考えられる。

PHR サービス事業者は、利用者からの信頼を得るためにも、一定の社会的合意に基づきサービス利用者の不利益が利益を上回ることのないよう、安全性を担保する必要がある。また、サービスの安全性について利用者が理解しやすいように情報提供または開示することが望ましい。
観点としては、個人情報保護法のもと個人情報やプライバシーといった個人の権利を侵害しないことや、情報が漏洩、悪用されることを抑止する情報セキュリティがある。[19]

---

[19] 安全性担保に関しては V.1.（４） PHR サービスにおける個人情報の保護・情報セキュリティも参照されたい。

PHR サービス事業者間で連携する場合、サービス連携する PHR の範囲・状況、データ提供先、利用目的、PHR サービス事業者の管理・相談体制等などについて、利用者が理解しやすいように情報提供または開示することが望ましい。

また PHR サービス事業者が自らのサービス連携先を決める際には、少なくとも、連携先サービス事業者のセキュリティレベルを把握していることが必要である。サービス連携を行う事業者間で取り決められたセキュリティレベルは、利用者に適切に公開されることや利用者が適切な PHR サービスを選択できるよう、サービス連携の担保の度合いについて公表したり、第三者による評価が行われたりすることで利用者の信頼を高める等の努力が期待される。

３．その他 PHR サービスの普及、質の向上に関連する事項

（１）PHR 利活用へのリテラシーの向上

PHR サービス事業者による安全かつ有効な PHR サービスを支援するために、PHR 関連団体、関連医学系学会や医師会等が、患者の個人情報の取扱いを担う医療機関や医療者及び PHR サービス事業者の育成に積極的に関わることが望ましい。具体的には、PHR サービス事業者は、医療者や関連する団体・学会等に対して、PHR に関する国内外の動向や利活用事例、最新の知見を提供する等、PHR 利活用の理解を高めるような取り組みを行うことを心がけるべきである。そのために、PHR や健康に対するリテラシーの向上に向けて、学校での健康教育や社会啓発を充実させることが求められる。さらに、PHR サービス事業者は、利用者に対しても、PHR サービスの使い方やセキュリティにおけるリスクを適切に説明する努力をすることが求められる。さらに、各社・団体の Web サイトにおける広告掲示など PHR に関する広報強化についても検討されるべきである。

（２）PHR サービス事業者への教育

PHR サービスは、利用者の健康状態や医療における意思決定に影響を及ぼす可能性を持つこと、利用者自身の情報を預かり本人の了承のもとで活用するサービスであること、利用者の要配慮個人情報を電子的に管理すること等から、その適切な運営のためには医療、倫理、法律、情報セキュリティに関する知識と理解が必要とされる。PHR サービス全体の水準を高く保つためには継続的な学びと教育の機会が必要であり、PHR サービス事業者内での適切な教育・研修の実施や、PHR サービス事業者による業界団体等によって定期的な勉強会や意見交換をする場や、相談窓口等が設けられることが望ましい。

（３）PHR サービスの運用体制の構築と質評価／フィードバック／認証

【PHR サービスの運用体制の構築】

PHR サービス事業者は、提供される PHR サービスの質を担保するために、安全性・有効性・信頼性に加え、利用者が得ることが期待される便益やプライバシーに対するリスクを明確にし適切な対応がなされるよう PHR サービスの運用体制を構築するべきである。また、利用者向けのサポートサービスの体制についても構築されることが望ましい。

推奨される事項

- データガバナンス体制を確立すること
  例えば、下記のような内容が想定される。
  - ✓ PIA（個人情報保護評価又はプライバシー影響評価）の手法を用い、データの内容や性質、量や範囲の必要十分性、データの流れ、データの取扱いに関わる者の範囲、データの利用目的、安全管理レベル等の事前評価を実施する。
- 脆弱性診断等システムにおける安全性の確保（バリデーションプロセス：顧客、監査など）に努めること。
- 情報管理責任者とカスタマーサポート体制を確立すること。
  例えば、下記のような内容が想定される。
  - ✓ PHR サービスについての文書化された取扱説明書、取扱い手順、又はそれに類するものを提供する。
  - ✓ 適切に開発、管理及びサポートを実施する専門分野に対する経験及び資格又は能力がある十分なスタッフの用意の有無を明示する。
  - ✓ インシデントが発生した際のユーザーへの報告方法を明確にする。
  - ✓ PSIRT[20]体制を構築する。
  - ✓ アプリケーションプライバシーポリシーを明示する。
  - ✓ 特商法対応（提供者の明示）を行う。
  - ✓ PHR サービスの運用やカスタマーサポートの体制を開示する。
  - ✓ PHR サービスの健康情報管理における実績を何らかの形で開示する。（例：国内外の学会論文・第三者機関が認定する実績データ）
  - ✓ PHR サービス停止時の事前告知、サービス終了時の告知方法を明示し、かつ他社サービスへの引継ぎ方法などを開示する。

[20] Product Security Incident Response Team の略。自社で開発・提供した IoT 機器/サービスのセキュリティ対策を担い、社内外の関係者との連携、脆弱性関連情報の収集、インシデント発生時の対応などを行う。

【PHR サービスの質評価】

PHR サービスの質を評価する方法として、PHR サービス事業者が自社の PHR サービスについて自己チェックを行うために作成された「PHR サービス自己チェックリスト」を用いて、各 PHR サービス事業者が安全性・有効性・信頼性を含む PHR サービス提供状況に沿って記載し、PHR サービスの質確保に努めることが望ましい。また、PHR サービス事業者や地方公共団体が、チェック状況を踏まえて各々の現状を可視化するよう、記入済の PHR サービス自己チェックリストを各社ホームページで公開することが望ましい。また、PHR サービス提供におけるバリデーションプロセス、責任者やカスタマーサポートの設置等の運用体制の構築や、サービス提供中に、問題や懸念があれば医療専門職が支援する等の信頼性を確保する体制を整えることも検討されるべきである。
※別添の PHR サービス自己チェックリスト参照

推奨される事項

・ 質評価のために PHR サービス自己チェックリストを活用すること

【認証・モニタリング制度】

本ガイドラインに沿った PHR サービスが提供されているかどうかの確認のためには、医師会をはじめとする医療者やアカデミア、及び PHR サービス事業者を含む専門委員会における検証・評価を行う体制を構築されることが望ましい。具体的には、PHR サービスの質の維持・向上を目的とした PHR サービス事業者の認証制度の構築や、サービス内容の確認とフィードバック等を行うモニタリング制度の確立等である。さらに、PHR サービスに関する問い合わせ窓口を設け、利用者からの PHR サービスに係る苦情の際の調査や、事業者からの質問に対応する仕組みを構築し、定期的にガイドラインのレビューを実施することも検討されるべきである。

最低限遵守する事項

マイナポータルに接続し、健診等情報を入手する PHR サービス事業者は、最低限の情報セキュリティの適格性を利用者等へ示すため、プライバシーマーク認定又は ISMS 認証などの情報セキュリティに係る第三者認証を取得すること。

推奨される事項

健診等情報を取り扱う PHR サービス事業者は、プライバシーマーク認定又は ISMS 認証などの情報セキュリティに係る第三者認証を取得すること。

（４）エビデンスの蓄積

PHR サービスは人々の健康を支える重要な基盤になることが期待されているが、そのためには PHR サービス利用の効果を証明するエビデンスの蓄積が必要である。PHR サービス事業者が大学や研究者等と幅広く連携し、真に人々の健康増進に資する PHR サービスを確立していくことが期待される。

VI.　広告その他の表示[21]

（本章における「広告その他の表示」とは、PHR サービス自体の広告のことであり、PHR サービス内の広告は対象外とします）

１．広告その他の表示上の考え方

（１）問題となりえる法規制

PHR サービスの広告その他の表示に関する法規制は多岐にわたるが、代表的なものとしては、景品表示法、不正競争防止法、薬機法、特定商取引法、消費者契約法などが挙げられる。以下では、各法令の概略を示すこととする。

①　景品表示法

- **優良誤認表示**

  商品又は役務の品質、規格その他の内容について、一般消費者に対し、実際のものよりも著しく優良であると示し、又は事実に相違して当該事業者と同種若しくは類似の商品若しくは役務を供給している他の事業者に係るものよりも著しく優良であると示す表示であって、不当に顧客を誘引し、一般消費者による自主的かつ合理的な選択を阻害するおそれがあると認められるもの(優良誤認表示)は禁止されている（景品表示法 5 条 1 号）。

- **有利誤認表示**

  商品又は役務の価格その他の取引条件について、実際のもの又は当該事業者と同種若しくは類似の商品若しくは役務を供給している他の事業者に係るものよりも取引の相手方に著しく有利であると一般消費者に誤認される表示であって、不当に顧客を誘引し、一般消費者による自主的かつ合理的な選択を阻害するおそれがあると認められるもの(有利誤認表示)を禁止されている（景品表示法 5 条 2 号）。

- **事業者が講ずべき表示の管理上の措置**

  商品又は役務の取引について、表示により不当に顧客を誘引し、一般消費者による自主的かつ合理的な選択を阻害することのないよう、商品又は役務の品質、規格その他の内容に係る表示に関する事項を適正に管理するために必要な体制の整備その他の必要な措置を講じることが求められている（景品表示法 26 条）。

---

[21] 「VI. 広告その他の表示」の内容は、ヘルスケア IoT コンソーシアム （現 ヘルスケア AIoT コンソーシアム）にて、令和 3 年 12 月に公表された「ヘルスケアアプリケーションの表示に関するガイドライン」の内容を基に作成されたものです。同ガイドラインの詳細については、以下のウェブサイトをご覧ください。
https://healthcareiotcons.com/news022/

例えば、商品又は役務の表示が、優良誤認表示又は有利誤認表示に当たらないかどうか確認することのほか、確認した事項を適正に管理するための措置を講じることが求められる。

- **措置命令と課徴金**

  優良誤認表示又は有利誤認表示を行った場合には、措置命令又は課徴金納付命令を課され得る（景品表示法 7 条 1 項、8 条 1 項）。なお、令和 5 年景品表示法改正により、優良誤認表示又は有利誤認表示を行った場合は、百万円以下の罰金が科され得ることとなった（本ガイドライン制定時点で未施行）。

② 不正競争防止法

不正競争防止法上、商品若しくは役務又はその広告若しくは取引に用いる書類若しくは通信にその商品の原産地、品質、内容、製造方法、用途若しくはその役務の質、内容、用途若しくは数量について誤認させるような表示等（誤認惹起行為）を不正競争（同法 2 条 1 項 20 号）として禁止されている。

「誤認させるような表示」に該当するかどうかは、個別・具体の事案に応じて、当該表示の内容や取引界の実情等、諸般の事情が考慮された上で、取引者・需要者に誤認を生じさせるおそれがあるかどうかという観点から判断される。

不正の目的をもって誤認惹起行為を行った場合は、罰則が科され得る（不正競争防止法 21 条 3 項 1 号）。

③ 薬機法

薬機法上、医療機器等の名称、製造方法、効能、効果又は性能に関して、明示的であると暗示的であるとを問わず、虚偽又は誇大広告は禁止されている（薬機法 66 条 1 項）。また、医療機器等の効能、効果又は性能について、医師その他の者がこれを保証したものと誤解されるおそれがある記事を広告し、記述し、又は流布することも禁止されている（同条 2 項）。

また、承認前の医療機器等の広告は禁止されている（薬機法 68 条）。

これらに違反した場合は、措置命令等が課され得るほか（薬機法 72 条の 5 第 1 項）、虚偽又は誇大広告を行った場合は課徴金納付命令が課され得る（同法 75 条の 5 の 2 第 1 項）。また、罰則の対象にもなり得る（同法 85 条 4 号、5 号）

④ 特定商取引法

特定商取引法は、消費者被害が生じやすい取引類型を定めた上で、当該取引類型に該当する場合には一定の規制を課すものである。

例えば、通信機器又は情報処理の用に供する機器を利用する方法により売買契約又は役務を有償で提供する契約(以下「役務提供契約」という。)の申込みを受けて行う商品の販売又は役務の提供は、原則として「通信販売」に該当する(特定商取引法 2 条 1 項 1 号、2 項、同法施行規則 2 条 2 号)。

「通信販売」に該当する場合、広告や申込みの最終確認画面において、一定の内容の表示が義務付けられるほか（特定商取引法 11 条、12 条の 6）、誇大広告が禁止される（同法 12 条）。

これらに違反した場合、行政処分(指示、業務停止命令等)の対象となるほか(特定商取引法 14 条、15 条、15 条の 2)、誇大広告等規制や行政処分の違反については、罰則の対象となる(特定商取引法 70 条 2 号、71 条 2 号、72 条 1 項 1 号)。

⑤ 消費者契約法

事業者が消費者契約(有償・無償を問わない。)の締結について勧誘をするに際し、重要事項について事実と異なることを告げること(不実告知。消費者契約法 4 条 1 項 1 号)、又は重要事項等について消費者の利益となる旨を告げ、かつ、不利益となる事実を故意又は重過失によって告げなかったこと(不利益事実の不告知。同条 2 項)等があった場合には、消費者はこれにより締結された消費者契約を取り消すことができる。

（２）PHR サービスに関する表示

PHR サービスには多様なサービスの形態が考えられるところであるが、特に、利用者の健康づくり等のリコメンドをするサービスに関し、当該サービスを利用することにより一定の健康増進効果が認められる旨の広告をする場合においては、健康増進効果を過度に表示することがないよう留意すべきであり、表示を行うに足る合理的な根拠を有しているかを意識しながら表示内容を決定することが重要である。

なお、PHR サービスに係るプログラム医療機器その他の医療機器（薬機法上の承認又は認証を必要とするもの）について、当該承認等を受けていないものについては、その名称、製造方法、効能、効果又は性能に関する広告をしてはならない（薬機法６８条）。また、医療機器の広告には、医薬品等適正広告基準（薬生発 0929 第４号平成２９年９月２９日）が適用されるため、同基準を踏まえた上で広告を行う必要がある。例えば、①効能効果、性能及び安全性関係の表現等の制限、②医療用医療機器の広告の制限、③他社の製品の誹謗広告の制限、④医薬関係者等の推せんの制限、⑤不快、迷惑、不安又は恐怖を与えるおそれのある広告の制限、⑥テレビ、ラジオの提供番組等における広告の取扱い等について規定されている。加えて、医療機器の広告の観点からは、日本医療機器産業連合会が医療機器のプロモーションを行う際に遵守すべき行動基準として定めた「医療機器業プロモーションコード」等にも留意が必要である。

以下では、医療機器以外の広告や表示について説明する。

（３）法令上問題となるおそれのある広告その他の表示の要素

① 解消に至らない身体に係る問題事項等の例示

PHR サービスを利用することでは解消に至らない健康上の問題に係る不安や悩み等の問題事例を例示する表示や、PHR サービスの利用だけではおよそ得られない身体の変化をイラストや写真を用い

るなどにより表示することは、一般消費者が、表示全体から受ける印象によって当該アプリを使用するだけで当該身体に係る問題が解消されるものと誤認する蓋然性があり、そのような表示は、著しく事実に相違する表示又は実際のものより著しく優良であると人を誤認させるような表示に当たるものとして、景品表示法等上問題となるおそれがある。

② 人の疾病の診断、治療若しくは予防に使用されることが目的である旨等の表示

PHR サービスが人の特定の疾患の診断、治療、又は予防に使用されることが目的である旨を表示することや、特定の疾病名を示すことにより、当該疾病の予防・治療効果が得られるかのように表示することは、当該 PHR サービスが医療機器ではない場合にあっては、承認前の医療機器に該当すると判断される可能性があり、薬機法等上問題が生じるおそれがある。

③ 実験結果及びグラフ

広告その他の表示において試験結果やグラフを使用する場合、試験条件が視認性をもって明瞭に表示されていないことや試験結果を示すグラフを極端にトリミングやスケール調整等をすることにより、一般消費者が過大な効果が得られると誤認する蓋然性があるときは、景品表示法等上問題となるおそれがある。

また、一般的な学術情報や統計資料等を引用して表示する場合には、当該資料等の内容が訴求する効能効果の範囲を逸脱したものであるときは、景品表示法等上問題となるおそれがある。

なお、表示の根拠として用いた論文の試験結果やグラフを表示する場合にあっては、引用するグラフが最終製品を用いた試験のデータであると誤認されないよう、当該グラフの選択理由及び最終製品を用いた試験結果ではないことなどを、視認性をもって明瞭に表示するよう留意する必要がある。

④ 医師や専門家等の推奨、行政機関等の認証等

医師や専門家、行政機関、研究機関などの認証や推奨等を表示することが直ちに景品表示法等上問題となるものではないが、虚偽の認証、推奨等や、当該推奨等の不適切な引用等をする場合は、景品表示法等上問題となるおそれがある[22]。

⑤ 利用者によるレビュー・体験談等の表示

PHR サービスの利用者によるレビューや体験談について、事業者が、作為的に選び出したもののみを掲載する場合や、事業者が一般の利用者を騙って架空のレビューを行う場合、都合のよい部分のみを抽出した場合などは、景品表示法等上問題となるおそれがある。

また、対価を支払って利用者に対して肯定的なレビューをするよう依頼した場合など、利用者の自主的な意思による表示と認められない表示については、事業者が行う表示であると評価される可能性

---

[22] なお、医療機器等の効能、効果又は性能について、医師その他の者がこれを保証したものと誤解されるおそれがある記事を広告し、記述し、又は流布することは禁止されている（薬機法 66 条 2 項）。

があり、この場合には、一般消費者が事業者の表示であることを判別することができるようにする必要があることに留意が必要である。

⑥ 打消し表示

事業者が、商品・役務について、断定的表現や目立つ表現等を使って、品質等の内容や価格等の取引条件を強調した表示（いわゆる強調表示）をする場合において、当該強調表示の適用に例外等があるときは、強調表示からは一般消費者が通常は予期できない事項であって、一般消費者が商品・役務を選択するに当たって重要な考慮要素となるものに関する表示(いわゆる打消し表示)を分かりやすく適切に行わなければ、その強調表示は、景品表示法等上問題となるおそれがある。

⑦ No.1 表示

商品・役務についての「No.1」、「第 1 位」、「トップ」などの表示（No.1 表示）が、合理的な根拠に基づかず、事実と異なる場合には、景品表示法上問題となる。

No.1 表示が不当表示とならないためには、①No.1 表示の内容が客観的な調査に基づいていること、及び、②調査結果を正確かつ適正に引用していることの両方を満たす必要がある[23]。

[23] なお、医療機器の品質、効能効果、安全性その他について、他社の製品を誹謗するような広告を行ってはならないものとされている（医薬品等適正広告基準（薬生発 0929 第 4 号平成 29 年 9 月 29 日）第 4、9)。

２．景品表示法における表示の科学的根拠に関する事項

（１）景品表示法７条２項及び８条３項の適用について

消費者庁長官は、事業者が行った表示が優良誤認表示に該当するか否かを判断するため必要があると認めるときは、当該表示をした事業者に対し、期間を定めて、当該表示の裏付けとなる合理的な根拠を示す資料の提出を求めることができる。当該事業者が当該資料を提出しないときは、消費者庁が当該表示について実際のものとは異なるものであること等の具体的な立証を行うまでもなく、措置命令又は課徴金納付命令との関係では、当該表示は優良誤認表示に該当する表示であるとみなされ、又は推定されることとなる(不実証広告規制。景品表示法７条２項、８条３項、33 条１項)。

（２）合理的な根拠の判断基準

①　総論

表示の裏付けとなる資料が「合理的な根拠」と認められるためには、(i)提出資料が客観的に実証された内容のものであること、(ii)表示された効果、性能と提出された資料によって実証された内容が適切に対応していること、の２つの要件を満たす必要があると解されている(不実証広告ガイドライン５頁)。当該(i)(ii)の具体的内容について、以下に概要を示すが、詳細については不実証広告ガイドラインを参照されたい。

②　提出資料が客観的に実証された内容のものであること

・総論

提出資料は、表示された具体的な効果、性能が事実であることを説明できるものでなければならず、そのためには、客観的に実証された内容のものである必要がある。客観的に実証された内容のものとは、①試験・調査によって得られた結果、②専門家、専門家団体若しくは専門機関の見解又は学術文献、のいずれかに該当するものである(不実証広告ガイドライン５頁)。

・試験・調査によって得られた結果（不実証広告ガイドライン６頁）

試験・調査によって得られた結果を表示の裏付けとなる根拠として提出する場合、当該試験・調査の方法は、表示された商品・役務の効果、性能に関連する学術界又は産業界において一般的に認められた方法又は関連分野の専門家多数が認める方法によって実施する必要がある。

・専門家、専門家団体若しくは専門機関の見解又は学術文献（不実証広告ガイドライン７頁）

専門家等の見解又は学術文献を表示の裏付けとなる根拠として提出する場合、次のいずれかを満たす必要があるものと考えられる。

(i) 専門家等が、専門的知見に基づいて当該商品・役務の表示された効果、性能について客観

的に評価した見解又は学術文献であって、当該専門分野において一般的に認められているもの

(ii) 専門家等が、当該商品・役務とは関わりなく、表示された効果、性能について客観的に評価した見解又は学術文献であって、当該専門分野において一般的に認められているもの

③ 表示された効果、性能と提出資料によって実証された内容が適切に対応していること

提出資料が表示の裏付けとなる合理的な根拠を示すものであると認められるためには、前記のように、提出資料が、それ自体として客観的に実証された内容のものであることに加え、表示された効果、性能が提出資料によって実証された内容と適切に対応していなければならない(不実証広告ガイドライン 7 頁)。

（３）科学的根拠として明らかに適切ではないと考えられる具体例

① 総論

科学的根拠として明らかに適切とは考えられない例としては、以下が考えられる。具体的なケースは②乃至④が考えられるが、これらはあくまで一例であり、不適切な例を限定する趣旨ではないことに留意する必要がある。

- 表示の内容が、科学的根拠の内容に比べて過大である、又は当該根拠との関係性が認められないもの
- 限定的な条件下での結果であり、条件を限定しない場合には表示で訴求する効能効果が期待し難いと考えられる結果であるにもかかわらず、表示の内容では当該条件に何ら言及していないもの
- 根拠となる文献が撤回され、表示の科学的根拠となる文献が存在しなくなったもの

② 最終製品を用いた臨床試験 (ヒトを対象にした試験)

・試験の実施計画又は実施方法に不備がある場合

対象群と比較した効能効果を表示したい場合、介入群に評価指標が高値又は低値の者が恣意的に割り振られているなど、介入群と対照群で適切な参加者の割り付けが行われていない場合

・試験結果の評価に不備がある場合

対象群と比較した効能効果を表示したい場合、主要な評価項目における介入群と対照群の群間比較で統計的な有意差が認められていない場合

③ 最終製品に関する研究レビュー

- 研究レビュー結果の客観性・透明性を担保するために必要な資料について客観性・透明性が担保されない場合

- 研究レビューで採用した論文(臨床試験(ヒト試験)の内容(試験デザイン、試験方法、対象者、結果の評価等))について不備がある場合
- 研究レビューにおける対象の機能と PHR サービス上の機能との同等性が担保されない場合
- 採用論文数、最終的に肯定的と判断できる要素等を総合的に判断し適切に評価がなされているとはいえない場合

④ 不適切な表示及び科学的根拠の例

表示例：このアプリに従って、1 日数分の運動をするだけで、1 週間で 1 キロ減量できます。

不適切な科学的根拠の例： 継続的な運動が減量に一定程度寄与することは自明であり、このこと自体には厳密な科学的根拠が求められるものではないものと考えられる。しかし、実際に減量できるかどうかは、食生活等も関係するところ、1 日数分という極めて短い運動のみをもって減量することができると断言できるかどうかは自明であるとはいえないことから、最終製品を用いた臨床試験や最終製品に関する研究レビューが存在しない場合は、十分な科学的根拠があるとはいえない。

VII. 本ガイドラインの有効期限、見直し

PHR サービス事業者におけるガイドラインに定められた事項の遵守状況や、関係法令、関係ガイドライン等の発出や改訂、個人情報保護と事業者が提供するサービスへの 消費者意識・要求度の変化や、PHR サービスの安全性、予防・健康上の効果についての再検証の必要性など、社会環境の変化等に応じて随時見直し、概ね 2 年間で見直しを行うものとする。

別添１：PHRサービスの安全管理のためのリスクマネジメントプロセス

リスクマネジメントプロセスにおいては、「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」に整理がされている。当該ガイドラインは、保健医療情報システムにおけるリスクマネジメントプロセスを中心に記載しているため、本別添でPHRサービスにおけるリスクマネジメントについての観点を追記として記載する。

【継続的なリスクマネジメントの実施】

PHRサービスにおいては、取扱い情報やシステムの構成、利用者規模などが随時変化し得ることから、継続的なリスクマネジメントが求められる。特に大規模な変更があった際などにはリスクアセスメントを再度行うことが望ましい。

【PHRサービスにおける個人情報】

PHRサービスにおいては、データ項目としては要配慮個人情報にあたる情報であっても特定の個人を容易に識別しえない情報として保管する場合があることをリスクマネジメントの際には考慮する（例：PHRサービス利用者が入力した病歴や健康診断結果の検査値を保管して可視化するが、個人を特定できる情報を保管しないPHRサービス等）。

【要配慮個人情報を取り扱う事業者のリスクマネジメント】

特に要配慮個人情報を取り扱うPHRサービス事業者においては、システム等の全体構成図を作成の上で情報流を特定し、リスクアセスメントとリスク対応を実施すべきである。要配慮個人情報を取り扱わない場合でも、取り扱う情報量や利用者数が多いなど社会的な影響が大きい場合には、リスクアセスメントの上でリスク対応を行うことが求められる。

【リスク特定】

リスク特定のプロセスにおいて、PHRサービスでは以下のような構成要素が考えられるので参考にされたい。

- PHRサービス利用端末（スマートフォン等）
- PHRシステム
- PHRシステムを運用するサーバー
- PHRサービス利用端末とPHRシステムを運用するサーバーとの通信経路
- 他のシステムと直接のデータ連携を行う場合のAPI、通信経路

なお、医療情報システムと直接の接続を行う際には、その接続インタフェース部分については、医療情報システムと同等の安全管理を行うこと。

別添２：PHR サービス自己チェックリスト

PHRサービス自己チェックリスト

「最低限順守する事項」にも「推奨される事項」にも○がついていない項目は、ガイドライン内で対応を求めるものではありませんが、PHRサービスの企画・設計・運用上留意すべき視点として参考までに記載しております

点検日：
点検者：

【一般的事項】

最低限遵守する事項	推奨される事項			チェック：はい（対応済）	いいえ（対応未）	わからない（不明）	該当しない
		1．取り扱いの情報					
		1-1.	個人の生活に紐付く医療・介護・健康等情報（ライフログを含む）を取り扱っていますか				
		1-2.	以下の情報を取扱っていますか（扱っている項目にチェックをお願いします。複数選択可）				
			a. 個人情報保護法で定義される個人情報				
			b. 個人情報保護法で定義される要配慮個人情報				
			c. 個人情報保護法で定義される匿名加工情報				
			d. 個人情報保護法で定義される仮名加工情報				
			e.「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」で定義される健診等情報				
			f.「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」で定義される医療情報				
		2．説明と同意					
		2-1.	個人の福祉・健康を主目的とすることを明示していますか				
○		2-2.	契約の目的、PHRサービスの目的・使用用途等について正しく理解できるような方法で情報提供した上で、同意を取得していますか				
○		2-3.	個人情報の利用目的をできる限り特定していますか。				
	○	2-4.	個人情報の利用目的について契約締結時に再度通知していますか				
	○	2-5.	契約締結時の説明を電磁的手段を用いて行う際には、PHR利用者が当該説明に関して質問することが難しい場合もあるので、問い合わせ先の掲載などの手段により意図的に質問の機会を設けるよう努めていますか				
	○	2-6.	個人情報の取扱に関する苦情の適切かつ迅速な解決に向けて必要な体制を整備したうえで臨んでいますか				
○		2-7.	要配慮個人情報を取得する場合や、データ連携等により個人情報を第三者に提供する場合に同意を取得していますか				
○		2-8.	PHRサービス利用者が未成年者、成年被後見人、被保佐人及び被補助人など判断できる能力を有していない人の場合は、親権者またその他の代理人等から同意を得られていますか				
○		2-9.	個人情報は個人情報保護法に基づいて適切な手段を用いて取得していますか				
○		2-10.	以下の項目を利用者の知り得る方法で公表していますか				
○			①個人情報取扱事業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				
○			②全ての保有個人データの利用目的				
○			③保有個人データの利用目的の通知の求め又は開示等の請求に応じる手続及び保有個人データの利用目的の通知の求め又は開示の請求に係る手数料の額（定めた場合に限る）				
○			④保有個人データの安全管理のために講じた措置				
○			⑤保有個人データの取扱いに関する苦情の申出先				
○			⑥認定個人情報保護団体の対象事業者である場合には、当該認定個人情報保護団体の名称及び苦情の解決の申出先				
	○	2-11.	PHRサービスの内容を幅広い利用者（疾患を抱えている方からそうでない方、こどもから高齢者、日本人から外国人、障害のある人まで）に応じて説明をしていますか				
	○	2-12.	PHRサービスの利用によって、健康に悪影響を及ぼす可能性について考慮し、サービス活用前にかかりつけ医等の医療者に相談することが望ましい旨を伝えていますか				
	○	2-13.	救急・災害時の治療や支援に有用な個人データに該当するPHRを取り扱うサービス事業者は、サービス開始時に、「救急・災害時に、迅速に有効な診断・治療を行う目的で本人のPHRを利用し、又は医療機関等の第三者に提供すること」について予め利用者の意思の確認をしていますか				
	○	2-14.	契約締結時、医療機関へPHRサービスを提供する場合は、関連するガイドラインに準拠して財務諸表やIR情報等に基づく経営の健全性に関する情報提供をしていますか				
		契約期間中					
○		2-15.	要配慮個人情報を取得する場合や、データ連携等により個人情報を第三者に提供する場合の同意状況について、利用者が確認できる方策を確保していますか				
○		2-16.	個人情報保護法に基づいて、利用目的の遵守、適切な利用ができていますか				
○		2-17.	利用目的が変更となった際にはその都度、同意を取得していますか				
		契約終了時					
○		2-18.	サービス終了時は利用者へのPHRのエクスポートおよび他のPHRサービスへ当該PHRのインポートが実施可能な期間を十分に確保できていますか				
○		2-19.	サービス終了時は契約内容に従って情報の破棄等を確実に行えますか				
○		2-20.	サービス終了時は手順に則って情報の返却・移管・破棄を適切に実施したことの証跡は取得できていますか				
		3．解約に関する権利					
○		3-1.	解約の権利を設ける場合にはその旨を明示していますか				
○			該当する場合、解約後のデータの処理について明示していますか				
		4．ユーザビリティ/アクセシビリティ（利用し易さ・便利さについて）					
		4-1.	PHRサービスの内容に応じたユーザビリティやアクセシビリティの確保について検討していますか（参照：JIS X8341シリーズ*）				
		5．本人確認					
○		5-1.	本人確認を実施していますか				
		5-2.	実施している場合、どの方法を用いていますか（扱っている方法にチェックをお願いします。複数選択可）				
	○		a. オンラインでの本人確認（eKYC：electronic KYC（Know Your Customer）の略で、KYCをオンライン上で実現するための仕組みを指す）				
	○		b. 対面または郵送による本人確認（KYC：Know Your Customerの略で、本人確認を行う手続きを指す）				
	○		c. 氏名、住所、生年月日、メールアドレス等の情報入力				
	○		d. その他				
	○	5-3.	PHRを本人以外の医療者や事業者が利用することを想定しているサービスにおいては、利用者本人のデータであることを保証するための仕組みはありますか				
○		5-4.	モバイル端末あるいはPHR機能において本人確認・認証を行える仕組みを設けていますか				
		6．第三者へのデータ提供					
○		6-1.	個人情報の第三者提供に当たって、個人情報保護法、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基づいて、確認・記録をしていますか				
○		6-2.	医療機関に該当するPHRサービス事業者は個人情報保護法、各種ガイドラインに加え、医療・介護関係事業者における個人情報の適切な取り扱いのためのガイダンスを参照していますか				
○		6-3.	第三者提供停止請求を受け、その請求に理由があることが判明した時は、遅滞なく当該第三者提供を停止していますか				
	○	6-4.	匿名加工情報を第三者提供する場合、提供内容の説明や提供先などの取扱いを事業者のWebサイトやパンフレットで公開してますか				
	○	6-5.	改正次世代医療基盤法等の法令によって定められた方法に従って第三者提供を行えてますか				

*JISX8341-3:2016 達成基準 早見表（レベルA&AA） https://waic.jp/files/cheatsheet/waic_jis-x-8341-3_cheatsheet_201812.pdf

【有効性に関する事項】

最低限遵守する事項	推奨される事項			はい（対応済）	いいえ（対応未）	わからない（不明）	該当しない
		7．リコメンドサービス					
		7-1.	法令順守、リコメンドサービスに対するリスクアセスメントの実施及び開示				
○		7-1-1.	リコメンドサービスが医行為に該当しないか、医師法17条に抵触していないかを少なくとも社内で確認していますか				
○		7-1-2.	リコメンドサービスに使用するアプリケーションが医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律（薬機法）上のプログラム医療機器に該当するかを少なくとも社内で確認していますか				
○		7-1-3.	リコメンドサービスに使用するアプリケーションがプログラム医療機器に該当する場合、医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律（薬機法）に基づく承認等を得ていますか				
○		7-1-4.	リコメンドサービスに関する表示については、不当景品類及び不当表示防止法、薬機法等の各種法令に遵守していますか				
	○	7-1-5.	リコメンド機能の提供に際して、関連学会等によるエビデンスがあるものを提供していますか				
	○	7-1-6.	リコメンド機能の提供に際して、医療者等の監修を受けるなどして、有効性・安全性の確保に努めていますか				
	○	7-1-7.	リコメンド機能の提供に際して、エビデンスが十分でない場合には、データを蓄積し、有効性・安全性の検証に努めていますか				
		7-1-8.	疾病の診断・治療に関わるPHRサービスを提供していますか				
			該当する場合、医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律（薬機法）の規定を遵守していますか				
		7-1-9.	同サービスに対するリスクアセスメントの方法を開示していますか				
		7-2.	リコメンドサービスに対するリスクマネジメントシステムの確立				
	○	7-2-1.	リコメンドサービスに対するリスクマネジメントシステム（PDCAサイクルの設定や体制）を確立していますか				
	○	7-2-2.	リコメンドサービスのための組織体制や責任等に言及した情報を開示していますか				
	○	7-2-3.	リコメンドサービスのプロセスやリソース、指導内容の根拠を提示できていますか				
	○	7-2-4.	リコメンドサービスに対する定期的レビューをしていますか				
		8．管理・閲覧サービス					
		8-1.	管理・閲覧サービスに対するリスクアセスメントの実施及び開示				
	○	8-1-1.	管理・閲覧サービスに対するリスクアセスメントを実施し、求めに応じ開示できる体制を確保していますか				
		8-2.	管理・閲覧サービスに対するリスクマネジメントシステムの確立				
	○	8-2-1.	管理・閲覧サービスに対するリスクマネジメントシステム（PDCAサイクルの設定や体制）を確立していますか				
	○	8-2-2.	管理・閲覧サービスのための組織体制や責任等に言及した情報を開示していますか				
	○	8-2-3.	管理・閲覧サービスに対する定期的レビューをしていますか。また、そのレビュー期間は、第3者認証を取得し、その基準に従っていますか				
	○	8-2-4.	PHRの管理に当たり、データの入力者、データの測定者、データを測定したデバイス、データを測定した環境、外部から取得した場合はデータの由来（マイナポータル等）、同意取得の範囲、データの削除や修正が行われたことが分かる情報（データベース上でフラグを立てる等を含む）などをメタ情報として記録していますか				
		8-3.	管理・閲覧サービスに対する利用者側の利便性				
○		8-3-1.	利用者が自身のPHRを自由に閲覧できるようになっていますか				
○		8-3-2.	利用者の求めに応じてPHRを削除できるようになっていますか				
○		8-3-3.	健診等情報を取り扱う場合は、業界で合意された一般的な規格に従った形でのインポート及びPHRサービス内のデータのエクスポートができるようになっていますか				
	○	8-3-4.	PHRの追加・削除・修正・他サービスへの移動を利用者自身が管理できる機能はありますか				
	○	8-3-5.	健診等情報以外の情報についても、本人の求めに応じてデータをエクスポートできるようになっていますか				
	○	8-3-6.	代理人等がデータの管理・活用を行える機能及び、利用者本人へ管理機能を移譲する機能はありますか				

【安全性（機密性）に関する事項】

最低限遵守する事項	推奨される事項	9. 個人情報の保護・情報セキュリティ	はい（対応済）	いいえ（対応未）	わからない（不明）	該当しない
		9-1. 情報セキュリティ対策				
○		9-1-1. 情報セキュリティに係る第三者認証（プライバシーマーク認証、ISMS認証、セキュリティ管理に係る内部統制保証報告書等）を取得していますか				
		9-1-2. 取り扱う情報の要求レベルに応じて、「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」の「２．情報セキュリティ対策＞２.１.安全管理措置＞（２）本指針に基づく遵守すべき事項」に定義される各項目について対応していますか				
	○	9-1-3. 情報セキュリティポリシーを策定していますか				
	○	9-1-4. 策定した情報セキュリティポリシーを公開していますか				
		9-2. 脆弱性診断等システムにおける安全性				
	○	9-2-1. バリデーションプロセス（顧客、監査など）の経験がありますか				
		9-3. 個人情報の正確性の担保				
	○	9-3-1. 個人データは利用目的の達成に必要な範囲内において、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際は遅滞なく削除し、復元不可能な手段で削除できていますか				
	○	9-3-2. 復元不可能な削除方式については、総務省「地方公共団体における情報セキュリティポリシーに関するガイドライン」等を参照していますか				
	○	9-3-3. 消去データから個人を特定できないようになっていますか				
		9-4. 個人情報に係る規定の整備				
	○	9-4-1. サービス事業者は安全管理に係る基本方針として以下の事項を運用管理規定に含めていますか				
	○	・本ガイドライン、提供事業者指針および医療情報安全管理指針の順守				
	○	・個人情報保護法やその他最新の関連法令等の順守				
	○	・個人情報に関して他の情報と区別した適切な管理				
	○	・情報セキュリティポリシーの順守を担保する組織体制の構築				
		9-5. 委託契約の締結				
	○	9-5-1. 委託契約には、委託先における委託された個人データの取扱状況を委託元が合理的に把握することが盛り込まれていますか				
		9-6. 定期的な情報セキュリティの見直し				
	○	9-6-1. 定期的に情報セキュリティ対策を見直して改善できていますか				
		9-7. データガバナンス体制				
	○	9-7-1. データガバナンス体制を確立していますか（例：PIA（個人情報保護評価又はプライバシー影響評価）の手法を用い、データの内容や性質、量や範囲の必要十分性、データの流れ、データの取扱いに関わる者の範囲、データの利用目的、安全管理レベル等の事前評価を実施するなど）				
		10. 運用体制や責任者				
		10-1. 情報管理責任者とカスタマーサポート				
	○	10-1-1. 情報管理責任者を置き、サービス利用者に明示していますか				
	○	10-1-2. PHRサービスについての文書化された取扱説明書、取扱い手順、またはそれに類するものはありますか				
	○	ある場合、その文書をサービス利用者に開示していますか				
	○	10-1-3. アプリケーションプライバシーポリシーを明示していますか				
	○	10-1-4. PHRサービス停止時の事前告知、サービス終了時の告知方法を明示し、かつ他社サービスへの引継ぎ方法などを開示していますか				
		10-2. 運用体制				
	○	10-2-1. 適切に開発、管理及びサポートを実施する専門分野に対する経験及び資格または能力がある十分なスタッフを明示していますか				
	○	10-2-2. インシデントが発生した際のユーザーへの報告方法が明確になっていますか				
	○	10-2-3. PSIRT体制を構築していますか				
	○	10-2-4. 特商法対応（提供者の明示）を行っていますか				
		10-3. クラウド事業者の選定				
		10-3-1. 取り扱う情報の要求レベルに応じて、十分な情報セキュリティ対策を行っているクラウド事業者やサービスを選定していますか				

【信頼性に関する事項】

最低限遵守する事項	推奨される事項	11. サービスにおける信頼性	はい（対応済）	いいえ（対応未）	わからない（不明）	該当しない
	○	11-1. 当該PHRサービスの運用やカスタマーサポートの体制を開示していますか				
	○	11-2. 当該PHRサービスの健康情報管理における実績を何らかの形で開示していますか（例：国内外の学会論文・第三者機関が認定する実績データ）				
		11-3. 運用ポリシーを公開していますか				
		11-4. 当該PHRサービスは、第三者へのデータ提供を行っていますか				
		11-5. 当該PHRサービスは、利用者によるデータポータビリティを確保していますか				
		12. PHRサービスに対する質評価				
	○	12-1. 自社サービスの品質をチェックするために、本チェックリストを活用していますか				
	○	12-2. 実施したチェック結果を自社のHP等で公開していますか				
		13. 運用や体制の開示				
		13-1. 医師法、薬機法を含む各種法令、ガイドライン、通達等の遵守及び開示				
		13-1-1. 当該事業者のPHRサービスに関わる個人情報保護法、医師法、薬機法を含む各種法令、これらの法令等に関するガイドライン、通達等の内容を理解し、遵守していますか				
		13-2. 不具合発生時の体制及び対応方法の開示				
		13-2-1. 当該PHRサービスの不具合発生時の体制及び対応方法を提示していますか				