健康情報を活用した個人・社会の健康づくりに向けた
民間事業者のPHRサービスに関わるガイドライン策定

民間事業者のPHRサービスに関わるガイドライン

（第2版）

一般社団法人PHR普及推進協議会
（令和4年9月改定）

目次

はじめに

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

（２） 民間PHRサービスガイドラインの目的

（３） PHRサービスとは

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

（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

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

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

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

（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

（３） 周辺データを活用した健康増進、医療の質向上

（４） PHRサービス利用者の健康、安全、権利の確保

（５） 利用者への説明と同意に基づくサービス提供

（６） PHRサービスの質の担保と向上

（７） PHRサービス事業者間での連携

（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

（９） 継続的な改訂が可能な体制の構築

（１０）国際的な動向を踏まえたPHRサービス提供にかかるルールの整備

V. 民間PHRサービスガイドラインの具体的適用

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）

（２） 本人確認

（３） PHRデータの管理・閲覧

（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

（５） リコメンドの方法（有効性・安全性の確保）

（６） 他の事業者・第三者へのデータ提供

２．PHRサービスの提供体制に関する事項

（１） PHRサービス事業者間の連携（相互運用性）

（２） 医療機関との連携

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

（２） PHRサービス事業者への教育

（３） PHRサービスと体制の質評価／フィードバック／認証

（４） エビデンスの蓄積

今後の検討の進め方

別添資料

＜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

＜別添２＞民間PHRサービスリファレンスアーキテクチャ

＜別添３＞PHRサービス自己チェックリスト

はじめに

一般社団法人PHR普及推進協議会は、パーソナルヘルスレコード（PHR）の適正な普及推進のため、情報交換・情報発信を行い、社会の健康、安全のより一層の向上に寄与することを目的として、PHRの普及やPHRデータの流通促進に関する課題、利用事例、効果等の調査・研究事業を行っています。

社会の超高齢化、生活習慣病の増大に伴いセルフケアの重要性が増す中で、ICTの普及が進み、個人の健康に関わるデータを電子記録として本人や家族が日常的に記録し、活用することが出来るPHRの利活用に期待が集まっています。PHRは個人の生涯の健康、幸福に役立つ重要なツールとなる可能性を秘めています。さらに、PHRの活用により、医学の発展や新産業の創生にも寄与し、民間企業におけるPHRを活用したサービス提供やイノベーションが加速されることが予測されています。しかし、民間事業者がPHRサービスを取扱う際に踏まえるべきモラルやルールが整理されておらず、PHRサービスの適正な普及推進における課題となっています。

PHRサービスの活用を広げるためには、PHRサービスが個人や社会の健康づくりに役立つものであり、安心して活用できるものであると広く認識していただく必要があります。そのためには、まず、PHRサービスのもととなる個人の健康に関わるデータはその人個人に由来し、本人が権利を有するという基本的な考え方を共有することが大切です。このたび、経済産業省の補助事業である「令和2年度ヘルスケアサービス品質評価構築支援事業（業界自主ガイドライン等策定支援）」の採択をうけ、『民間事業者のPHRサービスに関わるガイドライン作成に当たっての提言』を作成することといたしました。令和3年度から4年度にかけては、PHR普及において喫緊の課題である「PHR項目・流通規格の標準化」および「PHRサービスの質の確保のための方策」について検討を行い、その内容を改訂版に盛り込むとともに、急速にPHRサービスの実装が進む状況を踏まえ、ガイドラインとして提示をすることといたしました。本ガイドラインは、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整理し、提示しています。

我々は、民間事業者による多種多様なPHRサービスの提供が、「個人の意思を尊重した健康づくり」や「人と人とのつながり強化」、ひいては「住みやすい国づくり」に寄与すると確信しています。そのためには、PHRサービスに関わる「産（企業利益、CSR）」「官（町づくり、地方創生）」「学（研究の推進）」「民（市民の健康増進）」が一体となり、各々に役立つ社会基盤を育てていくことが求められます。

本ガイドラインが、国民・患者・家族の健康増進・管理、病気の予防、社会の健康に繋げるための良質なPHRサービスの創造・普及を可能とする社会基盤育成の一助になれば幸いです。

令和 4 年9月吉日

一般社団法人PHR普及推進協議会　代表理事　石見　拓

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、民間PHRサービス事業者（以降、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）が整理されていないことが課題となっている。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サービス事業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、PHR業界の発展に繋げることである。

（3）PHR サービスとは

PHR サービスとは、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、国民・患者が自ら利用する ICT を活用したサービスで、リコメンド機能、管理・閲覧機能、第三者提供機能のいずれかを含むものを指す。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。

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、自治体、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 2019～「令和」新時代：「Society 5.0」への挑戦～（令和元年 6 月 21 日閣議決定)』において、生涯にわたる健診・検診情報の予防等への分析・活用を進めるため、マイナポータルを活用する PHR との関係も含め、健診・検診情報を 2022 年度を目途に標準化・電子化し蓄積する方策が掲げられた。また『経済財政運営と改革の基本方針 2020～危機の克服、そして新しい未来へ～（令和 2 年 7 月 17 日閣議決定)』においても、PHR の拡充を図るため、2022 年を目途に、マイナンバーカードを活用して、生まれてから生涯にわたる健康データを提供できるよう取り組むとともに、当該データの医療・介護研究等への活用の在り方について検討する方針が示された。『経済財政運営と改革の基本方針 2021 日本の未来を拓く 4 つの原動力～グリーン、デジタル、活力ある地方創り、少子化対策～（令和 3 年 6 月 18 日閣議決定)』においても、医療・特定健診等の情報を民間ＰＨＲサービスの利活用も含めて自身で閲覧・活用できる仕組みについて、2022 年度までに、集中的な取組を進めることや、画像・ 検査情報、介護情報を含めた自身の保健医療情報を閲覧できる仕組みの整備を、データヘルス改革に関する工程表に則り、着実に推進する方針が示された。あわせて、感染症、災害、救急等の対応に万全を期すためにも、医療・介護分野におけるデータ利活用やオンライン化を加速し、PHR の拡充も含めたデータヘルス改革を推進することが掲げられている。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[i]」が策定されているが、PHR に関する明確な指針はこれまで示されていなかった。その中で、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ている。2020 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」として再組成された。

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」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令和 4 年 4 月 1 日一部改正され、総務省・厚生労働省・経済産業省の 3 省か

[i] 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 」
・経済産業省・総務省「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」

ら公表されている。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（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、国が定める「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」（以後、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利活用にかかる「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）」について検討が進んでいる。国が定める個人が自らの健康管理に利用可能な健診等情報には、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、予防接種歴、乳幼児健診、特定健診、各種健診、レセプト記載の薬剤情報等が含まれる。一方で、日常的に記録されるいわゆるライフログは現時点では検討の対象となっていない。また、国民自身の利用が想定されない研究開発の推進等を目的として利用される健診等情報及び匿名加工された健診等情報は検討の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＞

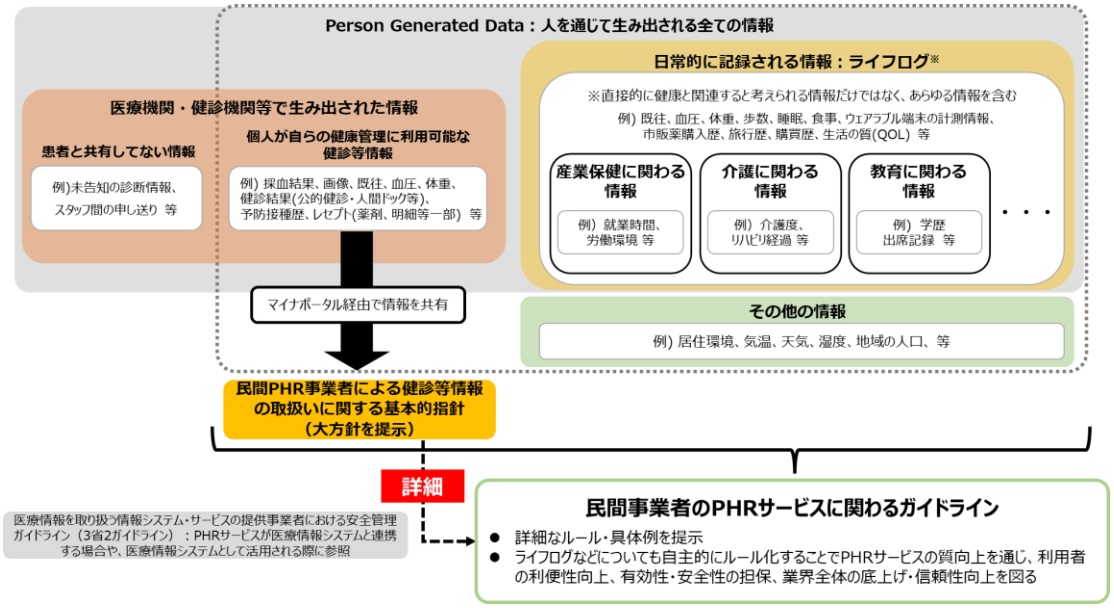
本ガイドラインの対象は、全てのPHRサービス（医療情報システム[ii]として提供されるものを除く）を提供する事業者を想定しており、ライフログのみを取り扱うPHRサービス等、国の検討対象外のサービスも含む。「健診等情報」を取り扱うPHR事業者は、国のPHR指針の参照が求められるが、本ガイドラインを遵守することで更なるPHRサービスの質向上が望まれる。本ガイドライン策定の目的は、PHRサービスの有効性と安全性の向上を図り、個人と社会の健康増進に寄与するとともにPHR業界の発展に繋げることであり、ここに記載された内容をクリアすることにとどまらず、提供するPHRサービスの質向上に繋げていただくことを期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

[ii] 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。

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[iii]」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】

[iii] 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（具体例：予防接種歴、乳幼児健診、特定健診、各種健診、レセプト記載の薬剤情報等）

（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）
- 医療法（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1年12月4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3年1月5日）
- 健康増進法（平成14年8月2日. 最終改正令和3年5月19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3年5月19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4年4月20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1年5月31日）
- 保健師助産師看護師法（昭和23年7月30日. 最終改正平成30年6月27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に関する法律（平成29年5月12日. 最終改正令和3年5月19日）

＜公的指針・ガイドライン等＞

- 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）
- 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）
- 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3年1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3年10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3年1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. 平成29年3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4年4月1日更新）
- 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4年3月一部改正）
- 個人データの漏えい等の事案が発生した場合等の対応について（平成29年個人情報保護委員会告示第１号）
- 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）
- 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4年1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2版）（総務省）（平成30年7月）
- 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）（平成4年3月31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）
- 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）
- 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）（令和2年8月）
- 医療情報システムの安全管理に関するガイドライン 第5.1版（厚生労働省）（令和4年3月）
- 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4年4月一部改正）
- 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）」

＜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1.0版（内閣府大臣官房番号制度担当室）（令和2年7月27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
民間 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、国民・患者が自ら利用する ICT を活用したサービスで、リコメンド機能、管理・閲覧機能、第三者提供機能のいずれかを含むもの。管理・閲覧機能には、ウェアラブル端末等を通じて日常的に記録される情報（ライフログ）等の健康に関連する情報の収集を含む。
民間 PHR サービス事業者	PHR サービスを提供する民間事業者（医療機関含む）（別添 2 参照）
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、下記のとおりである 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 データ	PHR サービスで活用される様々なデータ。健診結果や遺伝情報等、医療や健康増進に直接関係すると考えられるデータにとどまらず、行動歴や職業、購買歴、さらには気温や天気といった健康に関連し得るデータを含む。なお、上述のようなデータがすなわち PHR データであるというわけではなく、当該データが PHR サービスで医療や健康増進に関係するデータと関連付けて活用される際に、PHR データとしての意味を持つことを留意されたい。

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（EHR）	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また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 データの伝達また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等のほか、(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PGD（Person-Generated Data）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、病気の有無に関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データ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データ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データを蓄積・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」の確保が求められる。PHRデータ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データや提供される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データには、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

データ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、高齢者や障害を持つ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およ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利用者に対して、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すべきである。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データを管理・活用できるようなサービスを提供する際には、その親権者や法定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、責任能力が認められた後には、PHRデータ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、明示的な同意を取得しておくことが望ましい。

（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には、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、デバイスの差異や不具合、なら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サービスを同時また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持し、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サービス事業者ならびに社会に対して、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サービスにかか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サービス提供にかかるルールの整備

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、本邦におけるPHRサービス事業を発展させるために、国際的な標準化や相互運用性の確保を意識したPHRサービス提供にかか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データの一部は個人情報（個人情報保護法2条1項）、要配慮個人情報（同3項）や個人データ（同法16条3項）に該当し得るものであり、PHRデータを含む個人情報データベース[iv]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。

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。

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

[iv]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

（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）[v]。特に、要配慮個人情報については、基本的にオプトアウト[vi]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うえ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する必要がある。

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

[v] 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)参照。

[vi] 「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。

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子どもについて、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）。

また、PHRデータ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：法第23条第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、35ページを参照のこと

【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）[vii]。「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

[vii] 「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）。

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データの返却等

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データのエクスポート及び他のPHRサービス事業者への当該PHRデータ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データが利用者の重要な資産であることに留意し、利用者がPHRデータ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サービス事業者間の連携（相互運用性）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も必要である。

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。
- 要配慮個人情報に該当するPHRデータ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データ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・災害時に本人に適切な治療や支援を行えるよう、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データを取り扱うPHRサービス事業者は、PHRサービス開始時に、「救急・災害時に、迅速に有効な診断・治療を行えるように本人のPHRデータを利用し、又は第三者に提供すること」について、あらかじめ同意の取得を試みることが望ましい。この際は想定されるデータの提供先を特定しておくことが望ましい。
- 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）。
- 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が望ましい。

（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利用者が利用するサービスについて、PHRデータを本人あるいは代理人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データ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データが確かにPHR利用者本人のデータであることを保証する（真正性）の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きを指す）、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[viii]）、マイナンバーカード認証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

[viii] 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。

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データ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データが確かにPHR利用者本人のPHRデータ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データのリスクに応じた方法（eKYC（electronic Know Your Customer）の利用、対面または郵送、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データの管理・閲覧

考え方

PHRデータ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データ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データ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データを代理の者が管理・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データは、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データの発生源や取得方法、PHRデータの移動・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ことで、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、血圧計などその他の様々な計測機器と連携して使用されることが考えられる。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データを自由に閲覧できること。
- 利用者の求めに応じてPHRデータを削除できること。
- 健診等情報を取り扱う場合は、そのエクスポートができること。

推奨される事項

- PHRデータの追加・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。
- 医療機関、健康診断由来など本人が計測・入力したものではないPHRデータについては個別の項目の削除や修正は認めず、一括削除のみとする形が望ましい。
- PHRデータの管理・閲覧サービスの提供に当たっては、関連する学会等が推奨する項目、データ交換形式、基準値を活用することが望ましい（53ページ参照）。
- 救急災害時および生活習慣改善に関わる項目を取り扱う場合は、当ガイドラインが推奨するデータ交換形式（予定）でのエクスポートができることが望ましい（49ページ。相互運用性の項参照）。
- 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。（２．（１）相互運用性の項を参照）
- 各PHRデータにおいて、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、をメタ情報として記録することが望ましい。
- 代理人がPHR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の実施及び開示することが望ましい。
- 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。
- 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[ix]は、その取り扱うPHRデータの漏えい[x]、滅失[xi]又は毀損[xii]（以下「漏えい等」という。）の防止その他のPHRデータの安全管理のために必要かつ適切な措置を講じなければならない（個人情報保護法23条）。当該措置は、PHRデータが漏えい等をした場合に本人が被る権利利益の侵害の大きさを考慮し、事業の規模及び性質、PHRデータの取扱状況（取り扱うPHRデータの性質及び量を含む）、PHRデータを記録した媒体の性質等に起因するリスクに応じて、必要かつ適切な内容としなければならない（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

[ix] 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 データの管理等のみを行う場合などが考えられる。

[x] 個人データが外部に流出することをいう（通則 GL3-5-1-1）。

[xi] 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）。

[xii] 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）。

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関わらず、PHRデータ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。

以下に情報の分類の一例を示す。定義は用語集を参照されたい。

PHR検討会での定義	情報種別	具体例	求められるセキュリティ
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、レセプト情報、薬歴	高 ↑
ライフログ	要配慮個人情報	人種、思想や信仰に関わる情報	
	比較的リスクの高い情報	アレルギー歴、詳細な位置情報	
	比較的リスクの低い情報	歩数、活動量、体重、体脂肪率、家庭血圧、食事日誌、睡眠日誌、介護記録	
	環境・生活情報	居住環境、気温、天気	
			↓ 低

【図2：情報セキュリティ対策における情報の分類の一例】

※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、他項で記載のとお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利用者に転嫁されたり、PHR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
   「個人データの漏えい等の事案が発生した場合等の対応について(平成29年個人情報保護委員会告示第1号)」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利用者等に被害が生じると、PHR利用者等はPHRサービス事業者に対し、契約責任また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利用者に対する影響を速やかにPHR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公的な第三者認証として、プライバシーマーク認定または 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[xiii]（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）を利用者に示すことが望ましい。

[xiii] 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。

【仮名加工情報及び匿名加工情報の作成及び利用】

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サービス事業者が仮名加工情報や匿名加工医療情報を作成した上で、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場合も考え得る（なお、仮名加工情報については、第三者提供が基本的に禁止されている（個人情報保護法42条1項））。また、PHRサービス事業者が仮名加工情報、匿名加工情報や匿名加工医療情報を作成した上で利用する場合も考えられる。この際には、個人情報保護法及び同法に関する規制（次世代医療基盤法等）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。また、そのような仮名加工情報、匿名加工情報や匿名加工医療情報を受領するなどした仮名加工情報取扱事業者、匿名加工情報取扱事業者や匿名加工医療情報取扱事業者に該当するPHRサービス事業者についても、これら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データを正確かつ最新の内容に保つとともに、利用する必要がなくなったときは、当該PHRデータ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。

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データ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

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、医師や看護師等以外の者が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）。

医師や看護師等以外の者でも、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PHR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。）。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して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）。

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データを蓄積・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、提供する内容のエビデンスを提示したり、医学的な監修を得たりするなどにより、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、エビデンス蓄積しながらサービスを提供していくことが望ましい。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。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データ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データ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

- 医師や看護師等以外のものは、医行為や診療の補助に該当するPHRサービスを提供してはならない（医行為や診療の補助の具体例は、38ページを参照のこと）。
- 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データ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）、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、および、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＞

- 病気や障害を有する者に対して、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。
- 病気や障害を有する者に対して、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、有効性・安全性の確保に努めることが重要であり、エビデンスに基づいた適切なリコメンドが提供されるべきである。また、「医療者等の監修を受ける」「根拠のある文献を参照にする」などが求められるが、有効性・安全性のエビデンスがない場合には、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。

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、保険適応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応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、予め、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、予め書面で「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、養育者によって子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。

また、以下の場合には、そもそも「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指針（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データの提供

医療機関に該当するPHRサービス事業者が、第三者提供を含めた個人情報の取扱いをする際には、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Ver2.2を参照のこと

推奨される事項

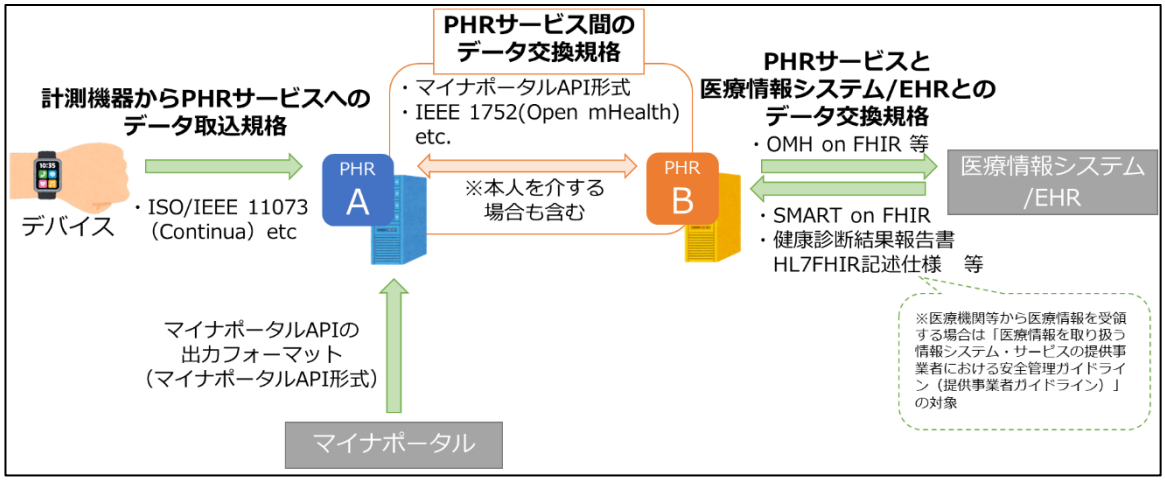
匿名加工情報を第三者提供する場合、提供内容を説明しておくこと、提供先など取扱いを適宜、事業者のWebサイトやパンフレット等で公開すること。

2．PHRサービスの提供体制に関する事項

（1）PHRサービス事業者間の連携（相互運用性）

考え方

PHRデータは、前章「（6）リコメンドの方法（有効性・安全性の確保）」等で示してきたように様々なサービスで利用される。このような多様な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PHRサービスは生涯に渡り継続的に利用されるが、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。よって、利用者がPHRを有効かつ継続的に活用するために、データの持ち主本人が自身のデータを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。データポータビリティの確保には、PHRサービス及び関連事業者間におけるPHRデータの相互運用性が重要となる。PHRデータの相互運用性を考慮する際に重要な、PHRサービスに関連するデータ交換規格は、主に対象とする領域によって下図のように区分できる。ウェアラブルデバイス等の計測機器とPHRサービス間のデータ交換規格、民間事業者によるPHRサービスと医療情報システム（EHR）間のデータ交換規格については、それぞれ検討が進められているため（図3）、本ガイドラインにおいてはPHRサービス間でのデータ交換規格に焦点を絞ることとした。



【図3：PHRサービスに関連するデータ交換規格の整理】

一般に、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相互運用性を担保す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り得るため、すべてのデー

タについてPHRサービス間の連携を確保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。よって、利用者が複数サービスでのデータ活用や、サービス終了時に他事業者にてPHRデータを継続利用できるよう、利用者が使用中のPHRサービスから個人が活用すべきデータを出力可能とする権利を保障することがPHRサービスに求められる要件であると考えられる。

一方で、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には、サービス利用者にとって特に価値が高いと考えられる項目については、幅広い相互運用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データを出力できるデータポータビリティを提供することが望ましい。そのためには、具体的な項目とそのデータ交換規格が共有される必要がある。PHR普及推進協議会では、今後、これらを「PHRデータ標準交換規格」として推奨する方針とした。PHRデータ標準交換規格の選定、作成に当たっては、学会等が各々の専門領域における重要項目を提示している場合は、これらの項目に対してデータ交換規格を定めることとした。本ガイドラインでは、まず一定の相互運用性の確保を促しPHRサービスの底上げを図るために、PHRが最も効果を発揮すると期待される生活習慣改善及び救急災害時の利用という観点から、関係学会等と項目の選定について議論を進めてきた。その結果として、臨床6学会合同で策定された「生活習慣病自己管理項目セット集」[xiv]及び、R4年度「厚生労働科学研究費補助金（地域医療基盤開発推進研究事業）救急医療等における基盤整備のための情報項目等の標準化に資する研究」にて検討が進められている「救急医療および災害医療における必要な情報項目（仮）」[xv]について、PHRデータ標準交換規格を提示していく方針とした。

PHRデータ標準交換規格の提示に当たっては、国際的な状況も踏まえて既に普及している、あるいは普及が見込まれる既存のデータ交換規格をできるだけ活用する方向で検討しており、マイナポータルAPIのデータフォーマット、IEEE1752（Open mHealth）、JAHIS電子版お薬手帳データフォーマット等が現在その候補となっている。本項の最後に、現在のデータ交換規格案の概要を示す。

なお、紹介した項目以外においても、今後各専門領域の学会等の協力を得てPHRデータ標準交換規格を策定していく予定である。

また、将来的にはPHRサービス間だけでなく、デバイスとPHRサービス間及びPHRサービスと医療情報システム間のデータ交換規格についても、整理・統合されていくことが望

[xiv] “代表的な生活習慣病である 4 疾患（糖尿病、高血圧、脂質異常症、慢性腎臓病（CKD））についての各診療ガイドラインを主として策定している 4 学会（日本糖尿病学会、日本高血圧学会、日本動脈硬化学会、日本腎臓学会）、および検体検査の測定法やデータの標準化に関連する日本臨床検査医学会、医療情報全体の標準化や活用を推進する日本医療情報学会の計 6 学会によって、どのような目的のデータベース項目構築の際でも採用するべき「生活習慣病ミニマム項目セット集」、およびそのユースケースとしての「生活習慣病自己管理項目セット集」の策定が行われ、第 1 版が 2014 年に公開された”（「生活習慣病ミニマム項目セット」の改訂の目的 https://www.jami.jp/medicalFields/2018Oct23_01.pdf より抜粋）。改訂版は 2018 年 10 月に公開され、各項目の基準値を提示した PHR 推奨設定も存在する。2022 年 9 月時点での最新版は https://www.jami.jp/medicalFields/2018Oct23.php よりダウンロード可能。

[xv] 令和 4 年度厚生労働科学研究費補助金（地域医療基盤開発推進研究事業）「救急医療等における基盤整備のための情報項目等の標準化に資する研究」として策定が進められている項目集であり、救急医療および災害医療における必要な項目について、救急医学会を始めとした学会の協力を得ながらまとめられている。令和 4 年度中に完成予定。

ましい。

データをPHRサービス間で移行する際には、個人を経由することによってデータの変更がなされてしまう可能性を鑑み、データの由来や真正性、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や、エクスポート時もメタデータと合わせて出力したり、利用者の同意のもとに事業者間で直接受け渡したりできる連携手法などの対応が望ましい。

他項でも触れられている通り、PHRデータには、病歴・健診結果・信条等の要配慮個人情報が含まれる場合がある。そのため、個人データの提供を伴う相互運用を行う際にも、利用者から適切に同意を取得する必要がある。加えて、情報漏洩の防止策を含め、利用者が安心・安全に使用できる環境を整備しなければ利活用が進まないと考えられる。PHRサービス事業者は、利用者自らが相互運用させるPHRデータの範囲・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配慮すべきである。

PHRサービス事業者が相互運用先を決める際には、ISMSやプライバシーマークの取得等、一定レベルのセキュリティ水準を持つ企業を選定することが望ましい。少なくとも、相互運用先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。相互運用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が望ましい。

利用者が適切なPHRサービスを選択できるよう、相互運用性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が望ましい。

PHRサービスには、本人認証・セキュリティ・外部計測機器とのインタフェース・課金・その他、いくつかの共通する機能がある。近い将来、これらの共通機能をまとめ、PHRサービスのハブとなる情報基盤を提供する事業者が出現するかもしれない。そのような共通基盤を提供する事業者は、PHRデータの流通を促進するために、基盤上のPHRサービス事業者や基盤提供事業者間で相互運用性が確保できる標準仕様を作成すべきである。相互運用のための標準仕様策定に当たっては、対象となる項目を医学的見地から検討し、対応するPHRサービス事業者の負担とPHR利用者の利便性のバランスが取れるものにすることが求められる。また、既存の規格を使うことで導入コスト・維持コストを抑えることも重要であり、データ交換規格については、国際規格を見据えた仕様が求められる。なお、ある事業者から別の事業者にPHRデータが移動した場合において、ある事業者に引き続きデータが残っている可能性がある。PHR利用者が双方の事業者からデータを削除したい場合には、各々の事業者に対してPHR利用者が削除の指示をしなければならない可能性があることに留意する旨もPHR利用者に対して提示すべきである。

最低限遵守する事項

- PHR利用者が、健診等情報を国のPHR指針が定めるデータフォーマットで利用者本人が必要な時にエクスポートできること。

・　第三者への個人データの提供・移動や預託を行う場合は、利用者から適切に同意を取得すること。

推奨される事項

・　PHRサービス間のポータビリティを確保するために、本ガイドラインが推奨するPHRデータ標準交換規格[xvi]によるデータのエクスポート・インポート機能を備えること（PHRデータ標準交換規格にない項目についても、厚生労働省標準規格[xvii]に定められた項目については、これに対応する規格によるエクスポート・インポート機能を備えることが望ましい。）
・　PHRサービス事業者同士がデータ項目の整理やデータのフォーマット等の国際的な動向も踏まえた標準化、API連携、ブロックチェーン利用等の必要な環境整備を図ること。個別にサービス間での相互運用のための各種整備をすることは効率的ではないため、将来的にはプラットフォーマーがこれを代行し、相互運用性を高めることも考慮される。
・　データをPHRサービス間で移行する際には、データの由来や真正性、同意取得の範囲に関わる情報を保持し、エクスポート時に出力したり、利用者の同意のもとに事業者間で受け渡しするなどの対応が望ましい。
・　相互運用を行うサービス間で、情報セキュリティ基準を定め利用者が把握できるように公開すること。
・　PHRサービス事業者が相互運用先を決める際には、ISMSやプライバシーマークの取得等、一定レベルのセキュリティ水準を持つ企業を選定すること。
・　関連学会との連携やエビデンスの蓄積により、策定されたフォーマットが定期的に更新される仕組みを構築すること。

[xvi] 2022 年 9 月時点で、生活習慣病の予防・管理における活用を想定した PHR サービスにおいては「生活習慣病自己管理項目セット集」「PHR 推奨設定」。救急医療および災害医療における活用を想定した PHR サービスにおいては、R4 年度厚生労働科学研究費補助金（地域医療基盤開発推進研究事業）『救急医療等における基盤整備のための情報項目等の標準化に資する研究』の成果物として発表予定である「救急医療および災害医療における必要な情報項目（仮）」を対象として、データ交換規格を定める予定。
[xvii] 保健医療分野の適切な情報化を進めることを目的に、病名、医薬品名、臨床検査項目名、データの形式、データの伝達方法などを「厚生労働省標準規格」として採択・推奨しているもの。（http://helics.umin.ac.jp/helicsStdList.html 参照）

＜**PHRデータ標準交換規格案**＞

○データ交換規格
- マイナポータル API 形式
- IEEE P1752 Open Mobile Health
- HL7 FHIR
- JAHIS 電子版お薬手帳データフォーマット

参考：図3：PHRサービスに関連するデータ交換規格の整理

○データ形式
- XML（※現時点でマイナポータル API が XML 形式のため）
- JSON

○特定のフォーマットによるデータエクスポートの担保が必要な項目
- 特定健診、乳幼児健診、薬剤情報、予防接種歴等、マイナポータル経由で提供される項目（健診等情報）

※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する

○項目コード・用語
- JLAC10
- 健診標準フォーマット　（参考URL https://www.kenshin-hyojun.jp/）
- YJコード

＜**望ましい例**＞

- データの情報源、取得方法等データの質に関するメタ情報も合わせて、サービス間でデータの相互運用をする。
- サービス間でデータ定義の異なるデータを取り扱う際には、利用者に対してデータ定義が異なるためにデータが正確に引き継がれない可能性がある旨等の注意喚起を行う。

＜**不適切な例**＞

- 情報漏洩防止を含め利用者が安心・安全に使用できる環境になっていない。
- 個人情報保護法上の例外に該当しないにも関わらず、利用者の同意なしにサービス間でデータの授受をすること。
- 個人情報保護法上の例外に該当しないにも関わらず、利用者の同意なしに個人データの第三者提供を行うこと。

（2）医療機関との連携

考え方

PHRサービスの提供に際しては、安全性・有効性を保つために、かかりつけ医/産業医等を含め、利用者の健康・福祉のために多職種で連携することが望ましい。「医療と連携するサービス」と「医療が関わることを前提としないサービス」の両方が拡がるように、必要なときは医療者（かかりつけ医）が使えるサービスを提供することが望ましい。また、「治療と仕事の両立支援」「自治体健診との連携による医療の質向上」等を目的としたPHRサービスの創出も望ましい。その際に、医療機関でも個人の健康情報を閲覧できるよう、PHRデータのポータビリティの確保に努めることが望ましい。

推奨される事項

- PHRの中で救急・災害時に迅速に提示・閲覧できるような仕組みを活用すること。
- 医療サービスの質向上に資するデータについて、医療機関との連携を促す仕組みを創出すること。

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、医療者及び医療関連学会や医師会等が、PHRサービス事業者育成に積極的に関わることが望ましい。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。

（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・信頼性を踏まえた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

- 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、また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ま

たは能力がある十分なスタッフを明示する。
- ✓ アク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する。
- ✓ 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。

【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「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サービス事業者や自治体が、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。

推奨される事項

- 質評価のために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サービスにかか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またはISMS認証などの情報セキュリティに係る公的な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またはISMS認証などの情報セキュリティに係る公的な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。

今後の検討の進め方

本ガイドラインは、これまでの検討会における関係者間の議論、PHRサービス事業者へのヒアリングを踏まえた検討の結果であるが、今後は、より多くのPHRサービス事業者、医療者及びPHRサービスを活用して健康増進の取り組みを行っている地方公共団体等の関係団体、PHRサービスを利用する個人、患者・家族とも意見交換を行い、さらに実務的、技術的、法制的、社会的、及びその他の専門的見地から、具体的内容の検討を継続していく予定である。

国の民間利活用作業班において、PHR事業者として遵守すべき情報の管理・利活用に係るルールとして国のPHR指針がまとめられ、2021年4月23日に公表された。また、当指針を補完するものとして、より高い水準のPHRサービスの提供のための民間事業者ガイドラインの策定が望まれており、PHR事業者間において、最新の利用可能な技術や知見に基づき、より先進的・高度な取組を推進する観点で検討していくことが期待されている。2021年3月からの国のマイナポータルを活用した特定健診結果の閲覧開始及び新型コロナウイルスの感染拡大に伴う社会情勢の変化に加えて、PHRサービスの提供に関わる技術革新が進み、多種多様なPHRサービスが展開されると考えられることから、このような変化を踏まえたPHRサービスのあり方について検討していくことも必要である。

PHR普及推進協議会が目指すのは、PHRが「産（企業利益、CSR）」「官（町づくり、地方創生）」「学（研究の推進）」「民（市民の健康増進）」の各々に役立つ社会基盤になり得ることである。そのために、本ガイドラインの社会実装による良質なPHRサービスの普及に向けて、今後も継続的にPHRサービス事業者や自治体関係者、PHRサービス利用者へのヒアリング等を実施し、さらに検討を深めていきたい。

付録

【検討委員】

＜一般社団法人 PHR 普及推進協議会＞

名誉会長

永井　良三　　自治医科大学 学長

代表理事

石見　拓　　京都大学大学院医学研究科 社会健康医学系専攻 予防医療学分野　教授

副理事長

阪本　雄一郎　　佐賀大学医学部 救急医学講座　教授

理事

阿部　達也　　株式会社ヘルステック研究所　代表取締役

天野　雄介　　東和薬品株式会社　執行役員事業推進本部長/ T スクエアソリューションズ株式会社　代表取締役社長

大神　明　　産業医科大学 産業生態科学研究所 作業関連疾患予防学　教授

黒田　誠　　元 総合メディカル株式会社　特別参与

小林　寛史　　一般社団法人 ICT まちづくり共通プラットフォーム推進機構　代表理事

水戸　重之　　TMI 総合法律事務所　パートナー弁護士

矢作　尚久　　慶應義塾大学大学院 政策・メディア研究科　准教授

山口　育子　　認定 NPO 法人ささえあい医療人権センターCOML　理事長

山本　景一　　和歌山県立医科大学 情報基盤センター　准教授

監事

野田　博明　　公益財団法人日本 AED 財団　理事・事務局長

顧問

山崎　俊巳　　一般社団法人エコロジー・カフェ　理事

＜専門委員＞

木村　映善　　愛媛大学大学院医学系研究科 医療情報学講座　教授

窪寺　健　　日本医師会総合政策研究機構　客員研究員

黒田　知宏　　京都大学医学部附属病院 医療情報企画部　教授

長島　公之　　公益社団法人 日本医師会　常任理事

樋口　範雄　　武蔵野大学法学部　教授

星川　安之　　公益財団法人 共用品推進機構　専務理事

松田　義和　　一般社団法人 京都府医師会　理事

＜部会員＞

伊藤　友弥	あいち小児保健医療総合センター救急科　医長
小林　大介	京都大学 環境安全保健機構 産業厚生部門　助教
齋藤　俊	TMI 総合法律事務所　アソシエイト弁護士
島本　大也	京都大学大学院医学研究科 社会健康医学系専攻 予防医療学分野　特定助教
高橋　翼	合同会社 beyondS　代表社員
立山　由紀子	京都大学大学院医学研究科 社会健康医学系専攻 予防医療学分野　特定助教
森川　和彦	東京都立小児総合医療センター 臨床研究支援センター　医長
山田　洋太	株式会社 iCARE　代表取締役

※役職名ごとに五十音順で表記（委員の所属等は検討当時のもの）

【作業班員】

＜PHR標準項目・規格作業班＞

班長

山本　景一	和歌山県立医科大学 情報基盤センター

班員

鹿妻　洋之	オムロンヘルスケア株式会社
狩野　真也	シミックホールディングス株式会社
木村　映善	愛媛大学大学院医学系研究科 医療情報学講座
窪寺　健	日本医師会総合政策研究機構
黒田　知宏	京都大学医学部附属病院 医療情報企画部
小林　大介	京都大学 環境安全保健機構 産業厚生部門
澤田　砂織	公益財団法人 京都高度技術研究所（ASTEM）
島本　大也	京都大学大学院医学研究科 社会健康医学系専攻 予防医療学分野
高橋　翼	合同会社 beyondS
名田　茂	ＴIS 株式会社
古屋　博隆	テルモ株式会社
三宅　祥徳	KDDI 株式会社
森川　和彦	東京都立小児総合医療センター 臨床研究支援センター
矢作　尚久	慶應義塾大学大学院 政策・メディア研究科
渡邊　克也	PHC ホールディングス株式会社

＜PHRサービスの質（安全性・有効性・信頼性）に関わる作業班＞

班長

大神　明	産業医科大学 産業生態科学研究所 作業関連疾患予防学

班員

荒木　秀明	シミックホールディングス株式会社
伊藤　友弥	あいち小児保健医療総合センター救急科
川添　博之	日本マイクロソフト株式会社
齋藤　俊	TMI 総合法律事務所
阪本　雄一郎	佐賀大学医学部 救急医学講座
高橋　由光	京都大学大学院医学研究科 社会健康医学系専攻 健康情報学分野
立山　由紀子	京都大学大学院医学研究科 社会健康医学系専攻 予防医療学分野
長島　公之	公益社団法人 日本医師会
樋口　範雄	武蔵野大学法学部

松田　義和	一般社団法人 京都府医師会
三木　竜介	株式会社リンクアンドコミュニケーション
水戸　重之	TMI 総合法律事務所
山田　洋太	株式会社 iCARE

＜第1版の検討＞

【検討会日程】

2020年8月14日　　第1回民間PHRガイドライン策定にかかる準備会議
2020年9月2日　　第2回民間PHRガイドライン策定にかかる準備会議

＜全体会議＞
2020年9月30日　　第1回民間PHRガイドライン策定検討会
2020年12月23日　　第2回民間PHRガイドライン策定検討会

＜専門部会＞
医療
2020年10月22日　　第1回医療専門部会
2020年11月12日　　第2回医療専門部会

ELSI（倫理的・法的・社会的課題）
2020年10月28日　　第1回ELSI専門部会
2020年11月18日　　第2回ELSI専門部会

情報
2020年10月19日　　第1回情報専門部会
2020年11月17日　　第2回情報専門部会

民間
2020年10月29日　　第1回民間専門部会
2020年11月19日　　第2回民間専門部会
2020年12月8日　　第3回民間専門部会
2020年12月14日　　第4回民間専門部会
2021年1月26日　　第5回民間専門部会
2021年2月19日　　第6回民間専門部会

【民間PHR事業者ヒアリング日程】

2020年11月19日	第1回民間PHR事業者ヒアリング
2020年12月8日	第2回民間PHR事業者ヒアリング
2020年12月14日	第3回民間PHR事業者ヒアリング
2021年2月19日	第4回民間PHR事業者ヒアリング

※ヒアリング実施企業（実施企業数21社：2021年2月26日現在）

アストラゼネカ株式会社、イノルールズ株式会社、オムロンヘルスケア株式会社、株式会社オールアバウト、キューサイ株式会社、KDDI株式会社、株式会社三和製作所、株式会社JMDC、シミックホールディングス株式会社、ソフトバンク株式会社、田辺三菱製薬株式会社、TIS株式会社、Tスクエアソリューションズ株式会社、テルモ株式会社、東和薬品株式会社、PHC株式会社、株式会社ベネフィット・ワン、メドピア株式会社、株式会社ユニマットリタイアメント・コミュニティ、株式会社ユーズテック、株式会社リーバー

今後のヒアリング予定企業：株式会社エムテイーアイ、株式会社JTB　他
（民間理事・部会員：株式会社iCARE、株式会社ヘルステック研究所）

＜第2版改訂における検討＞

【PHRサービスガイドライン策定特別委員会日程】

2021年6月2日	第1回会議
2021年11月1日	第2回会議
2022年1月31日	第3回会議

【作業班会議日程】

PHR標準項目・規格作業班

2021年7月16日	第1回会議
2021年9月6日	第2回会議
2021年10月5日	第3回会議
2021年12月1日	第4回会議
2022年1月11日	第5回会議

PHRサービスの質（安全性・有効性・信頼性）に関する作業班

2021年7月28日	第1回会議
2021年8月24日	第2回会議
2021年10月1日	第3回会議
2021年11月19日	第4回会議
2022年1月20日	第5回会議

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：民間PHRサービスリファレンスアーキテクチャ

内閣府「戦略的イノベーション創造プログラム（SIP）第2期／ビッグデータ・AIを活用したサイバー空間基盤技術のアーキテクチャ構築ならびに実証研究事業*」及び、同実証研究事業の成果である一般社団法人データ流通推進協議会「2019年度SIPパーソナルデータ分野アーキテクチャ構築DTA公開*」において、PHRサービスも含めたパーソナルデータを取り扱うサービスについては、各事業者が自らの事業のアーキテクチャを設計・整理し、パーソナルデータの取扱いの適正性や潜在する課題を顕在化し、適切なパーソナルデータの利活用モデルを構築することが推奨されている。

本別添では、一例として、マイナポータルAPIと接続して健診等情報を取り扱うPHRサービス事業者のアーキテクチャを参考として示す。
なお、PHRサービス事業者の立場から見た時の取引形態として、以下の分類が考えられるが、今回はBtoC（個人がPHRサービス事業者と直接契約を行う）の場合についてのアーキテクチャの一例を示す。

取引形態	説明	補足	契約における留意点
BtoC	事業者が個人と直接契約してサービスを提供する	組織が仲介する場合もある	
BtoBtoC(E)	事業者と組織（医療機関・健診機関・健保組合など）が契約した上で患者や被保険者にPHRサービスを提供する	PHR機能を持った健保向け特定保健指導支援システムも存在する	個人は、組織（自治体）との契約に加え、事業者のサービスへの利用同意も行う
BtoGtoC	事業者と自治体が契約の上で住民にPHRサービスを提供する		
BtoB	事業者は組織と契約してPHRサービス業務を提供する	事業者はPHRシステムベンダーとして業務委託を受ける立ち位置になる	個人は、組織（自治体）とのみ契約する
BtoG	事業者は自治体と契約してPHRサービス業務を提供する		

※B=Business（法人・組織）、C=Consumer（一般消費者・個人）、E=Employee、G=Local Government（地方自治体）

* SIP サイバー/アーキテクチャ構築及び実証研究の成果報告（https://www8.cao.go.jp/cstp/stmain/20200318siparchitecture.html）
* 2019 年度 SIP パーソナルデータ分野アーキテクチャ構築 DTA 公開（https://data-trading.org/sipb-1_personaldataarchitecuture_dta/）

■ステークホルダーリスト（例）

目的：関与する個人、事業者の一覧表を作成することで、パーソナルデータ の取り扱われる範囲を明確し、プライバシー原則などを遵守すべきプレイヤーに抜けがないかを確認する。

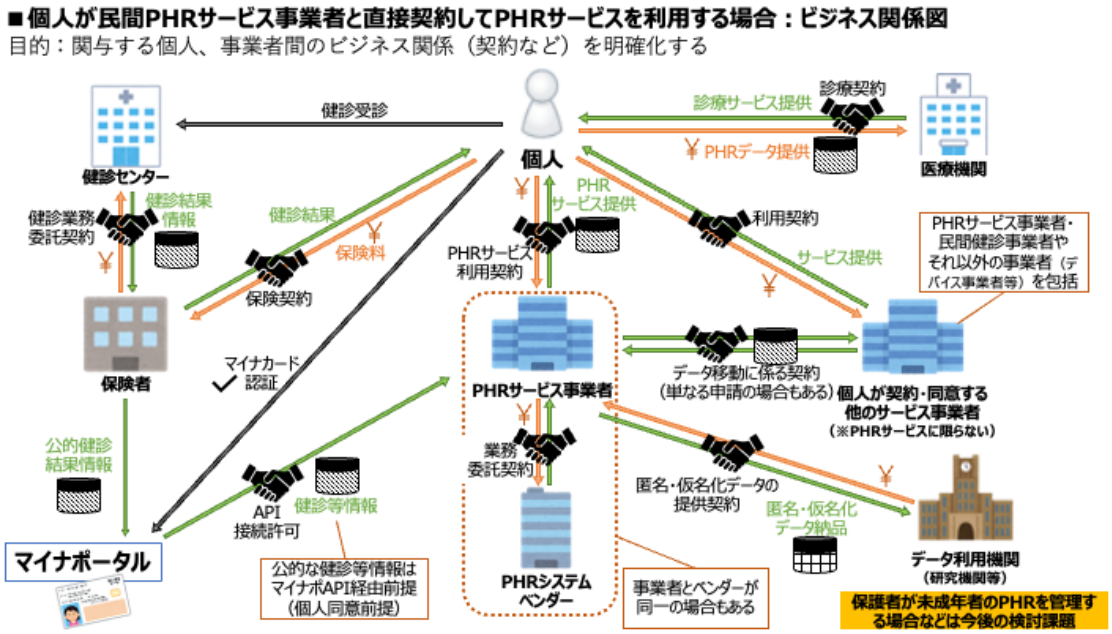
名称	概要（主に個人情報保護法での位置づけ等）	ISO/IEC 29100での分類(*)/ 役割
個人	PHRサービスを利用している個人	PII principal
マイナポータル	国が提供するマイナポータルを活用したPHRサービス	Data controller
医療機関1	国立大学病院、国立病院（個人情報保護法上の独立行政法人）	Data controller
医療機関2	自治体により設置された病院（個人情報保護法上の地方独立行政法人）	Data controller
医療機関3	民間病院または診療所（個人情報保護法上の個人情報取扱事業者）	Data controller
調剤薬局	病院、診療所からの処方箋を受け取り、調剤を担当（個人情報取扱事業者）	Data controller
介護施設	介護施設（個人情報取扱事業者）	Data controller
健診センター	健診を主たる業務とする機関（個人情報取扱事業者）	Data controller
PHRサービス事業者	個人の信託を受け個人データを預かり、PHRサービスを提供する（個人情報取扱事業者）	Data controller
PHRシステムベンダー	PHRサービス事業者からの委託によりPHRシステムの開発管理及び個人データの管理を行う（個人情報保護法上の委託先に該当）	Data processor
他サービス事業者	健康保険・介護保健の枠外で実施される民間の健康サービス提供事業者など、個人が契約する他のサービス事業者（個人情報取扱事業者）	Data controller
データ利用機関	匿名化・仮名化された個人情報を利用する研究機関。原則的に、データ取得はしない（個人情報取扱事業者に該当しない）	非該当

（参考）ISO/IEC 29100 アクターとその役割定義

- PII Principals：PIIが関係する自然人
- PII controller：PII処理の行われる理由（目的）及び方法（意味）を決定する
- PII processor：PIIコントローラに代わってPII処理を実行し、またPIIコントローラの指示に従って動作し、規定のプライバシー要件を順守し、対応するプライバシーコントロールを実装する
- 3rdParty：PIIをPIIコントローラやPIIプロセッサから受け取ることができるが、処理はしない

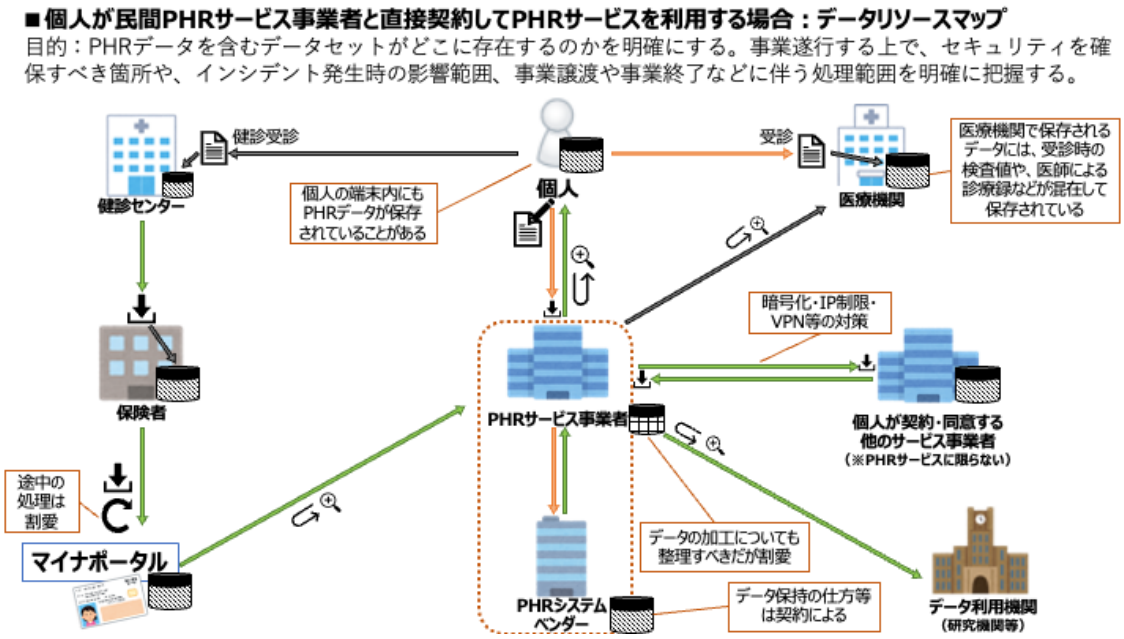
■ビジネス関係図（例）

目的：関与する個人、事業者間のビジネス関係（契約など）を明確化する。



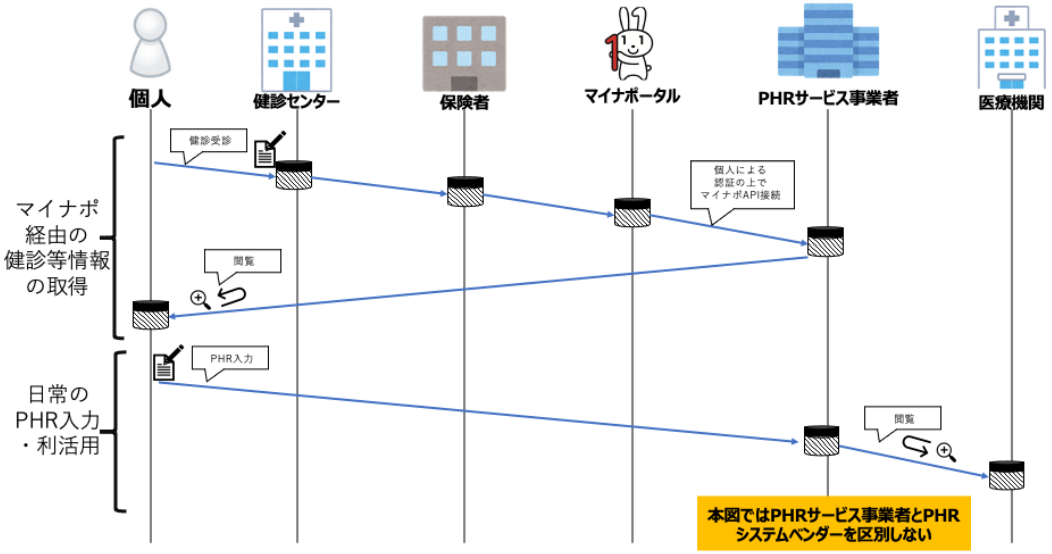
■データリソースマップ（例）

目的：PHRデータを含むデータセットがどこに存在するのかを明確にする。事業遂行する上で、セキュリティを確保すべき箇所や、インシデント発生時の影響範囲、事業譲渡や事業終了などに伴う処理範囲を明確に把握する。



■データフローシーケンス（例）

目的：関係者間でのデータセットの移動、処理フローを明確化する。



別添３：PHRサービス自己チェックリスト

点検日： _____
点検者： _____

【一般的事項】	チェック			
1．取り扱いの情報	はい（対応済）	いいえ（対応未）	わからない（不明）	該当しない
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.　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				
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　X 8341-3:2016*）				
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				

【有効性に関する事項】

6. リコメンドサービス			はい（対応済）	いいえ（対応未）	わからない（不明）	該当しない
6-1.	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					
	6-1-1.	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				
	6-1-2.	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				
		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				
	6-1-3.	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				
	6-1-4.	同サービスに対するリスクアセスメントの方法や内容を開示していますか				
6-2.	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					
	6-2-1.	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				
	6-2-2.	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				
	6-2-3.	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				
	6-2-4.	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				
7. 管理・閲覧サービス						
7-1.	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					
	7-1-1.	管理・閲覧サービスに対するリスクアセスメントの方法や内容を開示していますか				
7-2.	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					
	7-2-1.	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				
	7-2-2.	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				
	7-2-3.	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				
7-3.	管理・閲覧サービスに対する利用者側の利便性					
	7-3-1.	利用者が自身のPHRデータを自由に閲覧できるようになっていますか				
	7-3-2.	利用者の求めに応じてPHRデータを削除できるようになっていますか				
	7-3-3.	健診等情報を取り扱う場合は、その情報をエクスポートできるようになっていますか				
	7-3-4.	PHR普及推進協議会が定めるPHRコア項目**を取り扱っていますか？				
		該当する場合は、その情報をPHR普及推進協議会が推奨する流通規格でエクスポートできるようになっていますか。				

【安全性（機密性）に関する事項】

8. 第三者機関による監査	はい（対応済）	いいえ（対応未）	わからない（不明）	該当しない
8-1. 情報セキュリティ対策				
8-1-1. 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				
8-1-2. 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				
8-2. 脆弱性診断等システムにおける安全性				
8-2-1. 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. 運用体制や責任者				
9-1. 情報管理責任者とカスタマーサポート				
9-1-1. 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				
9-2. 運用体制				
9-2-1. 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				
9-2-2. アク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				
9-3. クラウド事業者の選定				
9-3-1. 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】

10. 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
10-1. 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				
10-2. 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				
10-3. 運用ポリシーを公開していますか				
10-4. 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				
10-5. 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				
11. 運用や体制の開示				
11-1. 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				
11-1-1. 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				
11-2. 不具合発生時の体制及び対応方法の開示				
11-2-1. 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				

*JIS X 8341-3:2016 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
**PHR普及推進協議会が推奨するPHRコア項目と流通規格