民間事業者の PHR サービスに関わるガイドライン（第 3 版）

【追補２】PHR の自治体への導入における留意点

一般社団法人 PHR 普及推進協議会

（2024 年 6 月）

はじめに

本文書の位置づけに関して

本文書は、自治体が PHR サービスを導入する場合やデータ利活用をする際の留意事項についてまとめたものである。民間 PHR サービス事業者との連携において留意すべき点や、自治体が PHR サービスの運営主体となる場合についてや本文中の用語、検討の経緯については、一般社団法人 PHR 普及推進協議会の「民間事業者の PHR サービスに関わるガイドライン（第 3 版)」をあわせて参照いただきたい。

本文書と C4IRJ のツールキットとの関係

- 自治体において PHR サービスを実装し、データ活用をするに際しての基本原則やチェック項目を示し、当該自治体の現状分析、課題抽出と解決策の提示を通じて、実装・普及を推進する。また、企業への発注に際しての参考事項とすることで、自治体間の連携を容易にし、ベンダーロックインを避けるとともに、導入・維持コストの削減をめざす。
- 企業において適切なデータガバナンスを実現し、ビジネス上の予測可能性を高める。
- 市民の Well & Healthy Ageing を実現し、プライバシー等の侵害リスクを最小化する。

これらのための、自治体における PHR 導入を中心としたヘルスケアデータ活用のための原則を確認し、自治体における保健・医療・介護の DX（デジタルトランスフォーメーション）の推進に資するものとする。

本文書は、2023 年に世界経済フォーラム第四次産業革命日本センター（C4IRJ）が作成した「自治体向け PHR・データ利用ツールキット Ver.0」をベースとして一般社団法人 PHR 普及推進協議会において作成したものである。

１．自治体への導入に際して守るべき原則（基本原則）

以下の 6 つの原則に従った PHR サービスの実装やヘルスケアデータの利活用を行うこと。

(1) 個人の自律・本人への利益

(2) 透明性・プライバシー

(3) 相互運用性・オープン性

(4) 公平性・包摂性

(5) 価値実現・社会的正義

(6) 持続可能性

本 6 原則は、個人情報保護委員会「個人情報等の適正な取扱いに関係する政策の基本原則」[1]、GSCA「スマートシティ 5 原則」[2]やデジタル庁の「デジタル 5 原則」[3]、医療倫理 4 原則[4]等の守るべき原則を満たすものとして整理を行った。

(2)～(6)はスマートシティ 5 原則と同様のものであるが、特に PHR サービスにおいては各個人の関与が重要であるため、(1)（医療倫理 4 原則における自律尊重と善行の要素）を加えた形での整理となっている。

[1] 1. 個人情報等の取扱いの必要性・相当性 2. 個人情報等の取扱いに関する適法性 3. 個人情報等の利用目的との関連性・利用の適正性 4. 個人情報等の取扱いに関する外延の明確性 5. 個人情報等の取扱いの安全性 6. 個人情報等に係る本人関与の実効性 7. 個人情報等の取扱いに関する透明性と信頼性
https://www.ppc.go.jp/files/pdf/kihongensoku.pdf

[2] 透明性とプライバシー保護（Transparency & Privacy）、安全・安心・回復性（Safety,Security & Resiliency）、相互運用性とオープン性（Interoperability & Openness）、公平性、社会的包摂、社会的影響（Equity,Inclusion & Societal impact）、運用面と財政面の持続可能性（Operational & Financial Sustainability） https://globalsmartcitiesalliance.org/?page_id=90

[3] デジタル完結・自動化原則、アジャイルガバナンス原則（機動的で柔軟なガバナンス）、官民連携原則（GtoBtoC モデル）、相互運用性確保原則、共通基盤利用原則
https://www.digital.go.jp/meeting/posts/91qdfD4B

[4] 自律尊重（respect for autonomy）、無危害（non-maleficence）、善行（beneficence）、正義（justice）

２．個人の自律・本人への利益

データ主体である各個人（市民）の自律を尊重し、PHR サービス等を通じた健康上もしくはそれ以外の（金銭面も含めた）利益があるか、本人の関与が適切になされているかに関する項目である。

✓ 本人確認は適切にできているか

そもそもデータが本人に渡されていること、利益が本人に還元されることの前提として、適切な本人確認が求められる。行政機関のデータとの接続や医療データ連携に際しては、基本 4 情報（氏名／住所／性別／生年月日）を用いた本人確認（そのための運転免許証やパスポート等の提示）なども必要となる場合がある。また、マイナンバーカードと公的個人認証サービス（Japanese Public Key Infrastructure: JPKI）を利用した、インターネットを介した本人確認も可能である。すべての PHR サービスの運用上必要なわけではないが、自治体をまたいだデータ移転など、相互運用性の点でも適切な手法を用いる必要がある。

✓ 本人の健康上その他の利益が明確であるか

PHR サービスの導入やデータ利活用によって、本人への利益が明確に期待されること。
データ二次利用の場合、データ主体本人への利益が直接的には存在しない場合もある点につき留意し、提供する条件・範囲を示して医学への貢献等があることを理解してもらう必要がある（次項目）。

✓ （第三者提供に即して）本人への利益還元（ポイント等）の仕組みがあるか

PHR サービスによる価値実現は本人へのサービス提供やその質の向上が中心となる。二次利用を行い、データを第三者に提供する場合、ポイントなどにより本人に対しても適切な利益が還元されることが望ましい。ただし、そうした利益還元は、持続可能性を念頭に置く場合、必ずしも十分な金銭的見返りは提供できない場合もあるため、その価額等が提供するデータのプライバシー等へのリスクにみあったものであるかを踏まえ、ユーザーの理解を得るように心がける。

✓ 本人によるデータ管理が可能か（データポータビリティがあるか）

PHR サービスに関しては、単に医療機関や自治体が有するデータを閲覧できるシステムとなることも多い。しかし、本人にとっての利便性を考慮するなら、データの適切な形式でのダウンロードや電子的な移転が可能となっている（データポータビリティの担保がなされてい

る）ことが必要である。本項目の実現に関しては、PHR 指針[5]において求められている範囲を踏まえ、システム的な負担やセキュリティなどのリスクとの兼ね合いにも配慮しながら、相互運用性担保に向けた実装をする必要がある（他項目参照）。

✓ **本人又はデータ管理者が本人の同意状況が確認できるツールが有るか**

個人情報保護法や EU の一般データ保護規則（General Data Protection Regulation：GDPR）において、本人同意が求められる局面は多い。その際に、本人が何に関して同意をしているかが確認可能なシステムが含まれていることが望ましい。さらに、本人の意思を随時確認し、同意撤回が可能となること（ダイナミックコンセント）や、子供や高齢者等本人の意思能力に問題がある場合における代理人等の意思確認ができるようになっているとなおよい（研究目的での利用時等においてこれらが必要となる場合があることに注意すること）。

✓ **本人による異議申し立て等の窓口があるか**

個人情報保護法や PHR 指針で求められている本人による異議申し立てや削除等の請求への対応が全て適切に実施されること。自治体においては、それらへの対応窓口とともに企業との役割分担を明確にし、データの削除や修正等可能な対応に関しても明確なルールが示されていること。

３．透明性・プライバシー

データの利活用・PHR サービスの運用に際しては、個人情報保護法制に従い、十分なプライバシーへの配慮やセキュリティ対策を行う。また、意思決定過程や運用に際して透明性を確保し、可能な限りプライバシーリスクの潜在的な影響や脅威を評価した上での実施をする。

✓ **データの利用目的が十分に明確に示されているか**

データの利用目的に関しては、それを読んだ市民にとってどのように使われるか理解可能な程度の適切な粒度で示す必要がある。公衆衛生の向上、医学の進歩といったあまりに広範な目的は望ましくはない。

✓ **データ収集は適正な方法でなされているか**

データ収集手段が個人情報保護法その他法律に反する方法での収集となってはならない。特に、第三者からデータ提供を受ける際に、適正な方法での提供となっていること。

[5] 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
https://www.meti.go.jp/press/2021/04/20210423003/20210423003.html

✓ **データの管理主体（コントローラー）とその管理方法が明確に示されているか**

データを管理するのが自治体なのか、自治体から委託された企業等なのか、各個人で管理する形を取るのか等、どのような形での運用となるかを明確にすること。これは自治体のシステムや医療情報システムとの接続の仕方にも関連する点である。自治体による業務の委託としての管理であるのか、自治体から第三者提供がなされて別事業での利用がなされるのかに関しては、明確に示す必要がある（次項目とも関連）。

✓ **データ利用に際しての責任の所在は明確か**

管理監督に関しては前項のコントローラーの責任となるが、そこからデータの第三者提供をする場合、以降の責任の所在がどの様になっているかを確認する必要がある。例えば、匿名加工情報を提供する際は、あらかじめ第三者に提供される情報の項目及びその提供の方法について公表する必要があることや、次世代医療基盤法に基づく提供を想定する場合は、一定の制約がなされることになる等、契約により制約することも必要に応じて検討する。

✓ **セキュリティ対策は適切になされているか**

PHR サービス事業者に求められるセキュリティ対策としては、PHR 指針で一定のものが示されているが、医療情報システムとの接続においては、医療情報に関するいわゆる 3 省 2 ガイドライン等の関連するガイドラインへの準拠や、自治体とのシステム接続の場合に求められるセキュリティ基準との関係で適切な水準の確保をすること。

✓ **（匿名加工をする場合）適切な加工がなされているか**

「匿名化」をする際には、個人情報保護法における「匿名加工情報」としての運用を行うのか、同法における「仮名加工情報」等特定の個人が識別できるままの状態なのか、統計化する等個人情報ではない状態にするのか、どの程度の加工を行うのか、を明確にすること。一時的にでも生データを持たざるを得ない場合があることに留意が必要である。なお、秘密計算等、暗号化を利用する場合や、画像データを扱う場合等、法的に特定の個人は識別可能との評価である場合が多いことに留意する必要がある。

✓ **（AI を用いる場合）AI による判断基準は明確に示されているか**

データに基づいて分析をし、本人にリコメンデーションを返す場合等、人工知能（AI）を用いた判断を行う場合は、AI に関する特別な規制（AI 関連の国内外の原則、特に EU において定められているものや、薬機法におけるプログラム医療機器等の規制等）への配慮が必要である。例えば、どのような判断根拠（アルゴリズム）で評価がなされているかを可能な限り透明化する（説明可能な AI を利用する）ことが求められる。

✓ **その他プライバシー関連法規の遵守状況が明確か**

個人情報保護法、自治体の条例等との関係での遵守状況を明確にすること。可能な限りプライバシーリスクの潜在的な影響や脅威を評価する（Privacy Impact Assessment：PIA）ことで、事前の対応を図ること。なお、上記の同意取得がある、適切な匿名加工がなされているといったこと以外に、公衆衛生の向上目的としての利用、行政目的での（法令に基づいた）利用、学術研究目的での利用の余地があることに留意すること（医療・介護のガイダンス参照）。

（参考）PIA に関しては、G20 Global Smart Cities Alliance においてモデルポリシー[6]が示されている。こうしたスマートシティ一般としての評価の一環としてヘルスケア領域においても PIA を実施するのが望ましい。
PIA を条例化することについて：つくばの事例等を念頭に記載

４．相互運用性・オープン性

自治体の公共的な性質から、組織間の壁を意識せずデータ利活用が最大限に行われるように、特にベンダーロックインへの対応も含めて、データ利用やその結果に関するオープン性を担保することが求められる。また、類似のシステムが自治体内もしくは複数自治体において乱立することがしばしば見られ、結果としてユーザーである市民にとって不都合が生じる場合がある。そのため、システム間において様々なデータに接続することが可能となる相互運用性を担保しながらエコシステムの実現を図るべきである。以下の項目を満たすことが求められる。

✓ **円滑なデータ交換・活用を担保できるような標準規格の利用が行われているか**

医学系学会において定められた「PHR 推奨設定」等、標準化に関する活動に関しては可能な限り連携を行い、一般に使われているオープンな標準規格が存在する場合には可能な限りそれを用いること。

✓ **API 連携が可能でデータの移行が容易である等、自治体を超えた相互運用が可能となっているか**

マイナポータルを通じた API 連携等の国の動きも踏まえ、PHR アプリ間での相互運用性を確

[6] http://globalsmartcitiesalliance.org/wp-content/uploads/2021/02/PIA-v1.2-JA.pdf

保できるような取り組みを行うこと。例えば、国のPHR指針で求めているように、互換性の高いデータファイルにより利用者へのエクスポート機能及び利用者からのインポート機能を具備することで、利用者を介した相互運用性を確保することに加えて、適切性を確認した事業者間での直接のデータ連携を可能とすることを推奨する。

✓ **（データの公益目的での二次利用の場合）データ利用の結果に関して公開等、適切な社会還元がなされるか**

データ分析・利用により、学術論文としての公表がなされた場合も含めてどのような結果が得られたか、実際に社会還元がなされたかに関する公開を適宜行うこと。期待した結果が得られなかった場合に関しても、その影響に関する判断の上、原則として公開を行うこと。

✓ **（匿名加工の上で）データのオープン化がなされているか**

自治体におけるオープンデータ化の推進に資する取り組みはヘルスケア領域においても求められる。そのため、前項の分析結果だけでなく、元のデータに関しても可能なものはオープンにすること。その際に、プライバシーへの配慮から、統計化ないし適切な匿名化を行う。「仮名加工」にとどまる匿名加工に関しては通常は公表できないことに注意すること。

５．公平性・包摂性

健康増進はあらゆる市民に共通の課題であり、あらゆる人材が能力を最大限発揮し、やりがいを感じられるような社会を実現することにもつながるため、誰一人取り残さないように努める必要がある。

✓ **特定のデバイスを必要とするサービスの場合、そのデバイスを持たない/使えない市民への配慮がなされているか**

デジタル化の恩恵を受けられるのは、実証事業段階では一部市民に限定されてもよいが、将来的には必ず全市民が利用可能な設計を心がける必要がある。例えば、スマートフォンやマイナンバーカード所有者等、特定の条件を要する場合には、非保有者への配慮として場合によっては紙等を用いた代替手段の検討も行うべきである。ただし、業務の効率性や持続可能性（他項）との兼ね合いでの実装とすること。

✓ **ユニバーサルデザインとなるような適切な配慮を含めUI/UXが適切にデザインされているか**

色覚障碍者、外国人等であっても適切に利用可能なサービスとすること。特に認知症高齢者等本人の同意能力がない場合にも補助者・代理人を通じたサービス提供をするといった配慮をすることが望ましい。ユーザーである市民が使わないサービス・システムであっては意味がないので、利用のストレスが少ない設計とすること。そのため、セキュリティ面に関しても合理的な操作で実施できるようになっていることが望ましい。

✓ **本人に対するリコメンデーション等によって不公平な取り扱いがなされないか**

サービスの利用（もしくは利用しないこと）による差別的な取り扱いは決してなされてはならない。サービスを受けられない場合があることに加えて、サービスの内容の公平性にも配慮し、公的サービス（医療や教育等）に関する適正化を目指す場合には、十分な検討が求められる。また、民間においては、保険商品との連動や雇用の関係に関して等、重要な影響を与える事項に関しては不利益的な方法でのデータ利用を禁ずる等する必要がある。

６．価値実現・社会的正義

PHR サービスの利用を通じて、各個人の健康増進その他本人の利益が実現することが第一義的には求められる（(1)の各項目）。そのうえで、データの二次利用を行う場合（あるいは、最初から第三者の利益のためにデータを収集し活用する場合）、それによって実現する価値が社会的な正義にかなったものであることが求められる。

✓ **データの質・真正性の担保ができているか**

そもそも扱うデータが意味のあるものとなっている必要がある。可能な限り真正性が担保された元データの再入力は避ける等、データの質の確保・真正性の担保が可能なシステム設計が求められる。また、データを取得した日時や場所、方法、修正履歴などを記録したメタデータが伴っていると、後のデータ活用の幅が広がる。可能であれば、データの監査も行えることが望ましい。

✓ **（本人以外への価値実現がなされる場合）どのような価値実現がなされるかが明確に示されており、それが妥当な目的か**

本人以外へのメリット（例えば感染症対策等）が期待される場合は、それが適切・妥当な目的・手段によるものであることを明示し、それ以外の目的での利用はなされないことを明示すること。

✓ **科学的に根拠が示された介入が予定されているか。**

新興感染症対策等、必ずしも科学的根拠が定かではない介入を検討する場合もある。可能な限り、科学的根拠が存在する場合はその内容を確認・評価すること。科学的根拠に関しては、事後的な検証の可能性もあることに留意すること。

✓ **価値実現に即して不利益が生じる場合への適切な配慮がなされているか**

前項と関連し、本人のプライバシーや自由を制限してでも実現すべき価値であるのかどうか、それによってどのような権利の制限・不利益が想定されるかの評価（(3)の PIA 等）をし、適切な配慮が求められる。

✓ **価値実現や不利益に関して第三者からの検証が可能か**

医学研究としての実施に際しては、研究機関における研究倫理審査委員会による承認が求められる。同様に、自治体内もしくは適切な第三者の機関における事前の審査を経た実施がなされることが望ましい。さらに、事後の監査等、明示された価値実現が実際になされたか、どのような不利益が発生したかに関して、情報提供の判断過程、提供した情報の内容等について、第三者による検証が可能な状態とすることが望まれる。

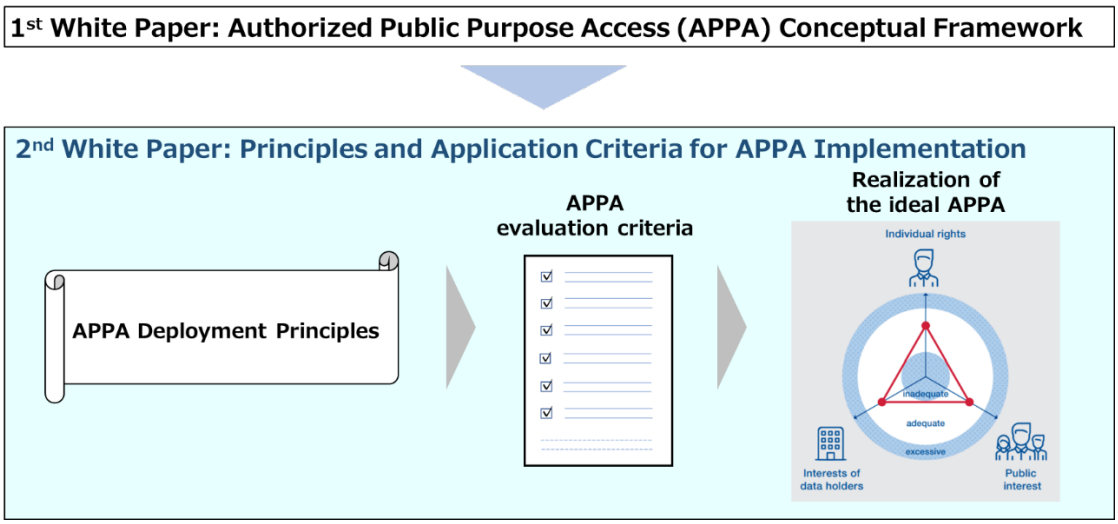
✓ **同意によらない第三者によるデータアクセスがなされる場合は、社会的合意のある公益目的等に限定されているか**

「公益目的」等の社会的な要請によるデータ利用に関しては、住民のコンセンサスを確認（説明会などを実施）の上で、個人情報に当たる元データをなるべく提供せず、最小限のデータへの最小限の利用者に対するアクセスコントロールを行う、目的に関して可能な限り明確化し限定する等の適切な手段による実施とする。本項に関しては、世界経済フォーラムによる提案である APPA（Authorised Public Purpose Access）[7][8]の観点も参考にする。

参考）世界経済フォーラム第四次産業革命日本センターは、ヘルスケアデータのガバナンスにおける国内外の課題を検討し、個人の人権・データホルダーにとっての合理性・公共の利益の三者のバランスがとられるためのデータ利活用モデル（APPA）の提案を行っている。

[7] "APPA –Authorized Public Purpose Access: Building Trust into Data Flows for Well-being and Innovation," 世界経済フォーラム

[8] "Resetting Data Governance: Authorized Public Purpose Access and Society Criteria for Implementation of APPA Principles," 世界経済フォーラム



APPA のコンセプトとその実装に向けた提案

提案のなかで、ヘルスケアのサービス提供の公共性の高さ、および個人の人権に配慮した、適切な官民連携の構築が、成功の鍵のひとつとなると結論づけており、事前同意によるコントロール（入口規制）から、アクセス設定・第三者審査（出口規制）への転換によるデータ活用の推進を提案している。

７．持続可能性

自然災害、不慮の事故、情報セキュリティなどによる障害が発生した場合でも、最低限の機能を維持しながら、早期に回復できる能力を確保するように努める必要がある。また、運用面・財政面の両方から持続可能でより効果的・効率的な事業であることを確認しながら実装するように努める必要がある。自治体における業務効率が上がることは、その直接的な効果だけでなく、自治体が他のサービスに注力できることで、間接的な恩恵も住民は受けられることとなる。

✓ **災害時やパンデミック時など、緊急時も含めてシステムの最低限の機能の維持が可能か（レジリエンスがあるか）**

医療や介護に関するシステムに関しては、それが使えないという状況はなるべく存在しないよう、停電やアクセス集中等も含めた緊急時の対応が可能なようにすること。一般的な健康

増進目的のアプリなど、緊急時の使用が不可欠ではないものに関しては、その限りではない。

✓ **中長期的に持続可能な（補助金頼みではない）モデルとなっているか**

多くのPHRサービスや地域医療連携システムにとって、金銭的に自立可能なものとすることが課題となっている。可能な限り、成果連動型民間委託契約（Pay For Success: PFS）・SIB（Social Impact Bond）等の活用や自治体における財源の確保も含めて、持続可能なモデルとする。そのため、個別の情報サービスだけでなく、連携する事業や別サービスとの関係での総合的な収益ないしコスト削減の評価を行うこと。

✓ **自治体の業務負荷が適切か**

ICTの導入（DX）はそれ自体が目的ではなく、自治体の業務プロセスの改善と合わせて実施することが求められる。そのため、運用に際して、保健所等の業務を圧迫することがあってはならない。ICT 活用は原則として現場の負担軽減がなされるものとなっていることが必要である。そのため、例えば、必要のない署名・押印等も廃止すること。

✓ **（官民連携に際して）民間側のインセンティブへの配慮がなされているか**

システム運用を行う企業にとって、対応内容が明確でなく行政側とのコミュニケーションコストを多く取られる等、特にセキュリティや相互運用性等の項目への対応コストが過大となる場合がある。また、自治体における実施であるという観点から、民間側の収益の機会を提供し、民業圧迫となっていないことも確認が必要である。

✓ **プログラム医療機器やオンライン診療等、医療関連の規制との関連で妥当な設計となっているか**

持続可能な実施ができるよう、プライバシー関連法規だけでなく、プログラム医療機器やオンライン診療、（医療）広告に関する規制など、各種の関連規制と関係に関しても、適切なサービス設計を行うこと。