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関する Q&A

令和３年４月

（令和４年４月一部改定）

（総務省、厚生労働省、経済産業省）

目次

１．本指針の基本的事項 1
２．情報セキュリティ対策 4
３．個人情報の適切な取扱い 6
４．健診等情報の保存及び管理並びに相互運用性の確保 10
５．要件遵守の担保 11
６．本指針の見直し 12

１．本指針の基本的事項

Ｑ１－１　健康相談サービスは、本指針の対象となるPHRサービスに含まれますか。

Ａ　単なる健康相談専用のコミュニケーションサービスであれば、基本的には対象外となります。一方で、同サービスにおいて、本指針の対象となる健診等情報を記録し、利用者が健康管理を行う機能も提供する場合は対象となります。

Ｑ１－２　３つの情報（＊）が対象として掲げられていますが、これらすべてに該当する場合に対象となりますか。又は１つでも該当すれば対象となりますか。

（＊）

・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

Ａ　１つでも該当すれば対象となります。

Ｑ１－３　「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」とありますが、この「マイナポータルAPI等」の「等」には何が含まれますか。

Ａ　本文１．１．の※に記載されているとおり、健康保険組合や医療機関等から入手する場合又は個人が自らアプリ等に入力する場合も含まれます。

Ｑ１－４　「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」が健診等情報とされているが、医療機関等から直接情報を入手する場合には本指針の対象となりますか。

Ａ　患者等の指示に基づいて医療機関等から医療情報を受領する場合には、本指針の対象とならず、「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」（令和２年８月（令和４年４月一部改定）総務省、経済産業省）（以下「提供事業者ガイドライン」という。）の遵守が求められます。この場合、本指針の対象外ではありますが、本指針の「３．個人情報の適切な取扱い」について、準用すべきと考えます。

Ｑ１－５　「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」には、具体的に何が該当しますか。該当するかどうかは、どのように判断すればよいですか。

Ａ　医療機関との連携を目的とする機能（医師に情報を提供し閲覧させることを想定したリコメンデーション機能等がある場合等）又は医療機関と連携する機能（医師が記録をオンラインで確認する機能等）等を備えたPHRサービスにおいて、個人が入力（測定器具か

ら自動的に記録される場合を含む。）する情報は対象となります。一方、PHR 事業者が提供するサービスが、本人における健康管理のみを目的としている場合は対象外です。

なお、後者の本人における健康管理のみを目的として提供された PHR サービスを利用している者が、自己の判断で、診療等において医師に見せることとなった場合等は対象外です。

Ｑ１－６　血糖値や体温など、具体的な情報の種類によって、対象であるかどうかは変わりますか。

Ａ　Ｑ１－２で示したように、以下３つのいずれかに、１つでも該当するか否かによります。

・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

Ｑ１－７　本指針を遵守すべき対象は、事業者単位ではなく、部署単位でもよいですか。

Ａ　原則、事業者単位ですが、PHR サービスを提供する部署が他の部署から経営及び運営が独立しているなどにより、提供する PHR サービスについて、その他の部署は一切関与しないなど、合理的な理由がある場合には、部署単位でもかまいません。

Ｑ１－８　自治体又は健康保険組合は本指針の対象となりますか。

Ａ　自治体又は健康保険組合は、条例や情報セキュリティ基準等が存在することから、本指針の対象とはしていません。

具体的には、自治体は、各自治体が策定する個人情報保護条例の適用対象となります。また、健康保険組合又は国民健康保険組合は、個人情報保護法の適用対象である他、「健康保険組合等における個人情報の適切な取扱いのためのガイダンス」（平成 29 年４月 14 日（令和２年 10 月一部改正）個人情報保護委員会、厚生労働省）又は「国民健康保険組合における個人情報の適切な取扱いのためのガイダンス」（平成 29 年４月 14 日（令和２年 10 月一部改正）個人情報保護委員会、厚生労働省）の適用対象となります。

なお、これらの条例等で規定されていない本指針「４．健診等情報の保存及び管理並びに相互運用性の確保」等については、本指針を参考に対応していただくことが望まれます。

Ｑ１－９　「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のみを取り扱う事業者」等は本指針の対象外とされていますが、その場合に遵守すべきガイドライン等はありますか。

Ａ　本指針の対象外とされている場合に関しても、それぞれの目的や取り扱う情報の種類等に応じて、関連する指針やガイドラインなどが存在する場合があります。各事業者の責任において、そうしたガイドライン等を確認し、遵守することが必要です。

Ｑ１－10　PHR 事業者の委託を受けてデータ保管のみを行う事業者は対象となりますか。

Ａ　PHR サービスを提供していない場合には、本指針の PHR 事業者には該当しませんが、データ保管を委託する PHR 事業者の監督の下、本指針の「２．情報セキュリティ対策」の遵守が求められます。

　なお、個人からデータを預かるだけのサービス（クラウドストレージサービス等）の場合には、本指針の対象外です。

Ｑ１－11　データは自社で保有せず、健診等情報の閲覧サービスのみを提供する事業者は対象となりますか。

Ａ　データ自体を保有していなくても対象となります。

Ｑ１－12　PHR 事業者からシステム開発を請け負う事業者は対象となりますか。

Ａ　対象となりません。

Ｑ１－13　本指針に違反した場合、罰則はありますか。

Ａ　本指針に基づく要請に違反していることで、罰則が適用されることはありませんが、個人情報保護法の要請を遵守できていない場合は、同法違反となります。

　なお、本指針を遵守していない場合には、PHR 事業者は、マイナポータル API 経由での健診等情報の入手ができなくなるほか、PHR サービスの利用者から、本指針による一定の基準を満たしていないと見なされ、他の事業者のサービスへの乗り換え等に繋がるおそれがあると考えます。

Ｑ１－14　本指針と「提供事業者ガイドライン」との関係を教えてください。

Ａ　患者等の指示に基づいて医療機関等から医療情報を受領する場合には 「提供事業者ガイドライン」の対象となります。例えば、利用者の指示に基づいて薬局から、システムを通じて直接、薬剤情報を受領する電子お薬手帳を提供する事業者等は、「提供事業者ガイドライン」の対象となります。

２．情報セキュリティ対策

Ｑ２－１　記載されている対策を必ず実施する必要がありますか。あるいは、各対策項目は例示で、同等の対策を採用すればよいですか。

Ａ　本指針に規定された対策そのものでなくても、同等程度以上の対策を講じることで代替することは可能です。また、実施しない合理的な理由がある場合には、チェックシートの末尾において、当該合理的な理由について記載してください。

Ｑ２－２　セキュリティポリシーの見直しはどの程度の頻度で行う必要がありますか。

Ａ　特定の期間を指定するものではありません。自社の状況（事業の規模及び性質、個人データの取扱状況（取り扱う個人データの性質及び量を含む。）、個人データを記録した媒体の性質等に起因するリスクの変化等）に鑑みて、必要に応じて見直しを行ってください。

Ｑ２－３　「経営を理解する立場の人」とはどのような人を想定していますか。

Ａ　経営層に対して、情報システム等の更新などに関して意見を言うことができる立場の人であり、一般的には役員クラスを想定しています。

Ｑ２－４　「情報資産の管理者」や「健診等情報を取り扱う人」とは、どのような人を指しますか。

Ａ　いわゆるサービスのユーザーではなく、PHR 事業者内において、健診等情報を管理又は取り扱う人のことを指します。

Ｑ２－５　「健診等情報の取扱い履歴を残しておくこと。」とあるが、具体的に何を行えばよいですか。

Ａ　健診等情報の取扱いに関して、サーバーやクラウドに情報へのアクセス等に関するログを残しておくことを想定しております。情報セキュリティに係る事故等が発生した場合に追跡できることが必要です。

Ｑ２－６　「他部署等による監査を実施すること」とありますが、ここで求められる監査の頻度や確認の粒度はどの程度ですか。

Ａ　具体的な頻度等の指定はしていません。自社の状況（事業の規模及び性質、個人データの取扱状況（取り扱う個人データの性質及び量を含む。）、個人データを記録した媒体の性質等に起因するリスクの変化等）に鑑みて、適切に実施してください。

Ｑ２－７　マイナポータル API により直接情報を取得する PHR 事業者は第三者認証が必要となっていますが、データ連携により、間接的に当該情報を取得する PHR 事業者は、第三者認証を取得する必要がありますか。

Ａ　いいえ、ありません。なお、本指針において、PHR 事業者間で健診等情報についてデータ連携する場合についても規定しており、情報を提供する PHR 事業者は、間接的に情報を取得する PHR 事業者が本指針に規定する対策を行っていることを確認することが求められています。

３．個人情報の適切な取扱い

Ｑ３－１　サービス利用規約の概要版の作成は必須ですか。具体的には何を記載しなければなりませんか。

Ａ　特定の内容の記載を義務とするものではなく、サービスの内容によって、利用規約が長大となる場合等に、利用者にとって分かりやすいように、１、２枚程度の概要版の作成を求めるものです。例えば、もともと利用規約が１枚に収まる場合にまで、概要版の作成を求める趣旨ではありません。

Ｑ３－２　「利用目的をできる限り特定し、利用目的及びその範囲等について、例えば、本指針に関する Q&A に示されているような方法により、サービス利用規約の概要を提示するなど、分かりやすく通知した上で、本人の同意を得なければならない。」とありますが、利用目的はどのように記載するのがよいですか。

Ａ　提供するサービス内容に応じて、ユーザーに分かりやすく利用目的を通知してください。例えば、以下のような記載が挙げられます。

・サービスの成果等の公表のための統計分析
・AI（人工知能）の開発及び運用業務のための分析
・利用者に対する健康状態のフォローアップ
・アプリケーションの改善・向上に関する研究
・提供サービス普及のためのマーケティング
・利用目的の範囲での第三者提供

また、PHR 事業者が、人を対象とする医学系研究を行う場合、「人を対象とする生命科学・医学系研究に関する倫理指針」（令和３年文部科学省・厚生労働省・経済産業省告示第１号）及び「人を対象とする生命科学・医学系研究に関する倫理指針ガイダンス」（令和３年４月文部科学省、厚生労働省、経済産業省）をご参照ください。

Ｑ３－３　第三者提供を利用目的として含む場合、同意を取得する際に、提供先ごとに個別に同意の有無を確認しなければなりませんか。もし、同意取得後、提供先が新たに追加された場合は、改めて同意の取得が必要ですか。

Ａ　必ずしも提供先ごとの個別の同意取得まで求めていません。あらかじめ、複数の提供先を含む団体等への第三者提供に関する包括的な同意を取得していれば、その後、提供先に細かな変更があった場合でも、同意の再取得は必要ありません。一方で、当初の同意取得に、将来追加する提供先についての包括的な同意を取得していない場合は、同意の再取得が必要です。

Ｑ３－４　第三者提供を利用目的として含む場合で、提供先における利用目的が大幅に変更となる場合の対応を教えてください。

A　利用目的が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変更となる場合、改めての同意取得が必要です。

Q３－５　「外国にある第三者」にはどのような場合に該当しますか。また、外国サーバーへのデータ保管等委託等を行う場合はどのような対応が必要となりますか。

A　例えば、外資系企業の日本法人が外国にある親会社に個人データを提供する場合は、その親会社は「外国にある第三者」に該当します。その際、原則として、あらかじめ外国にある第三者への提供を認める旨の本人の同意を得る必要があります。その他詳細につきましては、「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）」（平成 28 年 11 月（令和３年 10 月一部改正）、個人情報保護委員会）の「２－２　外国にある第三者」をご参照ください。

また、外国にある第三者に外国サーバーへのデータ保管等委託等を行う場合にも、本指針２．１．「■外部の組織と情報をやり取りする際に、情報の取扱いに関する注意事項について合意を取る」及び「■個人データの取扱いを委託する場合は委託先での安全管理措置を確保する」等の安全管理措置を遵守ください。

Q３－６　「健診等情報以外の個人情報も取り扱う場合には、当該情報についての利用目的の範囲内であることを確認すること」とありますが、「健診等情報以外の個人情報」とはどのような情報ですか。

A　例えば、いわゆるライフログの情報又は PHR サービス以外で取得した本人の生活関連情報等を言います。それらの情報について特定されている利用目的の範囲内で取り扱うことを求めるものです。

Q３－７　利用者による同意状況の確認について、具体的には何をすればよいですか。

A　利用者から問い合わせ等があった場合に、当該利用者が過去にどのような同意を行っていたか（同意した日付を含む。）を確認できるように、記録を残しておいてください。必ずしも過去の同意状況を提示するために新しく機能を追加することを求めているものではなく、機能追加が難しい場合は、メール又は電話等での問い合わせに対応することで構いません。アプリ画面上で利用者が随時、同意状況を確認できる機能等の提供を一律に求めるものではありません。

Q３－８　利用者が同意を撤回した場合、過去に遡って対応しなければなりませんか。既に第三者提供をした情報についても、消去依頼を出さなければなりませんか。

Ａ　いいえ。撤回された以降の個人情報の利用に関して、同意が得られていないものとして対応してください。また、利用者から、個人情報の利用停止や消去の請求があった場合については、３．３（１）①「利用停止請求を受けた場合の対応」、同（２）②「健診等情報の消去」をご参照ください。

なお、個人情報の保護に関する法律（デジタル社会の形成を図るための関係法律の整備に関する法律第 50 条関係）の第 33 条第５項において、原則として第三者提供の記録を本人に開示することが必要とされています。

Ｑ３－９　消去の定義を教えてください。

Ａ　「個人情報の保護に関する法律についてのガイドライン（通則編）」（平成 28 年 11 月（令和３年 10 月一部改正）、個人情報保護委員会）の 3-4-1 の定義、「当該個人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を含む。」と同じです。

Ｑ３-10　令和２年に改正された個人情報保護法により保有個人データの消去が義務化されていますが、本指針における健診等情報の消去は法規制に基づく遵守すべき事項ではないですか。

Ａ　個人情報保護法第 35 条第５項及び第６項では、利用する必要がなくなった場合等で本人から消去の請求のあった場合に消去を求めています。一方、本指針では、本人から消去の請求があった場合のほか、本人からの請求がなくとも健診等情報の利用の必要がなくなった場合にも消去を求めています。

Ｑ３－11　健診等情報の消去を行う場合の留意点を教えてください。

Ａ　利用者のデータを消去する場合は、当該利用者に対して、自身のデータが消去される旨を知らせ、確認を取り、その際、データを消去すると復元できない旨も分かりやすく伝えるのが望ましいと考えます。

Ｑ３－12　「医師又は薬剤師等」の「等」には、医師と薬剤師のほか、どのような者が含まれますか。

Ａ　歯科医師、保健師及び管理栄養士等の医療従事者等の利用者本人以外の者が含まれます。

Ｑ３－13　健診等情報に利用者以外の個人情報（医師又は薬剤師等の氏名等）が含まれていた場合は、必ず消去しなければなりませんか。

Ａ　いいえ。本指針としては、必ずしも消去を求めてはいません。個人情報保護法の規定を遵守することで、一般的な個人情報と同様に取り扱うことが可能です。

Ｑ３－14　健診等情報を匿名加工して第三者に提供することを予定している場合、その旨を利用目的として公表又は本人に通知することは必須ですか。

Ａ　本指針では定めておりませんが、匿名加工情報への加工を行うこと自体を、個人情報の利用目的とする必要はありません。また、匿名加工情報の作成又は第三者提供時は、必要事項を公表する義務があります。その他、匿名加工情報に関しては、匿名加工に関しては、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（仮名加工情報・匿名加工情報編）」（平成 28 年 11 月（令和３年 10 月一部改正）、個人情報保護委員会）等をご参照ください。

Ｑ３－15　PHR 事業者が、人を対象とする医学系研究を行う場合、留意する事項はありますか。

Ａ　健診等情報を取得する場合又は同情報の取得後に当初の利用目的の達成に必要な範囲を超えて利用目的を変更する場合にあっては、どのような目的で健診等情報の分析に利用されるのか、分かりやすく通知した上で、本人の同意を得なければなりません。

また、PHR 事業者が、人を対象とする医学系研究を行う場合、「人を対象とする生命科学・医学系研究に関する倫理指針」（令和３年文部科学省・厚生労働省・経済産業省告示第１号）及び「人を対象とする生命科学・医学系研究に関する倫理指針ガイダンス」（令和３年４月文部科学省、厚生労働省、経済産業省）をご参照ください。

４．健診等情報の保存及び管理並びに相互運用性の確保

Ｑ４－１　４．２．（１）①で、エクスポート機能及びインポート機能の対象とすべき情報について、「マイナポータル API 等」とあるが、この「等」には何が含まれますか。

Ａ　個人が紙媒体等で入手した健診等情報を個人自ら入力する場合等を想定しています。

Ｑ４－２　サービスを終了する場合などに、利用者又は他の PHR 事業者への健診等情報のエクスポート期間として、どの程度の期間が必要ですか。

Ａ　具体的な期間に関して一律に決まっているものではありません。サービスの内容、利用者への通知の状態、利用者と PHR 事業者との近接性、提供されるデータの性質等によって異なるため、サービス開始時に利用者にあらかじめ周知するなど齟齬が生じないように適切な対応を推奨いたします。

５．要件遵守の担保

Ｑ５－１　本指針に準拠していることは、どのように確認されるのですか。

Ａ　各事業者において、チェックシートにより定期的に確認し、その結果をホームページ等で分かりやすく公表する必要があります。

Ｑ５－２　チェックシートの公表は、必ずプライバシーポリシーや利用規約と同じページでないといけませんか。

Ａ　必ずしも「同じ」である必要はありませんが、利用者にとって、それらのページと同程度にアクセスしやすい場所に掲載することが必要です。

Ｑ５－３　今後、政府において、PHR 事業者の情報セキュリティ水準や第三者認証の取得状況を取りまとめて公表する予定はありますか。

Ａ　現時点では想定していません。

６．本指針の見直し

Ｑ６－１　この指針は定期的に見直されますか。具体的な見直し時期は決まっていますか。

Ａ　現段階では、次回の見直しについて具体的な時期等は決まっていません。指針に記載のとおり、個人情報保護法等の法令又はガイドラインの改正、本指針の運用状況及びPHR サービス又はセキュリティ技術等の拡大等の状況の変化を踏まえて、必要に応じて検討及び見直しを行うこととなります。

　なお、基本的指針の見直しがあった場合にはPHR 事業者は、一定の期間内に必要な対応を行い、新たなチェックシートを自社のホームページ等で公表する必要があります。