「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」（案）に対する意見

2021 年３月 12 日
（一社）日本経済団体連合会
イノベーション委員会ヘルステック戦略検討会

PHR は、自分の健康を自分で守るために不可欠な、Society5.0 時代のヘルスケアを実現する基盤であり、個人起点の健康管理・予防・未病対策を行い、個人が健康をデザインできる重要な仕組みとして期待される。民間 PHR が普及すれば、個人が自由に様々な種類の PHR の中から自身の嗜好にあったものを選択できるようになり、継続的な利用が期待できることから、企業が利用者にとって安心・安全な民間 PHR サービスを開発するための環境の整備が必要である。

こうした観点から、本指針（案）に対し、下記のとおり意見を述べる。

記

全般

- PHR の利用は、個別化された効果的な介入等により国民の予防・健康増進が期待されるため、安心・安全な PHR サービスの利活用の促進に向けて、情報の取扱いに関する本指針に加え、PHR の利活用を促進するような制度設計や環境整備の検討も行うことを期待する。

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

① 情報セキュリティに対する組織的な取り組み

- **■ 健診等情報については、入手、作成、利用、保管、交換、提供、消去及び破棄における取扱手順を定める（５ページ）**
- 「破棄」と「廃棄」の表現が混在しているため、意図した使い分けであれば意味の差異を明確にすべきである。意味の差異がないのならば統一が望ましい。

③ 情報システム及び通信ネットワークの運用管理

■ 情報システムの運用に関して運用ルールを策定する

➢ 設備（具体例）の使用状況を記録していること（７ページ）

- 「設備」の定義が不明瞭であり、どのような設備の使用状況を記録すべきか判断が困難であるため、「設備」の定義を明確にするとともに具体例を記載すべきである。

④ 情報システムのアクセス制御並びに情報システムの開発及び保守におけるセキュリティ対策

■ 情報（データ）及び情報システムへのアクセスを制限するために、システム管理者の ID の管理（パスワード等認証情報の管理等）を行う（８ページ）

- 医療情報システムの安全管理に関するガイドラインに準拠し「パスワードによる認証を採用する場合、その定期的な見直しを求めること。」と記載されているが、一般的にはパスワードを定期的に変更する必要はなく、流出時に速やかに変更する方向に進んでおり[1]、総務省のセキュリティ対策ガイドラインにもその旨が記載されている[2]。したがって、定期的な変更を求めない方針に統一すべきである。

⑤ 情報セキュリティ上の事故対応

■ 情報システムに障害が発生した場合、業務を再開するための対応手順を整理する

➢ 障害対策の仕組みが組織として効果的に機能するよう、よく検討していること（９ページ）

- 他項目と比較して抽象的な表現であるため、例えば情報セキュリティマネジメントシステム（ISMS）の確立・実施・維持を指針に含めるなど、検討の水準を具体的に示すことが望ましい。

---

[1] 米国立標準技術研究所（NIST）の認証に関するガイドライン「Electronic Authentication Guideline（電子的認証に関するガイドライン)」第３版（NIST SP 800-63-3）

[2] 総務省　国民のための情報セキュリティサイト
https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/staff/01.html

３．個人情報の適切な取扱い

３．１．情報の公表

３．１．２．利用目的の明示等

（２）本指針に基づく遵守すべき事項

① サービス利用規約およびプライバシーポリシー等の公表（12 ページ）

- 「サービス利用規約の概要版を必要に応じて作成する」の箇所について、具体的にどのような場合を指し示すのか不明瞭であり、事業者による判断が困難である。サービス利用規約の概要版の作成が必要となる場合の具体事例や判断基準を明示すべきである。

３．３．消去及び撤回

（１）法規制に基づく遵守すべき事項

② 利用停止等請求への対応の例外（14 ページ）

- 個人情報保護法および同ガイドラインを踏まえ、PHR サービスに関して、利用停止等請求に対応しなければならない場合の具体事例と判断基準を明示すべきである。
- 加えて、利用停止等が請求された当該保有個人データを含む PHR 情報に基づき、既に導き出された分析や統計情報等の結果の修正は、対応の例外とすることが望ましい。

（２）本指針に基づく遵守すべき事項

② 健診等情報の消去（14 ページ）

- 「その他の消去を行うことが困難な場合」や「本人の権利利益を保護するため必要なこれに代わる措置」という箇所について、具体的にどのような場合、措置を指し示すのか不明瞭であり、事業者による判断が困難である。健診等情報の消去が必要となる場合や、完全消去ではなくマスキング処理で個人情報を見えなくする方法も代替措置と認められるのかなど、認められる代替措置の具体事例と判断基準を明示すべきである。

③ 長期間利用がない場合の措置（14 ページ）

- 本項目は、一定期間に利用がない場合に、当該情報の「消去」を求めるものではなく、仮に消去するのであれば利用者に「通知・公表」することを求めるものと理解する。その趣旨を明確にするために、「利用者によるアクセスがなく、長期間利用されない健診等情報を削除する場合には、本人が認知しないままに、当該情報が削除されることは望ましくないため（以下略）」とすべきである。

４．健診等情報の保存及び管理並びに相互運用性の確保

４．２．相互運用性の確保

（１）本指針に基づく遵守すべき事項

① 利用者を介した相互運用性の確保（16 ページ）

- 学会をはじめとして進められている PHR のデータ項目や電子カルテの標準化に向けた取組みも鑑みた上で、健診等情報のフォーマットや互換性の高い汎用的なデータファイルの幅広い相互運用性を確保することが望ましい。

② サービス終了時の措置（16 ページ）

- 「エクスポートが実施可能な期間」が指し示す期間の長さが不明瞭であり、事業者による判断が困難であるため、具定例や判断基準を明示することが求められる。

５．要件遵守の担保（17 ページ）

- チェックシートによる定期的な確認を PHR 事業者に求めるのであれば、本指針ならびにチェックシートの内容に変更が生じた際、届け出ている PHR 事業者に通知することが必要である。
- 本指針で求められているセキュリティの要件、個人情報の取り扱いのルール等は第三者認証の取得の際に求められる水準と同等であることから、第三者認証の取得およびその公開によってチェックシートの結果公表に代替することを検討すべきではないか。

以　上