３省２ガイドライン
情報システム運用手順書

一般社団法人在宅栄養ケア推進基金

制定：　2024 年 4 月 5 日

■基本的事項

〇本指針の対象とする情報の定義

個人が自らの健康管理に利用可能な「個人情報の保護に関する法律」（平成 15 年法律第 57 号。以下「個人情報保護法」という。）上の要配慮個人情報。

・栄養ケア支援システム（iOsAPP）を用いて、個人から情報入手し、記録を行うものであって、必要に応じて医療機関等に提供する情報。

・健診等情報を取り扱う PHR サービスを提供する民間事業者（以下「PHR 事業者」の対象ではない。

■情報セキュリティ対策

〇安全管理措置

１、法規制に基づく遵守すべき事項

・個人情報保護法に基づく適切な取扱いとして、健診等情報を取り扱うに当たって、その漏えい、滅失又は毀損の防止その他の安全管理のために必要かつ適切な措置を講じる。

２、情報セキュリティに対する組織的な取り組み

・経営者が情報セキュリティポリシーの策定に関与し、実現に対して責任を持ち、定期的に情報セキュリティポリシーを見直すこととする。

・情報セキュリティ対策に関わる責任者を冨田実とし、担当者は中内玲奈とする。責任者は、各セキュリティ対策について（社内外を含め）、責任者及び担当者それぞれの役割を具体化し、役割を徹底する。

３、管理すべき重要な情報資産の区分

・管理すべき健診等情報は、クラウドサーバーに保管し、他の情報資産と区分する。また、情報資産の管理者は冨田実とする。

・重要度に応じた情報資産の取扱指針を定め、健診等情報を取り扱う人の範囲を定める。

４、個人情報の取扱状況を確認する手段

・個人情報データベース：　ウイルネットインターネットサービス（レンタルサーバー）

・個人データの項目：　個人名、生年月日、健診等データ

・責任者/取扱部署：　冨田実（業務執行理事）

・利用目的：　対象者（高齢者）の低栄養予防・フレイル対策に資するアドバイス

・アクセス権限者：冨田実（責任者）、中内玲奈（担当）、栄養ケア支援支援システム契約先の関係者、栄養ケア支援システム IDPW アカウント発行業務委託先（株式会社クロガネコミュニケーションズ）、保守メンテナンス業務委託先（株式会社パシフィックシステム）

５、健診等情報の取扱い手順

・入手方法：契約施設等（保険薬局ほか）が問診等で健診情報等を入手する。

・作成方法：健診情報等を栄養ケア支援システムへ入力し作成する。

・利用方法：高齢者の低栄養予防・フレイル対策に資するアドバイスに用いる。

・保管方法：ウイルネットインターネットサービス社のレンタルサーバーへ補完。

・交換方法：栄養ケア支援システム記録データの電子的交換は行わない。
・提供方法：アセスメントシート（紙面）にて情報提供する。
・消去/破棄方法：栄養ケア支援システム ID/PW 削除によりデータ消去/破棄する。
・漏洩防止/保護対策:アクセス権限者の限定、ログ管理・データ消去/破棄を確実に行う。

６、外部組織との情報の取扱い

・栄養ケア支援システム開発委託先（パシフィックシステム株式会社)、栄養ケア支援システム ID/PW 発行業務/メンテナンス業務委託先（株式会社クロガネコミュニケーションズ)、レンタルサーバー会社（株式会社ウイル）と、情報の取扱い（情報管理、受託情報の取扱い、受け渡し、返却及び廃棄等）について、注意事項を規定する。

７、個人データ委託先での安全管理措置

・自らが講ずべき安全管理措置と同等の措置が講じられるよう、監督を行う。

８、取扱状況の把握、安全管理措置の見直し

・個人データの取扱状況を定期的に自ら行う点検により監査を実施する。

９、従業者に対するセキュリティ対策

・従業者の採用時に、秘密保持（守秘義務）に関する事項を就業規則等に盛り込み、在職中及び退職後の機密保持義務も含む誓約書/雇用契約書を交わし、違反した従業員には懲戒手続きを行う。

１０、情報セキュリティに関するルール周知及び知識習得について

・従業員に対し、情報セキュリティポリシー及び関連規程の知識習得教育を行う。

○物理的セキュリティ

１、 健診等情報の保管場所の入退管理及び施錠管理

・健診等情報の保管区域を定め、侵入者の防止対策（施錠管理・入退室管理）を行う。

２、 自然災害又は人的災害による被害防止対策

・重要なコンピュータは安全な場所に設置し、電源及び通信ケーブルが損壊しない対策を施し、地震等による転倒防止、水漏れ防止等の対策を行う。

３、 重要書類、モバイル PC 及び記憶媒体等の盗難防止対策、紛失対策

・健診等情報を記載した書類が不要になった場合、シュレッダー等により確実に処分する。
・健診等情報書類を保管するキャビネットには、施錠管理を行う。
・健診等情報が存在する机上、書庫及び会議室等は整理整頓を行い、郵便物、FAX 及び印刷物等の放置を禁止し、重要な書類の裏面を再利用しない。

４、 モバイル PC 及び記憶媒体等について

・クラウド上のデータを含め、保存した情報が不要になった場合、消去ソフトを用いて、確実に処分し、モバイル PC 及び記憶媒体については、盗難防止対策及び紛失対策を行い、私有 PC の社内持ち込みを禁止する。

○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ルールの策定

５、 システム運用におけるセキュリティ要求事項を明確にし、情報システムの運用手順書（マニュアル）を整備し、システム操作、障害及びセキュリティ関連イベントのログ（記録）等）の運用状況を点検する。

６、 前項のログ（記録）については、定期的なレビューを行い、不正なアクセス等がないことを確認する。

・ウイルス対策ソフトをはじめとするアプリケーションの運用

１、ウイルス対策ソフトを導入し、パターンファイルの更新を定期的に行い、ウイルス対策ソフトが持っている機能（ファイアウォール機能、スパムメール対策機能及び有害サイト対策機能）を活用し、各サーバ及びクライアントPCの定期的なウイルス検査を実施する。

２、組織で許可されていないソフトウェアのインストール及びサービスの利用をし、PHRサービスの利用者に対して、適切なセキュリティ対策を利用端末に行うよう啓発する。

・情報システムの脆弱性対策

１、情報システムの脆弱性の解消（修正プログラムの適用及びWindows update等）を行い、脆弱性情報及び脅威に関する情報の入手方法を確認し、定期的に収集する。

２、情報システム導入の際には、不要なサービスの停止等、セキュリティを考慮した設定を実施する。

３、Webサイトの公開にあたっては、不正アクセス又は改ざんなどを受けない対策を行い、脆弱性の解消を行い、Webブラウザ及び電子メールソフトのセキュリティ設定を行う。

・通信ネットワークにおける暗号化等の保護策

１、TLS（version1.2以上）等を用いて通信データを暗号化する。

・モバイルPC、USBメモリなどの記憶媒体/データの盗難、紛失対策

１、モバイルPC又はUSBメモリ等の使用や外部持ち出しについて規程を定め、外部でモバイルPC又はUSBメモリ等を使用する場合のパスワード設定等の紛失/盗難対策を講じる。

・外部から受け取るファイルへの対策

１、ファイル無害化ソフトウェア/サービス等を導入し、外部ファイルの無害化を実施する。

○情報システムのアクセス制御並びに開発及び保守におけるセキュリティ対策

・情報システムへのアクセス制限のためのシステム管理者のIDの管理

７、 システム管理者IDの登録及び削除に関する規程を整備し、システム管理者毎にID及びパスワード等を割当て、当該ID及びパスワード等による識別及び認証を確実に行う。

８、 ID・パスワード認証には、容易に類推できないパスワードを設定し、不要になったシステム管理者のID・パスワードは削除する。

９、 離席する際は、パスワード等で保護されたスクリーンセーバーでパソコンを保護する。

・健診等情報に対するアクセス権限の設定

１、健診等情報に対するアクセス管理方針を定め、システム管理者毎にアクセス可能な情報、情報システム、業務アプリケーション及びサービス等を設定し、職務の変更又は異動に際して、システム管理者のアクセス権限を見直す。

・職務の変更又は異動時のシステム管理者のアクセス権限の見直し

１、外部から内部のシステムにアクセスする際、確実な認証を実施し、保護すべき健診等情報のデータベースは、サービス利用者が利用する機能（閲覧等）及び保守点検時のリモート管理機能を除き、外部接続しているネットワークから物理的に遮断する又はセグメント分割することによりアクセスできない対策を実施する。

２、不正なプログラムをダウンロードさせるおそれのあるサイトへのアクセスを遮断する対策を講じる。

・無線 LAN のセキュリティ対策

１、無線 LAN において健診等情報の通信を行う場合は、暗号化通信（WPA2 等）の設定を行い、無線 LAN の仕様を許可する端末及びその使用者の認証を行う。

・情報システムの開発及び保守並びにサービス利用に関する情報セキュリティ管理

１、情報システムの設計時に安全性を確保し、情報システムの脆弱性を突いた攻撃への対策を講ずる等の継続的な見直しを行う。

２、ソフトウェア及びクラウド等の他者が提供するサービスの導入及び変更に関する手順を整備し、本指針のセキュリティ対策の遵守を確認する。

３、外部委託によるソフトウェア/システム開発を行う場合、使用許諾及び知的財産等について取り決め、レビューを実施し、その記録を残し、セキュリティ管理の実施状況を把握する。

○情報セキュリティ上の事故対応

・情報システム障害時の業務再開までの対応手順

１０、 情報システムに障害が発生した場合、最低限運用に必要な時間及び許容停止時間を明確にし、障害対策の仕組みが組織として効果的に機能するよう対策を講じる。

１１、 システムの切り離し（即応処理）、必要なサービスを提供できるような機能（縮退機能）、情報の回復及び情報システムの復旧に必要となる機能等が、障害時に円滑に機能する対策を講じる。

１２、 日常システム運用の中で、バックアップデータ及び運用記録等を確保する。

１３、 障害発生時に必要な対応として、障害発生時の報告要領（電話連絡先の認知等）、障害対策の責任者と対応体制、システム切替え及び復旧手順並びに障害発生時の業務実施要領等を整備し、関係者への障害対応要領の周知、必要なスキルに関する教育及び訓練等の実施を行う。

・情報セキュリティ関連事故等（ウイルス感染、情報漏洩等）への緊急時対応手順

１、ウイルス感染又は情報漏えい等の発生時の組織内の関係者への報告、緊急処置の適用基準及び実行手順、被害状況の把握、原因の把握、対策の実施、被害者ほか影響を受ける可能性のある本人への通知、外部への周知方法、個人情報保護委員会への報告、通常システムへの復旧手順並びに業務再開手順等を整備する。

２、情報漏洩事実を確認した際は、速やかに責任者に報告し、5W1H の観点で調査し情報を整理した上で、対策本部で対応方針を決定し、被害の拡大防止と復旧のための措置を行う。

３、情報漏洩の場合、漏洩した個人情報の本人及び取引先等への通知、個人情報保護委員会及

び監督官庁等への報告並びにホームページ又はマスコミ等による公表について検討する。

■個人情報の適切な取り扱い

〇情報の公表・利用目的の特定：

・健診等情報の取扱い目的は、高齢者の低栄養予防・フレイル対策事業に特定する。

・具体的には、保険薬局で栄養ケア支援システムを用いて、低栄養チェック・アドバイスを行い、栄養アセスメント結果をアウトプットして、対象者（高齢者）に低栄養予防の気付きを与える。必要に応じて、栄養アセスメント結果を保険薬局のトレーシングレポートに付記して、主治医へ情報提供する場合もある。また、公民連携事業（医福食農連携による高齢者の低栄養予防事業）に前述の作業を行う場合もある。

・利用目的の変更は行わない。また、対象者（高齢者）に利用目的を示し、同意取得する。

〇利用目的の明示

・直接本人から健診等情報を取得する場合には、あらかじめ、本人に対し、その利用目的を明示した説明文書で説明する。

・事業の性質及び健診等情報の取扱状況についても、内容が本人に認識されるよう説明文書を用いて説明する。

〇保有する健診等情報等の本人への開示

・本人からの要求があった場合、保有する当該本人に係る健診等情報（保有個人データ）を開示する。

〇サービス利用規約及びプライバシーポリシー等の公表

・利用者及び第三者が当該 PHR 事業者の取組について評価できるよう、プライバシーポリシー及びサービス利用規約をホームページ等に掲載する。

・サービス利用規約の概要版を必要に応じて作成するとともに、ホームページのアクセスしやすい場所に掲載するなど分かりやすく公表する。

〇取得に係る事前の同意取得等

・健診等情報のうち要配慮個人情報を取得する際、あらかじめ、本人からの同意を取得する。

・当初の利用目的の達成に必要な範囲を超えて健診等情報を取り扱う場合（事業の承継後に、承継前の当初の利用目的の達成に必要な範囲を超えて、健診等情報を取り扱う場合を含む）は、あらかじめ本人の同意を得ることとする。

〇第三者提供に係る事前の同意取得

・第三者提供の同意の取得に当たっては、事業の規模及び性質並びに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すこととする。

・共同利用の場合、あらかじめ、次に掲げる事項を本人に通知又は本人が容易に知り得る状態にする。（共同利用をする旨 / 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 / 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及び住所並びに法人にあっては、その代表者の氏名）

〇健診等情報取得に係る同意取得時の利用目的の通知

・健診等情報の取得に際しては、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、

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、本人の同意を得る。

・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。

〇第三者提供に係る事前の同意取得

・健診等情報の第三者提供に際しては、提供先、その利用目的（必要に応じてその概要を提示する）及び提供される個人情報の内容等を特定し、分かりやすく通知した上で、本人の同意を得る。

・第三者提供の同意があった場合でも、本人の不利益が生じないよう配慮する。

〇利用者による同意状況の確認

・過去の同意状況を利用者が確認できる方策を確保する。

〇消去・撤回：利用停止等請求を受けた場合の対応

・本人から、当該本人が識別される保有個人データが、本人の同意なく健診等情報が取得された、目的外利用がされている、違法若しくは不当な行為を助長する等の不適正な方法により個人情報が利用されている、又は偽りその他不正の手段により取得された、事業者が利用する必要がなくなった、漏えい等事案が生じた、又は当該本人の権利若しくは正当な利益が害されるおそれがある、という理由によって、当該保有個人データの利用の停止又は消去の請求を受けた場合であって、その請求に理由があることが判明したときは、遅滞なく、利用停止等の措置を行う。

・上記の措置を講じることが困難な場合、本人の権利利益を保護するために代替措置をとる。

〇同意の撤回

・健診等情報の取得時及び第三者提供時の当該同意の撤回について、同意する際と同程度の容易さで行えるよう務める。

〇健診情報等の消去

・事業終了等により健診等情報の利用の必要がなくなった場合又は本人の求めがあった場合、自社が管理している健診等情報（管理を委託している場合を含む。）を消去する。

・上記の措置を講じることが困難な場合、本人の権利利益を保護するために代替措置をとる。

〇長期間利用がない場合の措置

・一定の期間、利用がない場合に消去等の措置を講じる旨（消去を行う時期等を含む。）を利用者に通知又は公表する。

〇健診等情報に含まれる利用者以外の個人情報の取扱い

・医師又は薬剤師等の氏名等は、要配慮個人情報には該当しないものの、医師又は薬剤師等の個人情報に該当することに留意し、利用目的の特定、同意の取得等に関して、個人情報保護法に基づき適切に取り扱う。

〇個人関連情報に関する留意事項

・第三者が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、当該第三者が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本人の同意が得られていることをあらかじめ確認する。

・第三者から個人関連情報の提供を受けて個人データとして取得するときは、当該第三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本人の同意をあらかじめ得ることとする。

○仮名加工情報に関する留意事項

・仮名加工情報を作成するときは、個人情報保護委員会規則で定める基準に従い当該個人情報を加工し、仮名加工情報の作成に用いた個人情報から削除した記述等及び加工方法の安全管理のための措置を講じ、利用目的を公表する。

・当該仮名加工情報は、法令に基づく場合を除くほか、第三者に提供しない。

○匿名化に関する留意事項

・匿名加工情報を作成するときは、個人情報保護委員会規則で定める基準に従い当該個人情報を加工し、匿名加工情報の作成に用いた個人情報から削除した記述等及び加工方法の安全管理のための措置を講じ、当該匿名加工情報に含まれる個人に関する情報の項目を公表する。

・当該匿名加工情報を第三者に提供するときは、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するとともに、第三者に対して、当該提供に係る情報が匿名加工情報である旨を明示する。

■健診等情報の保存及び管理並びに相互運用性の確保

○正確性の確保

・個人情報データベース等への個人情報の入力時の照合及び確認の手続を整備する。

・誤り等を発見した場合の訂正等の手続を整備する。

・記録事項の更新及び保存期間を設定する。

○第三者提供の記録

・健診等情報を第三者に提供する場合は、提供した年月日及び提供先等に関する記録を作成する。

・当該記録については、一定期間保存する。

・第三者提供を受けた場合、提供を受けた年月日及び提供元等に関する記録を作成し、一定期間保存する。

・本人からの請求があった場合、保有する健診等情報の第三者提供の記録を開示する。

○データ連携先事業者の適切性の確認

・PHR 事業者間で健診等情報を利用者を介さず直接的にデータ連携する場合、データ連携先事業者が本指針に規定する対策を行っていることを、当該データ連携先事業者のホームページ等での公表内容又は第三者認証の取得状況等により確認する。

■要件遵守の担保

○自主的な確認及びその結果の公表

・3 省 2 ガイドライン・チェックシートの確認事項に従って各要件を満たしているかどうかを定期的に確認する。

・3 省 2 ガイドライン・チェックシートによる確認結果を、サービス利用規約及びプライバシーポリシー等を公表しているページと同じページ等で公表する。

・公表する際に、結果の概要を分かりやすい表現で記載する。