第５回 介護情報利活用ワーキンググループ	資料５
令和５年４月５日	

厚生労働省 ひと、くらし、みらいのために Ministry of Health, Labour and Welfare

安全管理措置について

厚生労働省 老健局

Ministry of Health, Labour and Welfare of Japan

主体ごとに参照すべき安全管理措置に係る主な規定について

- 介護情報や医療情報を保有する主体ごとに参照すべき、安全管理措置に係る主な規定は以下のとおり。
- 特に介護事業所では、医療情報を扱う場合には医療機関と同様に、「医療情報システムの安全管理に関するガイドライン」も参照する必要がある。

	介護事業所	医療機関	自治体
①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	○	○	
②医療情報システムの安全管理に関するガイドライン	△ （医療情報を扱う場合）	○	
③個人情報の保護に関する法律についてのガイドライン（行政機関等編）			○

（参考）介護事業所が医療情報システムの安全管理に関するガイドラインを遵守する場合について
（「医療情報システムの安全管理に関するガイドライン 第5.2版」に関するQ＆A（令和４年４月）より抜粋）

Q－5 どのような場合に、介護事業者は本ガイドラインの内容を遵守する必要があるか。
A 本編3.1 章を踏まえて、下記のような事例等が想定されます。

- 介護事業者が取り扱うe-文書法の対象範囲となる文書に、医師等から提供を受けた患者の医療情報を記入し、電子保存を行う場合。別冊3.1 章に、医療情報が含まれることがある介護事業者の文書が例示されているため、ご参照ください。
- 上記のほか、医師等が作成した患者の医療情報を情報システムにより取り扱う場合。

医療機関及び介護事業所が講ずるべき安全管理措置等について
（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より抜粋）

■ 個人情報保護法第23条～第25条の規定により、以下のような安全管理措置等を講じなければならないとされている。

①安全管理措置

- 医療・介護関係事業者は、その取り扱う個人データの漏えい、滅失又は毀損の防止その他の個人データの安全管理のため、組織的、人的、物理的、及び技術的安全管理措置等を講じなければならない。

②従業者の監督

- 医療・介護関係事業者は、①の安全管理措置を遵守させるよう、従業者に対し必要かつ適切な監督をしなければならない。なお、「従業者」とは、医療資格者のみならず、当該事業者の指揮命令を受けて業務に従事する者全てを含むものであり、また、雇用関係のある者のみならず、理事、派遣労働者等も含むものである。
- 医療法第１５条では、病院等の管理者は、その病院等に勤務する医師等の従業者の監督義務が課せられている。（薬局や介護関係事業者についても、医薬品医療機器等法や介護保険法に基づく各種サービスに関する人員、設備及び運営に関する基準（以下「指定基準」という。）等に同様の規定あり。）

参考：個人情報保護法第23条～第25条

（安全管理措置）

第二十三条　個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又は毀損の防止その他の個人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。

（従業者の監督）

第二十四条　個人情報取扱事業者は、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。

（委託先の監督）

第二十五条　個人情報取扱事業者は、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。

（参考）安全管理措置として考えられる事項（１／２）
（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より抜粋）

■ 事業所の規模や従業者の様態等を勘案して、以下のような取組を参考に、必要な措置を行うものとされている。

①個人情報保護に関する規程の整備、公表

- 医療・介護関係事業者は、保有個人データの開示手順を定めた規程その他個人情報保護に関する規程を整備し、苦情への対応を行う体制も含めて、院内や事業所内等への掲示やホームページへの掲載を行うなど、患者・利用者等に対して周知徹底を図る。
- また、個人データを取り扱う情報システムの安全管理措置に関する規程等についても同様に整備を行うこと。

②個人情報保護推進のための組織体制等の整備

- 従業者の責任体制の明確化を図り、具体的な取組を進めるため、医療における個人情報保護に関し十分な知識を有する管理者、監督者等（例えば、役員などの組織横断的な監督が可能な者）を定める。又は個人情報保護の推進を図るための部署、若しくは委員会等を設置する。
- 医療・介護関係事業所で行っている個人データの安全管理措置について定期的に自己評価を行い、見直しや改善を行うべき事項について適切な改善を行う。

③個人データの漏えい等の問題が発生した場合等における報告連絡体制の整備

- １）個人データの漏えい等の事故が発生した場合、又は発生の可能性が高いと判断した場合、２）個人データの取扱いに関する規程等に違反している事実が生じた場合、又は兆候が高いと判断した場合における責任者等への報告連絡体制の整備を行う。
- 個人データの漏えい等の情報は、苦情等の一環として、外部から報告される場合も想定されることから、苦情への対応を行う体制との連携も図る。

④雇用契約時における個人情報保護に関する規程の整備

- 雇用契約や就業規則において、就業期間中はもとより離職後も含めた守秘義務を課すなど従業者の個人情報保護に関する規程を整備し、徹底を図る。なお、特に、医師等の医療資格者や介護サービスの従事者については、刑法、関係資格法又は介護保険法に基づく指定基準により守秘義務規定等が設けられており、その遵守を徹底する。

⑤従業者に対する教育研修の実施

- 取り扱う個人データの適切な保護が確保されるよう、従業者に対する教育研修の実施等により、個人データを実際の業務で取り扱うこととなる従業者の啓発を図り、従業者の個人情報保護意識を徹底する。
- この際、派遣労働者についても、「派遣先が講ずべき措置に関する指針」（平成１１年労働省告示第１３８号）において、「必要に応じた教育訓練に係る便宜を図るよう努めなければならない」とされていることを踏まえ、個人情報の取扱いに係る教育研修の実施に配慮する必要がある。

（参考）安全管理措置として考えられる事項（２／２）
（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より抜粋）

■ 事業所の規模や従業者の様態等を勘案して、以下のような取組を参考に、必要な措置を行うものとされている。

⑥物理的安全管理措置
- 個人データの盗難・紛失等を防止するため、以下のような物理的安全管理措置を行う。
  - 入退館（室）管理の実施
  - 盗難等に対する予防対策の実施（例えば、カメラによる撮影や作業への立会い等による記録又はモニタリングの実施、記録機能を持つ媒体の持込み・持出しの禁止又は検査の実施等）
  - 機器、装置等の固定など物理的な保護
- 不正な操作を防ぐため、業務上の必要性に基づき、以下のように、個人データを取り扱う端末に付与する機能を限定する。
  - スマートフォン、パソコン等の記録機能を有する機器の接続の制限及び機器の更新への対応

⑦技術的安全管理措置
- 個人データの盗難・紛失等を防止するため、個人データを取り扱う情報システムについて以下のような技術的安全管理措置を行う。
  - 個人データに対するアクセス管理（ＩＤやパスワード等による認証（※）、各職員の業務内容に応じて業務上必要な範囲にのみアクセスできるようなシステム構成の採用等）
    ※認証については、認証の３要素である「記憶」、「生体情報」、「物理媒体」のうち、２つの独立した要素を組み合わせて認証を行う方式（二要素認証）を採用することが望ましい。
  - 個人データに対するアクセス記録の保存
  - 不正が疑われる異常な記録の存否の定期的な確認
  - 個人データに対するファイアウォールの設置
  - 情報システムへの外部からのアクセス状況の監視及び当該監視システムの動作の定期的な確認
  - ソフトウェアに関する脆弱性対策（セキュリティパッチの適用、当該情報システム固有の脆弱性の発見及びその修正等）

⑧個人データの保存
- 個人データを長期にわたって保存する場合には、保存媒体の劣化防止など個人データが消失しないよう適切に保存する。
- 個人データの保存に当たっては、本人からの照会等に対応する場合など必要なときに迅速に対応できるよう、インデックスの整備など検索可能な状態で保存しておく。

⑨不要となった個人データの廃棄、消去
- 不要となった個人データを廃棄する場合には、焼却や溶解など、個人データを復元不可能な形にして廃棄する。
- 個人データを取り扱った情報機器を廃棄する場合は、記憶装置内の個人データを復元不可能な形に消去して廃棄する。
- これらの廃棄業務を委託する場合には、個人データの取扱いについても委託契約において明確に定める。

（参考）介護事業所におけるセキュリティについて
（介護サービス事業所におけるICT機器・ソフトウェア導入に関する手引きver.２より抜粋）

「４． 導入するICT 機器・ソフトウェアのセキュリティ上の課題と対策について」より一部抜粋

- 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（以下、「個人情報ガイダンス」という。）に示されているとおり、介護サービス事業所は多数の利用者やその家族について他人が容易には知り得ないような個人情報を詳細に知りうる立場にあり、個人情報の適切な取扱いが求められています。

- 個人情報ガイダンスが対象としている介護事業者の範囲は、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（以下「介護関係事業者」という。）であり、いずれについても、個人情報保護に関する他の法律や条例が適用される、国、地方公共団体、独立行政法人等が設置するものを除きます。（（いずれについても、個人情報保護に関する他の法律や条例が適用される、国、地方公共団体、独立行政法人等が設置するものを除きます。国、地方公共団体、独立行政法人については、別途、公的部門のガイドラインを参照する必要があります。ただし、医療・介護分野における個人情報保護の精神は同一であることから、これらの事業者も個人情報ガイダンスに十分配慮することが望ましいとされています。）

- 個人情報ガイダンスでは、介護関係事業者における個人情報の例として、ケアプラン、介護サービス提供にかかる計画、提供したサービス内容等の記録、事故の状況等の記録等を挙げています。

医療情報を取り扱う場合に求められる事項の例（１／４）
（医療情報システムの安全管理に関するガイドライン第5.2版　本編より抜粋）

■ 医療情報を取り扱う場合、以下のような対応を行うことが求められる。

方針の制定と公表

1. 個人情報保護に関する方針を策定し、公開すること。
2. 医療情報システムの安全管理に関する方針を策定すること。その方針には、次に掲げる事項を定めること。
    - 理念（基本方針と管理目的の表明）
    - 医療情報システムで扱う情報の範囲
    - 情報の取扱いや保存の方法及び期間
    - 不要・不法なアクセスを防止するための利用者識別の方法
    - 医療情報システム安全管理責任者
    - 苦情・質問の窓口

医療情報を取り扱う場合に求められる事項の例（２／４）
（医療情報システムの安全管理に関するガイドライン第5.2版　本編より抜粋）

■ 医療情報を取り扱う場合、以下のような対応を行うことが求められる。

組織的安全管理対策（体制、運用管理規程）

1. 医療情報システム安全管理責任者を設置するとともに、医療情報システム運用担当者を限定すること。ただし、小規模医療機関等で役割が自明の場合は、明確な規程を定めなくとも良い。
2. 個人情報が参照可能な場所においては、来訪者の記録・識別、入退制限等の入退管理を定めること。
3. 医療情報システムへのアクセス制限、記録、点検等を定めたアクセス管理規程を作成すること。
4. 個人情報の取扱いを委託する場合、委託契約において安全管理に関する条項を含めること。
5. 運用管理規程等において次の内容を定めること。
    - 医療機関等の体制
    - 契約書・マニュアル等の文書の管理方法
    - リスクに対する予防措置、発生時の対応の方法
    - 機器を用いる場合は機器の管理方法
    - 個人情報の記録媒体の管理（保管・授受等）の方法
    - 患者等への説明と同意を得る方法
    - 監査
    - 苦情・質問の受付窓口

医療情報を取り扱う場合に求められる事項の例（３／４）
（医療情報システムの安全管理に関するガイドライン第5.2版　本編より抜粋）

■ 医療情報を取り扱う場合、以下のような対応を行うことが求められる。

物理的安全対策

1. 個人情報が保存されている機器の設置場所及び記録媒体の保存場所には施錠すること。
2. 個人情報を入力・参照できる端末が設置されている区画は、業務時間帯以外は施錠するなど、運用管理規程等に基づき許可された者以外の者が立ち入ることができないようにするための対策を実施すること。ただし、上記の対策と同等レベルの他の対策がある場合はこの限りではない。
3. 個人情報が保存されている機器が設置されている区画への入退管理を実施すること。
4. 例えば、次に掲げる対策を実施すること。
   - 入退者に名札等の着用を義務付ける。
   - 台帳等によって入退者を記録する。
   - 入退者の記録を定期的にチェックし、妥当性を確認する。
5. 個人情報が保存されている機器等の重要な機器に盗難防止用チェーン等を設置すること。
6. 個人情報が入力・参照できる端末の覗き見防止対策を実施すること。

医療情報を取り扱う場合に求められる事項の例（４／４）
（医療情報システムの安全管理に関するガイドライン第5.2版　本編より抜粋）

■ 医療情報を取り扱う場合、以下のような対応を行うことが求められる。

人的安全対策

医療機関等の管理者は、個人情報の安全管理に関する施策が適切に実施されるよう措置するとともにその実施状況を監督するため、以下の措置をとること。

1. 従業者に対する人的安全管理措置
   ① 法令上の守秘義務のある者以外の者を従業者等として採用するに当たって、雇用契約に守秘・非開示に関する条項を含める等の安全管理対策を実施すること。
   ② 従業者に対し個人情報の安全管理に関する教育訓練を定期的に実施すること。
   ③ 従業者の退職後の個人情報保護規程を定めること。

2. 事務取扱受託業者の監督及び守秘義務契約
   ① 医療機関等の事務、運用等を外部の事業者に委託する場合は、個人情報保護のため、次に掲げる対策を実施すること。
      a 受託する事業者に対する罰則を定めた就業規則等で裏付けられた包括的な守秘契約を締結すること。
      b 保守作業等の医療情報システムに直接アクセスする作業の際には、作業者、作業内容及び作業結果を確認すること。
      c 清掃等の直接医療情報システムにアクセスしない作業の場合でも、作業結果を定期的に確認すること。
      d 受託する事業者が再委託を行うか否かを明確にすること。受託する事業者が再委託を行う場合は、受託する事業者と同等の個人情報保護に関する対策及び契約がなされることを条件とすること。
   ② (ソフトウェアの異常等でデータを救済する必要があるとき等、やむを得ない事情で受託する事業者の保守要員が医療情報にアクセスする場合は、罰則のある就業規則等で裏付けられた守秘契約等の秘密保持の対策を行うこと。

（参考）介護事業者が取り扱う文書等のうち、医療情報システムの安全管理に関するガイドラインの対象となりうるもの
（医療情報システムの安全管理に関するガイドライン第5.2版　別冊編より抜粋）

■ 介護事業者が取り扱う下記文書等は、e-文書法の対象範囲かつ医療情報が含まれることがあり、その場合、ガイドラインの「7 電子保存の要求事項について」、及び「9 診療録等をスキャナ等により電子化して保存する場合について」の対象となる。

- 訪問看護計画書及び訪問看護報告書
- 短期入所療養介護計画
- 特定施設サービス計画
- 施設サービス計画
- 訪問看護記録書、訪問看護指示書、特別訪問看護指示書、精神科訪問看護指示書、精神科特別訪問看護指示書、在宅患者訪問点滴注射指示書、訪問看護計画書及び訪問看護報告書
- 介護予防訪問看護計画書及び介護予防訪問看護報告書
- 介護予防短期入所療養介護計画
- 介護予防特定施設サービス計画
- 定期巡回・随時対応型訪問介護看護計画及び訪問看護報告書
- 療養通所介護計画
- 地域密着型特定施設サービス計画
- 地域密着型施設サービス計画
- 居宅サービス計画、看護小規模多機能型居宅介護計画及び看護小規模多機能型居宅介護報告書

（注）上記は、医療情報が含まれることがある介護事業者の文書の例示。
上記のほか、医師等が作成した患者の医療情報を情報システムにより取り扱う場合も医療情報システムの安全管理に関するガイドラインを遵守する必要がある。

自治体が講ずるべき安全管理措置等について
（個人情報の保護に関する法律についてのガイドライン（行政機関等編）より抜粋）

■ 個人情報保護法第66条の規定により、以下のような安全管理措置等を講じなければならないとされている。

- 行政機関の長等は、保有個人情報の漏えい、滅失又は毀損（以下「漏えい等」という。）の防止その他の保有個人情報の安全管理のため、必要かつ適切な措置（以下「安全管理措置」という。）を講じなければならない（法第66条第1項）。
- 安全管理措置の内容としては、例えば、保有個人情報にアクセスする権限を有する職員の範囲や権限の内容を業務に必要な最小限の範囲に限定する、あるいは保有個人情報が記録された媒体を保管する場所を定めた上で施錠等を行うといった対応が考えられる。
- とりわけ、大量の保有個人情報を取り扱う行政機関等や、取り扱う保有個人情報の性質等に照らして漏えい等が生じた場合に本人の権利利益が侵害される危険が大きい行政機関等においては、本ガイドライン（5-3-1（安全管理措置））その他委員会が示す資料等を参照の上、安全管理措置を確実に講じることが求められる。
- 求められる安全管理措置の内容は、保有個人情報の漏えい等が生じた場合に本人が被る権利利益の侵害の大きさを考慮し、事務又は業務の規模及び性質、保有個人情報の取扱状況（取り扱う保有個人情報の性質及び量を含む。）、保有個人情報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。
- また、デジタル化が進むなか、安全管理措置を適切に講じるためには、サイバーセキュリティの確保も重要である。サイバーセキュリティ対策を講ずるに当たっては、サイバーセキュリティ基本法（平成26年法律第104号）第26条第1項第2号に掲げられたサイバーセキュリティに関する対策の基準等を参考として、取り扱う保有個人情報の性質等に照らして適正な水準を確保する必要がある。

安全管理措置に関する論点について

■ 介護情報の共有に当たって講ずるべき安全管理措置について、以下の論点についてどう考えるか。

（＊）前回のWGにおいて提示したとおり、安全管理措置については調査研究事業等において、課題整理を行った上で、検討する方針としたところ。

- 介護情報基盤を介して電子的に介護情報や医療情報を共有する場合、介護事業所や医療機関が、従前の安全管理措置に加えて講ずるべき対応はあるか。

- 介護情報基盤を介して電子的に介護情報や医療情報を共有する場合、自治体が講ずるべき安全管理措置についてどのように考えるか。