乙第７２号証

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

令和４年３月

厚生労働省

改定履歴

版数	日付
第1版	平成17年3月
第2版	平成19年3月
第3版	平成20年3月
第4版	平成21年3月
第4.1版	平成22年2月
第4.2版	平成25年10月
第4.3版	平成28年3月
第5版	平成29年5月
第5.1版	令和3年1月
第5.2版	令和4年3月

【目次】

1. はじめに

本ガイドラインは、医療情報システムの安全管理や「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律」（平成16年法律第149号。以下「e-文書法」という。）への適切な対応を行うため、技術的及び運用管理上の観点から所要の対策を示したものである。ただし、医療情報の適切な取扱いの観点からは、医療情報システムに関わる対策のみを実施するだけで十分な措置が講じられているとは言い難い。したがって、本ガイドラインを使用する場合、医療情報システムの担当者であっても、「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」を十分理解し、医療情報システムに関わらない部分でも医療情報の適切な取扱いのための措置が講じられていることを確認することが必要である。

本ガイドラインは、病院、一般診療所、歯科診療所、助産所、薬局、訪問看護ステーション、介護事業者、医療情報連携ネットワーク運営事業者等（以下「医療機関等」という。）における電子的な医療情報の取扱いに係る責任者を対象とし、理解のしやすさを考慮して、現状で選択可能な技術にも具体的に言及した。したがって、本ガイドラインは技術的な記載の陳腐化を避けるために定期的に内容を見直す予定である。本ガイドラインを利用する場合は最新の版であることに十分留意すること。

第2版から第5.1版までの改定概要については別冊に掲載。

改定概要

【第 5.2 版】

本ガイドライン第 5.1 版の公表以降、医療等分野及び医療情報システムに対するサイバー攻撃が一層、多様化・巧妙化が進み、医療機関等における診療業務等に大きな影響が生じる被害も見られる。特にランサムウェアに代表される攻撃への対策は、喫緊の課題となっている。そのほか本ガイドラインを踏まえた対策を医療機関等が行う重要性が高まっている。

そのため、本ガイドラインについての理解をより促す観点から、安全対策として実施すべき内容に直接関係する部分と、安全対策を行う上での背景となる考え方や例示などの部分を分けて記述した。具体的には、利用用途に応じて閲覧しやすいように本編と別冊とに分冊化を行った。

ランサムウェア対策との関係では、6.10 章において、ランサムウェアによる攻撃への対応としてのバックアップのあり方等の対策を示した。また適切なリスク分析を行い、被害に遭った際の対策を速やかに講じられるよう、6.2 章において、医療情報システムに関する全体構成図（ネットワーク構成図、システム構成図等）、及びシステム責任者一覧（設置事業者等含む）を整備する旨について示した。

医療機関等が利用する医療情報システムにおいて外部サービスとの連携が進む中で、アプリケーション間の安全性を確保する観点から、6.5 章において外部アプリケーションとの連携における利用者の認証・認可に関する記述を示した。

本ガイドラインにおいて、従来から利用が認められているシステムやサービスの利用形態に関して、これらの利用が安全に管理されている状況下で利用が可能であることを、改めて示すよう、一部記述の追記等を行った。具体的には、BYOD については安全に管理されている環境下での利用について、6.9 章において具体的な記述を行った。また外部ネットワークを利用する上で医療機関等が負うべき管理内容を明示した。

電子署名については、リモート署名や立会人型電子署名など新たな利用形態が普及しつつあることを踏まえて、電子署名に関する 6.12 章の記載を整理した。具体的には、文書の作成者に資格が必要な場合に求められる署名についての要件等について示した。

その他関係制度の変更等に伴う修正を行った。電子署名が求められる文書の長期保存に必要なタイムスタンプについて、総務大臣の認定制度が創設されたことに伴う修正を 6.12 章において行った。併せて、電子署名に用いる暗号アルゴリズムの参照規格について、実務の状況を勘案して、JIS から ISO に参照規格を変更する旨を 6.12 章に示した。また外部保存を行う際の事業者の選定に関して、「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」（総務省・経済産業省　令和 2 年 8 月 21 日）における基準に揃えて 8.3 章の変更を行った。

その他、分かりやすさや表現の平仄を合わせる観点から、一部構成を修正した。

2. 本ガイドラインの読み方

本ガイドラインは本編において、医療機関等において実施すべき内容を示し、別冊でその考え方や、具体的な対応例などを示す形としている。医療機関等において、医療情報システムの安全対策上、求められる内容は本編において確認し、具体的な対策を検討するに際して、本編で述べた内容の考え方や具体例などを別冊において確認すること。本編においては次のような構成になっている。医療機関等の管理者、医療情報システム安全管理責任者及び医療機関等から業務を受託する事業者が、それぞれ関連する箇所を理解した上で、必要な対策を実施することを期待する。

なお、本ガイドラインでは、医療情報、医療情報システムという用語を用いているが、これは医療に関する患者情報（個人識別情報）を含む情報及びその情報を扱うシステムという意味で用いている。

【1章～6章及び10章】

医療情報を扱う全ての医療機関等が参照すべき内容を含んでいる。

【7章】

保存義務のある診療録等を電子的に保存する場合に参照すべき内容を含んでいる。

【8章】

保存義務のある診療録等を電子媒体により外部保存する場合に参照すべき内容を含んでいる。

【9章】

e-文書法に基づいてスキャナ等により電子化して保存する場合の指針を含んでいる。

なお、本ガイドラインの大部分は法律、厚生労働省通知、他の指針等の要求事項に対応する対策を示すことを目的としており、そのような部分では概ね、以下の項に分けて説明している。

A. 制度上の要求事項

法律、厚生労働省通知、他の指針等の要求事項を記載している。

B. 考え方

要求事項の解説及び原則的な対策方針について記載している。

C. 最低限のガイドライン

A 項の要求事項を満たすために必ず実施しなければならない対策を記載している。ただし、医療機関等の規模により実際に必要な対策が異なる場合や、幾つかの対策の中の一つを選択する場合もあるため、付表の運用管理表を活用し、適切な対策を採用して、実施しなければならない。

D. 推奨されるガイドライン

実施しなくても A 項の要求事項を満たすことが可能であるが、説明責任の観点から実施した方が理解を得やすい対策を記載している。

また、最低限のシステムには使用されていない技術を使用する上で一定の留意が必要な事項の記載も含んでいる。

なお、別紙の 3 つの付表は、安全管理上要求事項を満たすための技術的対策と運用的対策の関係を要約したもので、運用管理規程の作成に活用されることを期待して作成した。安全管理対策は技術的対策と運用的対策の両面でなされて初めて有効なものとなるが、技術的対策には複数の選択肢があることが多いため、付表を活用して、採用した技術的対策に相応した運用的な対策を実施すること。なお、付表は以下の項目で構成している。

1. 運用管理項目：安全管理上の要求事項で多少とも運用的対策が必要な項目
2. 実施項目：上記管理項目を実施レベルに細分化したもの
3. 対象：医療機関等の規模の目安
4. 技術的対策：技術的に可能な対策（一つの実施項目に対して選択可能な対策を列挙した）
5. 運用的対策：上記 4. の技術的対策を行った場合に必要な運用的対策の要約
6. 運用管理規程文例：運用的対策を規程に記載する場合の文例

各医療機関等は、実施項目に対して採用した技術的対策に応じ、必要な運用的対策を運用管理規程に含め、実際に規程が遵守されていることを確認することで、実施項目を達成することが可能となる。また、技術的対策を選択する前に、それぞれの運用的対策を検討することで、各医療機関等で運用可能な範囲の技術的対策を選択することも可能となる。一般に運用的対策の比重を大きくすれば医療情報システムの導入コストは下がるが、技術的対策の比重を大きくすれば利用者の運用的な負担は軽くなる。運用的対策と技術的対策について適切なバランスを求めることは非常に重要なので、運用的対策及び技術的対策の選択に、これらの付表が活用されることを期待する。