参考資料１

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

令和４年１月１９日

医療情報システムの安全管理に関するガイドライン改定について

厚生労働省 医政局研究開発振興課
医療情報技術推進室

Ministry of Health, Labour and Welfare of Japan

Ministry of Health, Labour and Welfare of Japan

今回対応した論点、対応方針及び対応状況（厚生労働省案）

ひと、くらし、みらいのために

厚生労働省
Ministry of Health, Labour and Welfare

「医療情報システムの安全管理に関するガイドライン」の改定に当たり
1 今回対応した論点、対応方針及び対応状況（厚生労働省案）（1/5）

◆ 今回改定対象とする論点につき、第３回作業班の議論を踏まえて、整理したものを以下に示す。

論点抽出カテゴリ	論点	論点の背景	対応方針（案）	対応状況	対応ページ ①5.1版からの見え消し ②5.2版本体 ③5.2版別冊
医療情報システム全般	制度的要求事項の明確化	◆「健康・医療・介護情報利活用検討会 医療等情報利活用ワーキンググループ（第7回）」において、「本ガイドラインの記載は、制度的な要求事項を主とし、技術的な記載や措置は例示として分けて整理すること、特に、ISMSの実践（リスク分析の結果）にもとづき、適用する安全対策が変わること（必ずしも例示の全てを求めるものではないこと）を分かりやすく記載することが必要ではないか。」とあり、所要の対応が求められる。	◆5.1版では6.2章C項6において「リスク分析により得られたリスクに対して、6.3 章～6.12 章に示す対策を実施すること。」と示しており、安全管理ガイドラインにおける対策が、リスク分析を踏まえたものであることをわかりやすく示す。 ◆B項については、全体的に例示的な部分や解説的な部分については、別冊に移動し、C項の安全対策に直接関係するものを中心とする。	○	①P44 ②P18 ③P32
4.3章関係	医療情報連携ネットワークの情報連携の類型	◆医療情報連携ネットワークを通じた情報提供は、第三者提供型を想定して4.3章は記述されているが、共同利用型も想定される。	◆地域医療連携の患者情報交換で共同利用ができる可能性について、ガイドライン、ＱＡに示す。	○	①P26 ②P9 ③P20 Q&A Q62

「医療情報システムの安全管理に関するガイドライン」の改定に当たり
1 今回対応した論点、対応方針及び対応状況（厚生労働省案）（2/5）

論点抽出カテゴリ	論点	論点の背景	対応方針（案）	対応状況	対応ページ ①5.1版からの見え消し ②5.2版本体 ③5.2版別冊
6.2章	システム構成図等の作成	◆医療機関等においてリスクアセスメントを行う前提として、医療機関等におけるシステム全体構成を示す資料の整備が求められる（2省ガイドラインにおいても、提供対象資料とされている）。 ◆外部からの攻撃があった場合の対応においても、システム構成を把握することは不可欠である。	◆6.2章のC項において、システム全体構成図（システム構成図、ネットワーク構成図等）の作成・管理を求める。	○	①P47 ②P19 ③　－
6.5章関係	アプリケーション間の連携における認証等に関する考え方	◆「健康・医療・介護情報利活用検討会 医療等情報利活用ワーキンググループ（第7回）」において、「アプリケーションごとに外部の利用者（自院職員以外）の認証・認可を行うための考え方等について整理することが必要」である旨を示し、所要の対応が求められる	◆API連携における認証について、6.5章B項に説明を加え、安全な対応を図るのに必要な観点等を記載する。 ◆HL7FHIRがこのガイドラインの対象であることを示す記載をする。	○	①P56 ②P24 ③　－

「医療情報システムの安全管理に関するガイドライン」の改定に当たり
1 今回対応した論点、対応方針及び対応状況（厚生労働省案）（3/5）

論点抽出カテゴリ	論点	論点の背景	対応方針（案）	対応状況	対応ページ ①5.1版からの見え消し ②5.2版本体 ③5.2版別冊
6.9章関係	BYODに関する記載の見直し	◆「健康・医療・介護情報利活用検討会 医療等情報利活用ワーキンググループ（第7回）」において、「個人情報の目的外利用や流出・漏洩等への対策を前提とした医療現場におけるスマートフォン等の活用、BYOD（Bring Your Own Device）への指摘があることを踏まえ、記載の検討が必要。」とされており、BYODに関するわかりやすい記載が求められる。	◆5.1版においては、ガイドラインにおいて原則禁止を謳いつつ、一定の条件下における利用できる場面について示すほか、同Q&Aにおいても「端末や OS 等に応じて推奨されている適切な方法」によることなど、具体的な対応例が示されている。 ◆一方、スマートフォンにおいては、管理者権限が、正規には利用者に認められていないなどがあり、結果としてBYODが難しいものも見られる。 ◆このような点を踏まえて、BYODに関する記述のうち、Q＆Aに示す内容の一部をガイドラインのB項等に反映して、ガイドラインの中で理解しやすいようにするのはどうか。またBYODが難しいケースについても、解説を加える。	○	①P70 ②P37 ③　－
6.10章関係	ランサムウェア等によるサイバー攻撃に対する記載	◆ランサムウェアによる被害により、医療機関等における診療等業務に大きな影響が生じている状況を踏まえて、これに対する注意喚起を行うことが求められている。	◆ランサムウェアによる被害等、昨今のサイバー攻撃による被害が後を絶たない状況を踏まえて、安全対策のあり方や安全管理ガイドラインにおける記述の仕方などを検討する。 ◆ランサムウェアに対する注意喚起についての記載を検討する。特に被害に遭っても、速やかに業務回復ができるようなバックアップの方式の必要性等も含めて、記載を行う。	○	①P73 ②P40 ③　－

「医療情報システムの安全管理に関するガイドライン」の改定に当たり
1 今回対応した論点、対応方針及び対応状況（厚生労働省案）（4/5）

論点抽出カテゴリ	論点	論点の背景	対応方針（案）	対応状況	対応ページ ①5.1版からの見え消し ②5.2版本体 ③5.2版別冊
6.11章関係	外部ネットワーク接続が可能であることの表現	◆治験の円滑化を図るために「規制改革実施計画」においても医療機関や関係者が電子カルテ等医療情報を授受するに当たって当事者が講ずべき安全対策と併せて、外部ネットワーク等が活用可能であることを分かりやすく周知すべき旨が示されている。	◆5.1版では外部ネットワーク接続は禁止していないものの、そのための技術的な方策に関する記述が中心となっていることから、外部ネットワーク接続が可能である、という前提を明示する。 ◆管理されていないネットワークの利用を禁止する旨の内容を記載する。	○	①P79 ②P44 ③P44
6.12章関係	タイプスタンプの総務大臣認定制度への変更（※）	◆「時刻認証業務の認定に関する規程」（令和3年4月1日、総務省告示第146号）により、タイムスタンプを行う認証、総務大臣の認定業務となり、一般財団法人日本データ通信協会は、その指定調査機関として指名されている。	◆6.12章C項2(1)を、以下のように変更する。 (1)　タイムスタンプは、「時刻認証業務の認定に関する規程」（令和3年4月1日、総務省告示第146号）に基づき認定された事業者（認定事業者）が提供するものを使用すること。なお、一般財団法人日本データ通信協会が認定した時刻認証事業者（以下「認定時刻認証事業者」という。）については、令和４年以降、国による認定制度に順次移行する予定であることから、当面の間、認定時刻認証事業者によるものを使用しても差し支え無い。	○	①P103 ②P54 ③　－

「医療情報システムの安全管理に関するガイドライン」の改定に当たり
1 今回対応した論点、対応方針及び対応状況（厚生労働省案）（5/5）

論点抽出カテゴリ	論点	論点の背景	対応方針（案）	対応状況	対応ページ ①5.1版からの見え消し ②5.2版本体 ③5.2版別冊
6.12章関係	電子署名の方式の明確化	◆電子文書の資格認証を普及させる必要性が、「規制改革推進会議医療介護WG」で示されており、この観点から「規制改革実施計画」においてもHPKI以外の電子署名が利用可能であることを明確にする旨が示されている。	◆6.12章に示す電子署名について、HPKIも含め、利用可能な内容や条件等をわかりやすく示す。	○	①P79 ②P44 ③P44
			◆6.12章で求める制度上の要件は、資格者が作成する文書について、その根拠法も明示することを検討する。	△ 制度上の要件は網羅性を以て記載する必要があることから、今年度改定では含めないものの、次年度の改定では網羅的に調査した結果を反映する。	①P99 ②P64 ③　－
			◆電子署名を生体認証だけで行うことは、電子署名法の電子署名には該当しない。あくまで生体認証についてはシステム利用者の本人認証の方法なので、6.5章に関係する事項である。	－	－
8.1.2章関係	外部保存受託事業者の選定基準のうち、JIS Q 27001及び15001の義務化	◆2省ガイドラインでは事業者について、JIS Q 27001及び15001を必須としていることとの整合性をとるべきとの議論がある	◆5.1版では2省ガイドラインとの整合性を踏まえて、必須としないものの、D項で求める内容は2省ガイドラインに加重した内容として、改定した。 ◆両認証いずれかの義務化（C項）の検討及び加重内容の維持（D項）などを検討する。	○	①P128 ②P67 ③　－

Ministry of Health, Labour and Welfare of Japan

中長期的な観点から見た論点、対応方針及び対応状況（厚生労働省案）

ひと、くらし、みらいのために

厚生労働省
Ministry of Health, Labour and Welfare

「医療情報システムの安全管理に関するガイドライン」の改定に当たり
2 中長期的な観点から見た論点、対応方針及び対応状況（厚生労働省案）（1/4）

◆ 中長期的に改定対象とする論点につき、第３回作業班の議論を踏まえて、整理したものを以下に示す。（一部今回改定にて対応済）

論点抽出カテゴリ	論点	論点の背景	対応方針（案）	対応状況	対応ページ ①5.1版からの見え消し ②5.2版本体 ③5.2版別冊
クラウドサービス利用の拡大	医療情報システムの構成と安全管理に関する整理	◆安全管理ガイドラインが対象とするシステム構成について、クラウドサービスの普及に伴い、院内の多様なシステムに関して、オンプレミスとの関係を整理することでセキュリティの前提となる構成の理解を促すこと求められる。	◆提言書では、第6章の冒頭に医療情報システムに関する基本的構成の整理を示したうえで、6章の各節に類型ごとにC項、D項を整理する等を示す。 ◆システム構成の整理を示すという議論と、各節に対応するという論点は、具体的な検討の範囲が異なることから、優先して対応する範囲を整理する。 ◆フルクラウドの場合に2省ガイドラインを参照すべき旨が記載されているが、IaaSのみ利用する場合なども同様であることから、この提言部分の対応の要否を確認する。	－	－
	医療機関等のシステム類型別対応	◆クラウドサービスが普及する中で、具体的な対策の在り方は、医療機関等が利用するシステム類型等により異なっており、技術的対応についてもこれを踏まえる必要がある。	◆上記論点と併せて、システム類型別（あるいは規模別の）方向性について検討し、具体的な内容を検討する。	－	－

「医療情報システムの安全管理に関するガイドライン」の改定に当たり
2 中長期的な観点から見た論点、対応方針及び対応状況（厚生労働省案）（2/4）

論点抽出カテゴリ	論点	論点の背景	対応方針（案）	対応状況	対応ページ ①5.1版からの見え消し ②5.2版本体 ③5.2版別冊
クラウドサービス利用の拡大	クラウドサービス事業者等の利用におけるリスクの把握等	◆様々な機能を持つクラウドサービスを複合的に利用する場合、扱うデータ種別ごとの事業者内部の複数事業者の関与状況や、データの国外通過・保管などが不明瞭になり、利用者からみて本ガイドラインへの適合性の判断が不十分になる。	◆提言書では、本論点に関して、「4章への追記」、「6.2.3リスク分析」への追記」が挙げられているが、この内容をすべてガイドラインに反映させるべきか、あるいはQAなどへの記載とすべきかを判断する。 ◆提言書の内容への対応を踏まえて、ガイドライン、QAその他の文書に対して、文案を整理する。	－	－
	クラウドを利用している場合の改造と保守について	◆6.8. 医療情報システムの改造と保守のＣ５はオンプレミスを念頭に置いたものなので、クラウド利用が想定されていない。	◆提言書では6.8において「クラウドサービスを契約する際には、クラウドサービスのSLAを十分に理解し、法定点検等によるサービスの停止等への対応を確認する」などの文言追記が挙げられている。 ◆追記の有無及び内容について、検討するのはどうか（例えば法定点検等によるシステム継続性確認は、クラウドサービスだけではないので、その部分の留意の論点と、SLAにより改造保守との関係で確認が必要なポイントを分けて示す必要があるか等）。	－	－
	クラウドサービスを通じた情報の持ち出し	◆6.9章では、端末の持ち出しのみ記載されているが、情報の持ち出しという観点でクラウドサービスなどは含まれていない。	◆5.1版では、6.2章で許可されないサービス利用の禁止のみ記載した（前回改定）。 ◆端末起点ではなく、情報起点で構成した場合の影響範囲を確認する。 ◆必要であればクラウドサービスでのデータ持ち出しに関する記述を設ける。 ◆6.9章については、現状のシステムやサービスの利用状況を踏まえてタイトルを修正する（利用などの観点を入れる）。	△ （一部対応：タイトル変更）	① ② ③

「医療情報システムの安全管理に関するガイドライン」の改定に当たり
2 中長期的な観点から見た論点、対応方針及び対応状況（厚生労働省案）（3/4）

論点抽出カテゴリ	論点	論点の背景	対応方針（案）	対応状況	対応ページ ①5.1版からの見え消し ②5.2版本体 ③5.2版別冊
サイバー攻撃の多様化への対応	医療機関等における内部ネットワークについて	◆医療機関等でのシステム利用の形態が、技術の進展により変化が起こっているため、今一度、医療機関等の内部ネットワークについて例示等含め、B項の考え方に詳述すべき。	◆提言書では6.5章、6.11章のB項との関係で、具体的な考え方を示すべき旨が示されている。 • 基本的な考え方（ネットワーク分離の考え方、アクセス可能な通信の最小化、アクセス履歴記録） • アクセス制御に関するバイ・デザインの導入 • 具体的な対策ポリシーの考え方 ◆提言書の内容に関し、記載の要否、記載箇所の整理（6.5章か、6.11章か）、記載内容の文案検討などのプロセスで整理する。	－	－
	ゼロトラスト等への対応	◆6.5章、6.11章はゼロトラストベースに整理しなおすべきではないか。	◆上記、内部ネットワークに関する論点と併せて検討する。 ◆5.1版では6.5章、6.11章B項において、内部脅威監視の有効性について示している。これをさらに進めて、内部脅威監視の必要性やゼロトラストの考え方をB項などに記述する、あるいは一部D項に対策項目として記述することを検討する。	－	－
	セキュリティの自動監視化についての記載	◆巧妙化するサイバー攻撃への対応として、自動監視が有効な手段の一つとして考えられる。	◆5.1版ではIDS,IPSについて記載済み。 ◆ゼロトラストの議論と合わせて、例えば6.11章B項などに検討する（EDR（Endpoint Detection and Response）など端末などエンドポイントに対する監視などと合わせて検討）。	－	－

「医療情報システムの安全管理に関するガイドライン」の改定に当たり
2 中長期的な観点から見た論点、対応方針及び対応状況（厚生労働省案）（４/４）

論点抽出カテゴリ	論点	論点の背景	対応方針（案）	対応状況	対応ページ ①5.1版からの見え消し ②5.2版本体 ③5.2版別冊
新技術への対応	ローカル５G対応への対応の要否	◆PHSサービスに代わり、５Gサービスが院内ネットワークとして採用される可能性があるため、その対応を図る。	◆提言書ではローカル５Gを採用する場合の免許に必要なセキュリティ対応などに関して、対策を検討し示すべき旨が示されている。 ◆5Gの利用に関する安全管理ガイドラインとの関係では、2019年度作業班では５Gを医療情報システムで利用する際の新規のセキュリティ課題はないと整理されている。そこで具体的なセキュリティ課題を整理して、検討する。 ◆ローカル５Gとして免許に必要なセキュリティ対応と、５G一般として利用する場合の対応策は異なる。ローカル５G利用に関する一般性を鑑みて、ガイドラインで示すべきかQA等で示すべきかを判断する。	ー	ー
制度・規格関係	長期署名方式の参照の変更	◆6.10では長期署名方式についてJIS規格を参照することとしているが、2008年以降改訂されておらず、実務的な影響を生じている。	◆提言書では、参照先をJISからISOに変更することを示している。 ◆実務的な影響範囲を確認したうえで、提言内容を踏まえて参照先の変更について検討する。	○	①P100 ②P52 ③P59

Ministry of Health, Labour and Welfare of Japan

「「医療情報システムの安全管理に関するガイドライン」に関するQ&A」の改定に当たり今回対応した論点及び、対応方針（厚生労働省案）

ひと、くらし、みらいのために

厚生労働省
Ministry of Health, Labour and Welfare

「「医療情報システムの安全管理に関するガイドライン」に関するQ&A」の改定に当たり今回対応した論点及び、対応方針（厚生労働省案）（１/２）

◆ Q&Aの改定対象とする論点につき、第３回作業班の議論を経て、すべて対応を行った。

論点抽出カテゴリ	論点	論点の背景	対応方針（案）	対応ページ
制度・規格関係	個人情報保護法改正に伴う医療機関等の責任	◆ 令和2年改正個人情報保護法により、個人情報保護委員会の命令違反に対する罰則が強化された。 ◆ 法人に対する罰則は、罰金刑30万円から1億円に大きく引き上げられている	◆ 医療機関等における個人情報保護法上の責任ということであるので、総論にQ4を新規に設けて対応した。 ◆ 内容は、医療機関等において是正措置や命令が発せられる場面を説明し、これに違反した場合の罰則について示した。	P2
わかりやすさの表現	外部接続が可能であることの記述	◆ QAにおいても、外部接続が可能であることをわかりやすく示すことが求められる	◆ Q24において、従来の記載で外部接続が可能であることを最初に持ってくることで、前提をわかりやすく示した。	P10
わかりやすさの表現	BYODについて	◆ BYODについて安全管理ガイドライン本体にわかりやすく記載することとされており、QAの内容を反映する対応をしている。 ◆ 上記を踏まえてQAでも対応することが求められる。	◆ Q32において、従来からBYODの解説を示しているが、その設問を、安全管理ガイドラインの修正に合わせて、簡易な記載とした。	P15
サイバー攻撃の多様化への対応	バックアップの取得	◆ 安全管理ガイドライン本体において、サイバー攻撃への対策として、バックアップの取得方法について追記した。 ◆ QAにおいて、具体例などを示して、より分かりやすい解説を示すことが求められる	◆ Q34で、安全管理ガイドラインの新規追記を踏まえた設問を創設し、具体例を解説を行う。 ◆ バックアップ取得の考え方や例示を記載した。	P16

「「医療情報システムの安全管理に関するガイドライン」に関するQ&A」の改定に当たり今回対応した論点及び、対応方針（厚生労働省案）（２/２）

論点抽出カテゴリ	論点	論点の背景	対応方針（案）	対応ページ
電子署名	制度上の要件についての解説	◆今般の改定で、電子署名に関して、具体的に整理を行った。 ◆これを踏まえて、対応するQAの修正をおこなう必要がある。	◆Q38に関する内容は、安全管理ガイドラインで詳述したため、削除した。	P20
電子署名	タイムスタンプ	◆制度変更に伴いタイムスタンプを提供する事業者に関する記載を修正する必要がある。	◆Q40における記述を制度変更に伴い、修正した。	P21
制度・規格関係	患者情報の共同利用	◆令和2年改正個人情報保護法により、共同利用に関する手続などが変更された ◆QAにおいてこの利用に関する解説が求められる。	◆Q62において、共同利用との関係で設問を新設し、解説を行った。	P30