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３月30日

「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（案）」に対する意見募集結果

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

パブリックコメントの結果概要

ひと、くらし、みらいのために

厚生労働省

Ministry of Health, Labour and Welfare

パブリックコメントの実施結果概要

実施期間：令和4年3月2日～令和4年3月21日
受付件数：48 件　うち　個人　11 件
法人　22 件
その他（匿名等）　15 件

意見対象

（※）1個人又は1法人が複数箇所意見出ししているため、受付件数と意見件数は一致しない。

意見箇所	意見対象のテーマ		件数
全般			7 件
改定概要			8 件
目次			1 件
第1章	はじめに		3 件
第2章	本ガイドラインの読み方		3 件
第3章	本ガイドラインの対象システム及び対象情報		
	3.2	8章の対象となる文書等について	1 件
	3.4	取扱いに注意を要する文書等	1 件
第4章	電子的な医療情報を扱う際の責任のあり方		
	4.1	医療機関等の管理者の情報保護責任について	1 件
	4.2	委託と第三者提供における責任分界	2 件
	4.3	例示による責任分界点の考え方の整理	3 件
	4.4	技術的対策と運用による対策における責任分界点	1 件
第5章	情報の相互運用性と標準化について		3 件

パブリックコメントの実施結果概要

意見箇所	意見対象のテーマ		件数
第6章	医療情報システムの基本的な安全管理		
	6.1	方針の制定と公表	2 件
	6.2	医療機関等における情報セキュリティマネジメントシステム(ISMS)の実践	11 件
	6.4	物理的安全対策	1 件
	6.5	技術的安全対策	32 件
	6.7	情報の破棄	2 件
	6.8	医療情報システムの改造と保守	2 件
	6.9	情報及び情報機器の持ち出し並びに外部利用について	14 件
	6.10	災害、サイバー攻撃等の非常時の対応	26 件
	6.11	外部のネットワーク等を通じた個人情報を含む医療情報の交換に当たっての安全管理	20 件
	6.12	法令で定められた記名・押印を電子署名で行うことについて	31 件
第8章	診療録及び診療所記録を外部に保存する際の基準		13 件
第9章	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		
	9.1	共通の要件	2 件
	9.4	紙の調剤済み処方箋をスキャナ等で電子化し保存する場合について	1 件
第10章	運用管理について		1 件
Q&A			1 件
計			193（延べ件数）

パブリックコメントにおける主なご意見とその対応（1/7）

ご意見の対象箇所		ご意見内容	対応内容
第4章	4.2　委託と第三者提供における責任分界	2省ガイドラインにおいて示すサービス仕様適合開示書との関係を明示するべきではないか。	◆別冊において、2省ガイドラインにおけるサービス仕様適合開示書に示された責任関係を確認すべき旨を記載した。
第6.5章	(1) 利用者の識別・認証	生体認証における個人情報保護法対応を示すべきではないか。	◇現状使用されている生体認証における個人情報該当性を確認したうえで、次回改定において検討する
	6.5 (6) ネットワーク上からの不正アクセス	ゼロデイ攻撃などに対するゼロトラスト対応を視野に入れて、EDRや振る舞い検知等の有効性を示したり、具体的な対応を示すのはどうか。	◆EDR、振る舞い検知が有効である旨の記載を行った。
	6.5 (6) ネットワーク上からの不正アクセス	「C12.　メールやファイル交換にあたっては、実行プログラム（マクロ等含む）が含まれるデータやファイルの送受信禁止、又はその実行停止の実施、無害化処理を行うこと。」とあるが、リモートメンテナンスの例外を示すべきではないか。	◆やむを得ず行うリモートメンテナンスの場合に、送信元における無害化処理がなされていることを確認する旨を記載した（6.8においても同様の記載を行った）。

【対応内容】
◆：ご意見を受けて、変更等の対応をいたします。
◇：今回はご意見として参考とさせていただきます。
－：原案の通りとさせていただきます。

パブリックコメントにおける主なご意見とその対応（2/7）

ご意見の対象箇所		ご意見内容	対応内容
第6.10章	6.10全般	サイバー攻撃は新項として分離して記述し、技術進展に追随できる構成とすべき。	◇サイバー攻撃に特化した記述についての精査を行う等の観点から、次回改定において検討する。
	(2) 医療情報システムの非常時使用への対応	非常時の電子カルテの対応について、医療機関等の規模に応じた指針などを示すべきではないか。	－ 各医療機関等における医療情報の管理方法や、診療に対する影響などを勘案して決定されるべきものであることから、今回はご意見として参考にさせていただくとした。
	(3) サイバー攻撃を受けた際の対応	不正なプログラムが混入したとすると、メールでウィルスを受信しただけでも発生しうる状態となるので、対応として過剰になるのではないか。	－ 不正ソフトウェアが稼働しうる環境におかれることを防止することを想定したものであることから、メールボックスに入っただけでは直ちに、対策しなければならない場面には該当しない。原案の通りとした。
	(3) サイバー攻撃を受けた際の対応	最低限の復旧手順は記載すべきではないか。また外部の情報セキュリティの専門家の協力もしくは助言を得ることについても示すべきではないか。	◆復旧するにあたっては、侵入継続と被害拡大を防ぐ観点からの方策を示すとともに、IPAなどの窓口がある旨を示した。

パブリックコメントにおける主なご意見とその対応（3/7）

ご意見の対象箇所		ご意見内容	対応内容
第6.11章	6.11章全般	章全体で「オープン・クローズ」を分けて記載している部分を、全て「オープンなネットワーク」の考え方に一本化する。	◇ゼロトラスト対応などとの関係で対策を整理する必要があることから、次回改定において検討する。
	(2)選択すべきネットワークのセキュリティの考え方	VPNはIPsecだけではなく、実績の十分あるほかのVPNも対応できるように、「IPsec」のみの記述に対して、「IPsecもしくは、より先進的なVPN」と変更する方がよりよいVPNによる暗号化やアクセス制御の対策ができる。	◆「IPsecもしくは新たな技術によりそれと同等以上の安全性が担保されているVPN」という旨の記載を行った。
第6.12章	電子署名法上の要件	「A.制度上の要求事項」に電子署名法第3条を追記すべきではないか。	－ 電子署名法第3条は、医療機関があらかじめ理解しておくことが重要である一方、医療機関の判断で選択するものであることから、「B.考え方」に記載することとして、原案の通りとした。
		「A.制度上の要求事項」に医師法や薬剤師法等の資格者に作成を求めている法律の条文を追記すべきではないか。	－ 法令で医師等の国家資格を有する者による作成が求められている文書では、医師法等への対応も求められるが、本ガイドラインは考え方を示しているものであることから、医師法、歯科医師法、薬剤師法等の条文の整理については、本ガイドラインとは別の形で追って示すこととする。

パブリックコメントにおける主なご意見とその対応（4/7）

ご意見の対象箇所		ご意見内容	対応内容
第6.12章	電子署名法上の要件	制度的要求事項が電子署名法第2条だけであるので、それ以外に電子署名法第3条に関する記述や、医師等資格確認の義務化などの記述は削除すべき。	－ 医療分野の特性を踏まえて身元確認の信用度が相当程度以上求められ、国際的な標準化とも整合性を図る必要があること、医師法等の法令を踏まえて資格確認が必要なことに加え、紙から電子化への移行に伴って作成の責任所在や国家資格の迅速な確認及び改ざん防止が可能となること等から、原案の通りとした。
		本人確認で身分証明書と住民票等の公的証明書を求めているが、顔写真付き身分証明書とeKYC等によるオンライン上での確認や、顔写真付き身分証明書と本人住所への転送不要郵便・本人限定受取郵便等の送付による確認などの方法も認められるべき。	◆ 本人の実在性の確認に当たって住民票等の公的証明書の提出を求めているが、新たな技術により、医療分野の特性を踏まえた現行の本人確認に必要な保証レベルと同等のレベルが担保される方法を用いることが可能となった場合には、これを活用することも可能であるため、本ガイドライン及び関連資料を参照の上、選択・採用することについて追記。

パブリックコメントにおける主なご意見とその対応（5/7）

ご意見の対象箇所		ご意見内容	対応内容
第6.12章	手続関係	医師等の国家資格の確認が医療機関等による立証で可能ならば、「本人性及び利用者個人の申請意思の確認」についても、医療機関等による立証（利用者の意思については同意書等を取得）で可能としていただきたい。	－本人確認に必要な保証レベルについては、患者の身体・生命に影響が生じる医療分野の特性を踏まえてリスク評価に基づき選択していることから、原案の通りとした。
		個人情報である「基本4情報」のコピー等の「書面の写しの保管」を求めることや、監査部門による定期監査を求めることは、要求が過剰であると考えられることから、「資格確認を行った実施記録の作成を行い、保存年限を定めてこれを保存すること。」に変更する。	－利用者の実在性、本人性及び利用者個人の申請意思の確認の際に、資格確認の結果と突合する必要があり、同姓同名など氏名のみによる突合では不十分であることから、基本4情報をもとに突合できるよう原案の通りとした。
		「事業者による利用者の医師等の国家資格保有の確認」に関し、「紙媒体の場合は、国家資格免許証等のコピーに実印が捺印され、印鑑登録証明書が添えてあること。電子媒体の場合は、本項と同等の電子署名（資格確認を除く）をスキャンしたデータに施すこと。」とあるが、対応可能な人が非常に少なく現実的ではないのではないかと危惧している。利便性も考慮した手法としていただきたい。	◆本人確認及び資格確認に必要な保証レベルと利便性のバランスを勘案し、郵送の場合は実印の捺印と印鑑登録証明書の提出、データの場合は本項と同等の電子署名（資格確認を除く）を求めているが、ご指摘を踏まえて、郵送の場合は、署名又は押印（実印が捺印され、印鑑登録証明書が添えてあること）による方法に修正。

パブリックコメントにおける主なご意見とその対応（6/7）

ご意見の対象箇所		ご意見内容	対応内容
第6.12章	事業者評価	「事業者が、上記の事項について、適切な外部からの評価を受けていること」の記述を入れることには、その内容が明確でないことから反対。	－ 本ガイドラインは考え方を示しているものであり、適切な外部からの評価に関する具体的な内容については、本ガイドラインとは別の形で追って示すこととする。

パブリックコメントにおける主なご意見とその対応（7/7）

ご意見の対象箇所		ご意見内容	対応内容
第8.3章	外部保存委託先事業者選定基準	「A. 制度上の要求事項」には外部保存先の類型として、1.医療法人等が適切に管理する場所、2.行政機関等が開設したデータセンター等、及び3.医療機関等が民間事業者等との契約に基づいて確保した安全な場所、が示されているが、C項に2.に関する記述がないので、追加するか、記述が無い理由等について追加してはいかがか。	◆個人情報保護法により、データセンターを運営する民間事業者においても安全管理に対する法的責任が生じることから、行政機関等が開設するデータセンターと区別する必要がないことにより、対策を共通化した旨を記載した。
		2. の(9)について、ISMAPに登録されたクラウドサービスでも良いかどうかについて明確にしていただきたい。	◆政府情報システムにおけるクラウドサービスの利用に係る基本方針が2021年3月に改定され、ISMAPを原則としていることから、取得を確認する認証対象として追記した。
第9.1章	共通の要件	「スキャニングにより、保存できない有用な情報などがある場合」は、具体的どのような場合があるか？	◆スキャニングにより、保存できない有用な情報などがある場合について、Q&Aに示した。

Ministry of Health, Labour and Welfare of Japan

中長期的な課題

ひと、くらし、みらいのために

厚生労働省
Ministry of Health, Labour and Welfare

中長期的な課題（１/4）

論点抽出カテゴリ	論点	論点の背景	対応方針（案）	対応状況
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が求められる	○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のはどうか。 ○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のはどうか。	－
	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のはどうか。	－

【対応状況】
－：現時点では未対応で、
今後、検討させていただきます。
△：現時点で一部対応済、
残りは今後、検討させていただきます。

中長期的な課題（ 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
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	○ 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 ○ 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	○ 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」などの文言追記すべきとの指摘がある。 ○ 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	○ 5.2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。 ○ 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のはどうか。 ○ 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のはどうか（利用などの観点を入れる）。	△

中長期的な課題（ 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
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	○ 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指摘されている。 • 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 ○ 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のはどうか。	ー
	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のはどうか。 ○ 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のはどうか。	ー
	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版改定時に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項などに検討するのはどうか（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）。	ー

中長期的な課題（ 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
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	○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指摘されている。 ○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、検討するのはどうか。 ○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のはどうか。	ー