「医療情報システムの安全管理に関するガイドライン第 6.0 版」の骨子（案）に関する御意見募集の結果について

令和５年３月 24 日
厚生労働省医政局特定医薬品開発支援・医療情報担当参事官室

「医療情報システムの安全管理に関するガイドライン第 6.0 版」の骨子（案）について、令和５年２月 16 日（木）～令和５年３月７日（火）まで御意見を募集したところ、本件に関する御意見を 36 件いただきました（なお、本件と直接関係しない御意見を３件承っております。）。

お寄せいただいた御意見については、適宜要約等の上、別紙のとおり取りまとめております。また、パブリックコメントの対象となる案件についての御意見のみを公表させていただいておりますので御了承ください。

今回、御意見をお寄せいただきました方々の御協力に厚く御礼申し上げます。

なお、今後第 6.0 版の本編（案）に関する御意見募集を行う予定です。

「医療情報システムの安全管理に関するガイドライン第6.0版」の骨子（案）に関する御意見募集結果

別紙

No.	御意見分類	御意見概要
1	全体構成の見直し	現状(第5.2版)では、本編、別冊の他にも多くの文書が存在する。(下記、(現状)参照) これらがそれぞれ、今回の第6版でどうなるかを明確にすべき。 ・C項、D項とを本編に記載する。 ・C項をできるだけシンプルに修正し、各C項の説明を追加する。 ・「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等の施行等について」及び個情法の観点以外のサイバーセキュリティ対策の必要な領域等を明確にする。等
2	全体構成の見直し	分冊してしまうと特定の編しか読まない事象が発生し、却って全体を見通さない人が増えるのではないか。
3	全体構成の見直し	「医療情報システムの安全管理に関するガイドライン第6.0版」の骨子（案） に反対である。 初歩から詳細にわたる事項や、ガイドライン発行時点における最新の知見を、教育的資料としてガイドラインに含めることにより、医療機関におけるサイバーセキュリティ対策の高度化を促進し、足かせとならないようにすべき。
4	全体構成の見直し	C項記載の方法 遵守事項をもっとシンプルにして、例示、場合、条件などは、解説文書側に含めて欲しい。遵守事項に条件等がある場合は、解説で説明する等。
5	全体構成の見直し	分冊化により各読者に必要な情報が届きやすくなる。また全体的に医療機関の情報リテラシーの向上に資する。 一方で、旧２省ガイドラインの対策項目一覧と安全管理ガイドラインとの対応表のように、ベンダ側が全ガイドラインを横断的かつ優先度順で俯瞰できる資料があると良い。
6	全体構成の見直し	第5.2版において用語の理解も含め政策に対応できない現場が多い。厚労省において「医療機関向けセキュリティ教育支援ポータルサイト」が開設され、ソフトウェア協会協力のもとで様々な講習開催していることは評価したいが認知度が低いため、周知・広報をお願いすることと、第6.0版での用語のわかりやすさ向上を求める。
7	全体構成の見直し	4編にすることは改定作業にて混乱を招く可能性があるため、従来の体裁のガイドラインを本編とし、ガバナンス編、マネジメント編、コントロール編の副読本を作成した方が良い。今後の改定などにおいても、関連ドキュメントへのインパクトを最小化できるとともに改定検討そのものも円滑に実施できるのではないか。
8	全体構成の見直し	経営層、企画層、運用層の三つにガイドラインを分割して整理し直す試みについては全面的に賛成。 その上で、経営層、企画層、運用層のそれぞれの責任者（一般的な知見では、CISO、CISO補佐、運用実務者となると思われる）の持つべき権限と能力・知見について明示する必要があると考える。 「診療録管理体制加算」における「医療情報システム安全管理責任者」は企画層の責任者であると考えるが、他のガイドラインと整合性を取って記述するべき。
9	全体構成の見直し	ガイドラインは、専門家が自主的に判断する際に考慮すべき事項（アセスメントするべきリスク）のリストアップを中心とし、専門家が自ら技術選択を行う際の考え方の道標を示すものとしていただきたい。 よって、これまでのガイドラインの中核を占めてきた、技術的な手段の選択に関する個別具体的な議論は、Q&Aや用語集等の本編とは別に「事例」として示すに留め、専門家による技術選択の幅を狭めることのないように留意していただきたい。
10	全体構成の見直し	経営層、企画層、運用層の三つにガイドラインが分割され、組織体制やシステム環境に応じて異なる適用範囲の宣言を促す方法が分かり易く、医療情報システムのセキュリティ管理を行う医療機関の組織整備を踏まえた観点からも適切な方向であると考える。
11	全体構成の見直し	今回の構成変更ではリスク評価が重要となると思われる。 医療機器のようにセキュリティ対応が困難な機器（一般の情報機器のような対応が行われない）についての対応が必要である。 医療機関がリスクを認識した上で、各種制限の中でリスク対応や安全性を向上できる指針にしていただきたい。 ２省ガイドラインとの関連性を考慮した対応も必要である。
12	全体構成の見直し	5.2版におけるセキュリティに係る具体的な推奨技術はQ&Aに落とし込まれるものである.。5.2版では推奨する技術を個別具体的な方法に固定する形で記載しており、技術の進歩に対して柔軟に対応できていない。 ついては、Q&Aに個別の技術について記載する場合には、例示に留めるべきである。
13	全体構成の見直し	運用上の便宜のため、以下3点の考慮を希望する。 (1)「第5.2版からの各項目の移行対応表」や「第6版各編の各項目の相関表」などの別添資料も整備いただきたい。 (2)各規模の施設やユースケースにおいて明確に規範を適用できるように規範各編本文に記載の要求事項と別添や特集での記載とを十分に整合されたい。 (3)本編のパブリックコメント募集時に、別添・特集等の資料についても、概要を記載いただきたい。
14	全体構成の見直し	詳細な改定内容の資料がなければ、検討ができない。サイバー攻撃の巧妙化により、ガイドラインをベースラインアプローチで改定することは困難であるので、リスクベースアプローチに変更することで、医療機関等のリスク対応が改善されると考えられる。
15	全体構成の見直し	セキュリティに関する技術的な内容について、本編に基本的な考えを示し、具体的な内容はQ＆Aに記載するという認識で正しいか。 当初の議論とは考え方が違うようであれば、骨子（案）の中で示すべきである。
16	外部委託、外部サービスの利用	従来は、院内勤務を前提としている内容が見られたが、在宅勤務で医療情報を扱う場面を想定した記載が必要である。
17	外部委託、外部サービスの利用	「医療情報システム・サービス事業者との協働」について ・経営陣が脆弱性対策をベンダに要求できているか、意識できるような表現を追加いただきたい。 ・栄養システムや画像システム等は、基幹となる電子カルテ・医事システムとは異なるベンダーの異なる管理がなされている場合があるので注意を促していたい。
18	外部委託、外部サービスの利用	クラウドサービスを利用する場合の項目の追加いただきたい。例えば、クラウドサービスではIdPによるデバイスの認証も選択肢としてありうる。 しかし、5.2版ではVPN、クライアント証明書の利用を必須としているため、その管理に別途仕組みの構築することとなり、医療機関の負担となる。
19	外部委託、外部サービスの利用	「医療情報システムを医療機関等に保有しない運用」ガイドラインの参照パターンを記載いただきたい。5.2版時点ではオンプレミスを前提としているため6.0版ではオンプレミスとクラウドのハイブリッドな運用についても記載いただきたい。
20	外部委託、外部サービスの利用	「医療情報システムに用いる情報機器等の管理」についてセキュリティインシデント発生時にサービス事業者側を責めるような論調も一部ある。 事業者側に予見不可能な責任を押し付けることのないよう、契約時点も含めた責任分界点を明確にしていくべきである。
21	外部委託、外部サービスの利用	設計・運用・管理をベンダに一任している医療機関も多い。過去の被害報告でもベンダーの責任分界点が曖昧であり、通常時から非常時に至るまでベンダー対応が不足している。この状況においてベンダにのみ対応を課すことは酷である。医療機関等に対応しうるベンダーの認証制度を求め、ベンダーは医療機関等に対して、遵守すべきガイドラインをまとめてアプローチすべきである。
22	外部委託、外部サービスの利用	事業者とのリスクコミュニケーションについて、医療機関の責務として明示いただきたい。

23	情報セキュリティに関する考え方の整理	ユーザーのセキュリティリテラシーは医療機関の教育・訓練で管理すべきであり初心者向けのガイドは必要である。 院内へのリモートアクセスが増加しているため、メールセキュリティの重要性、なりすましメール対策のためにDMARCについても言及すべきである。
24	情報セキュリティに関する考え方の整理	医療機関においてシステム担当者の人員は確保できず、専門性が増大しているため、システム担当のあり方について記載いただきたい。 また、2022年の診療録管理体制加算の改定により、医療機関は専任の医療情報システム安全管理責任者が情報セキュリティに関する研修を行う必要があるため、情報セキュリティの研修内容についても示してほしい。
25	情報セキュリティに関する考え方の整理	サイバーセキュリティ、情報セキュリティに関して医療機関が実施すべきことの明確化 医療機関がサイバーセキュリティ、情報セキュリティに関して実施すべきことと、本ガイドライン及び別添、別冊、チェックリスト、Q&A、特集との関係を明確にして、それを記載し周知徹底すべきではないか。
26	情報セキュリティに関する考え方の整理	半田病院や大阪急性期・総合医療センターの事例を鑑みて、閉域網ネットワークに関わらず院内ネットワークのネットワーク機器やサーバー群（OS、MW、Packages）の病院内のネットワーク機器やITシステムの最低限の脆弱性管理等を必須化していただきたい。
27	情報セキュリティに関する考え方の整理	事前対策と事後対応がある。対策には、設計、構築、運用がある。骨子には、インシデント発生時の指針を記載すべき。 小規模組織ではセキュリティ対策は軽視されがちであるのでサイバー攻撃がされやすくなる。
28	情報セキュリティに関する考え方の整理	日本が標的となったサイバー攻撃の件数は2021年と2022年を比較すると613%増となっている。サイバー攻撃における身代金の支払いの禁止や、データ復旧をベンダーへ依頼する際の透明性（ベンダー名や発注金額、データ復旧プロセスを開示することなどの義務付け）を確保して身代金の支払いを抑止することが必要である。
29	情報セキュリティに関する考え方の整理	「医療情報システムに用いる情報機器等の管理」について EoLを超えたシステム利用や費用を抑えるため性能的に限界のものを利用している医療機関もある。性能の低さにより更新プログラム適用等、情報セキュリティ対策を取れない実態がある。運用管理していく上で性能評価も見ていけるようなガイドラインにしていただきたい。
30	情報セキュリティに関する考え方の整理	「データ保護」や「モニタリング（可視化）」といった項目も必要ではないか。 クラウドサービス利用必要な対策、ゼロトラスト思考を踏まえたネットワーク上の対策、新技術並びに制度及び規格の変更への対応が必要である。 ・認証と認可による不正アクセスの排除 ・機密性・可用性・完全性を保つことによるデータの保護 ・データをデータセンタ環境に留める仕組みの構築 ・ゼロトラストセキュリティの構築 等
31	新技術、制度・規格の変更への対応	下記3点と6.0版との関係を明確に示す必要がある。医療機関の対応を明確に示す必要がある。 (1)医療機関へのサイバー攻撃などでは、ガイドラインでは対応できないものも存在する。 (2)「医療機関における医療機器のサイバーセキュリティ確保のための手引書」が発出された。 (3)医療法施行規則第14条第2項を新設し、サイバーセキュリティの確保に必要な措置のパブコメ実施された。
32	新技術、制度・規格の変更への対応	モバイル端末等を使って医療機関等の外部から接続する場合について、HTTPS/TLS以外での接続も適切な暗号化とクライアント認証の上で利用可能であることを明記することをご検討いただきたい。
33	その他	システムの利用者に対する連絡等の様な項を設けると良いのではないかと考える。 システムの運用担当者等と利用者とのコミュニケーション不足を解消し、問題の発生を抑制すべきである。
34	その他	ガイドラインの技術的な内容を各医療機関のフォーマットに合わせて回答している。骨子の中に、確認フォームの具体例を挙げていただきサービス仕様適合開示書の活用推進を促してほしい。
35	その他	文書構成、記載ルールの厳格化 PDF文書は、しおり付きとして電子的な可読性を高めて欲しい。電子的に読むことを想定した場合は最低限で必須Wordの変更履歴付きで前版との違いを公表して欲しい。
36	その他	新旧版の理解を深めるためにも、資料等を提供いただきたい。 ・5.2版から6.0版への項目の移行対応表 ・6.0版において、各編の各項目がどのような関係性を持っているのか。また、第5.2版から引き継いでいるものか、新設されたか確認できる相関表