「医療法施行規則の一部を改正する省令案」に対する
御意見募集の結果について

令和５年３月 10 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

「医療法施行規則の一部を改正する省令案」について、令和４年 12 月 16 日（金）から令和５年１月 16 日（月）まで御意見を募集したところ、計８件の御意見を頂きました。お寄せいただいた御意見の概要とそれに対する考え方について、別添のとおり取りまとめましたので御報告いたします。

なお、取りまとめの都合上、いただいた御意見は、適宜整理集約しております。

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お礼申し上げます。今後とも、厚生労働行政の推進に御協力いただきますよう、よろしくお願いいたします。

別添

医療法施行規則の一部を改正する省令案について

No.	御意見の内容	厚生労働省の考え方
1	「サイバーセキュリティの確保について必要な措置を講じること」を医療法施行規則 14 条に追加するという基本的な方針には賛成するが、「サイバーセキュリティ」という言葉で表現する、或いは、サイバーセキュリティに限定することには違和感を感じる。 本来の目的は、医療機関が保有する情報の安全な管理と、情報通信環境によって支援される医療活動の安定した運用の確保の筈であるし、その手段として対象とすべきは、医療機関が保有する所謂オンプレミスの IT 環境だけでなく、医療機関が利用する所謂クラウド型の情報環境や、医療機関が紙面で保管する診療情報の管理環境にも及ぶ筈だと考えるし、セキュリティ対策を具体的に示す情報セキュリティの CIA に言及するべきものであると考える。でなければ、この規定を持って医療機関の管理者は特別な義務を課せられる IT の導入を忌避することになりかねず、却って情報の安全性が損なわれかねないと、危惧する。 14 条 1 項の表現と近しく、かつ、適切な適用範囲を考えるならば、「病院又は診療所の管理者はその病院又は診療所に存するあるいは利用する情報通信・管理環境につき秘匿性・完全性・可用性が損なわれないよう必要な注意をしなければならない。」などの表現になるのではないか。	今回の改正では、医療機関がサイバーセキュリティ（サイバーセキュリティ基本法（平成 26 年法律第 104 号）第２条に規定するサイバーセキュリティをいう。）の確保のために必要な措置を講じることを規定しており、サイバー攻撃に対する措置のみならず、医療の提供に著しい支障を及ぼす恐れがないように必要な措置を講じることとしており、例えば情報通信ネットワークの安全性及び信頼性の確保のために必要な措置を講じることも範疇に入れています。 また、御指摘の情報セキュリティの CIA については、「医療情報システムの安全管理に関するガイドライン」（以下、「安全管理ガイドライン」という。）第 5.2 版別冊用語集において言及しているところですが、今後、安全管理ガイドラインの改定の中でその考え方を記載するよう検討してまいります。
2	以下の条文の追加をご検討いただきたい。 第十四条の２ 病院又は診療所の管理者はその病院又は診療所が利用する医用機器を含め医療情報を扱う 全ての情報システムと、それらのシステムの導入、運用、利用、保守及び廃棄に関わる人及び組織につき、関連するガイダンスにそって次にあげる項目を含め、安全管理に必要な注意をしなければならない。 一 「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」が合意形成の為の開示書等において医療機関等へ対応を求める内容を把握し、実施すること。 二 情報システム･サービスの提供事業者が提供するシステムの安全管理の妥当性について事業者内部の評価あるいは第三者評価の実施	御意見ありがとうございます。本改正では、医療機関の管理者が遵守すべき事項として、サイバーセキュリティの確保のために必要な措置を講じることを規定しています。 「必要な措置」については、「医療法施行規則の一部を改正する省令について」（令和５年３月 10 日付け産情発 0310 第２号厚生労働省大臣官房医薬産業振興・医療情報審議官通知。以下「令和５年３月 10 日付け審議官通知」という。）において、安全管理ガイドラインを御参照の上、適切な対応をしていただくようお願いしています。

	を把握すること。 三　サイバーセキュリティに関しては特に以下の注意を払うこと ア　平時の予防対応 a　医療機関向けサイバーセキュリティ対策研修をおこなうこと。 b　脆弱性が指摘されている機器に対し確実なアップデートをおこなうこと c　サイバーセキュリティに関する情報共有体制を構築しておくこと d　サイバー攻撃に対する検知機能をそなえること イ　インシデント発生後の初動対応 a　インシデント発生時の対策手順を決めておくこと b　行政機関等への報告をおこなうこと ウ　復旧対応 a　バックアップの作成・管理を徹底すること b　緊急対応手順の作成と訓練を実施すること	なお、医療機関と受託事業者の責任分解については、安全管理ガイドライン第 5.2 版本編「4.2.1. 委託における責任分界」において、「委託の場合、管理責任の主体はあくまでも医療機関等の管理者である」旨を記載したうえで、受託事業者には当該ガイドラインの関連箇所について理解し、必要な対策を実施することを求めております。
3	○　電子カルテの仕組みについてはオンプレミスやクラウドなど様々な方式があり、セキュリティの考え方も統一できない現状がある。また、多数の医療情報システム及びそのベンダーに対して、医療機関規模によっては情報管理担当者が把握することは極めて困難な状況である。病院各施設が対策を講じることも重要ですが、医療情報システムベンダーに、一定の条件を付加すること、及び統一書式にてセキュリティ対策を講じること等を求める法整備も必要ではないか。 ○　サイバーセキュリティー対策は病院管理者の責務であり、医療情報システムを提供するベンダーの管理も病院管理者の責務である。ベンダーもセキュリティに関してガイドラインを満たしたシステムを提供する必要がある旨も補足等で記載していただきたい。	御意見ありがとうございます。 御指摘の医療情報システムのベンダーも含め事業者の責務として、サイバーセキュリティ基本法（平成 26 年法律第 104 号）第 7 条において、「サイバー関連事業者（インターネットその他の高度情報通信ネットワークの整備、情報通信技術の活用又はサイバーセキュリティに関する事業を行う者をいう。以下同じ。）その他の事業者は、基本理念にのっとり、その事業活動に関し、自主的かつ積極的にサイバーセキュリティの確保に努めるとともに、国又は地方公共団体が実施するサイバーセキュリティに関する施策に協力するよう努めるものとする。」と位置づけられています。 また、安全管理ガイドライン第 5.2 版は、システム導入、運用、利用、保守及び廃棄に関わる人及び組織を対象にしており、御指摘の医療情報システムベンダーにおいても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求めています。 なお、医療機関におけるサイバーセキュリティ対策の主体は、医療機関であり、まずは医療機関において必要な対策を講じる必要があるところ、安全管理ガイドラインでも記載している通り、技術的な対応についてはシステムベンダー等と医療機関等が共同で対策を行うことを求めています。

4	○　第 14 条 1 項、2 項において、医療機関内だけではなく、委託事業者等に関しても医療機関等が責任をもって監視するように明記してほしい。 ○　追加する第 2 項を遵守するために、外部委託が可能である旨を明確にして欲しい。主たる責務は病院又は診療所に存在することは変わらないが、その全体又は一部を委託可能であることを明確にしてほしい。	御意見ありがとうございます。本改正では、医療機関の管理者が遵守すべき事項として、サイバーセキュリティの確保のために必要な措置を講じることを規定しています。 「必要な措置」については、令和５年３月 10 日付け審議官通知において、安全管理ガイドラインを御参照の上、適切な対応をしていただくようお願いしています。 安全管理ガイドライン第 5.2 版本編「２.本ガイドラインの読み方」において記載している通り、ガイドラインの対象として医療機関等から業務を受託する事業者も想定しており、受託事業者が当該ガイドラインの関連箇所について理解し、必要な対策を実施することを求めております。 また、安全管理ガイドライン第 5.2 版本編「4.2.1.　委託」において、「委託の場合、管理責任の主体はあくまでも医療機関等の管理者である」旨を記載しております。 本改正については、事業者にも周知しているところであり、医療機関と事業者が連携して取り組む方策については、引き続き検討してまいります。
5	情報処理安全確保支援士（国家資格）が活躍する等を必須要件とした国の認証等により、委託事業者を定義してほしい。	御意見ありがとうございます。今後の政策立案の検討の参考とさせていただきます。 なお、安全管理ガイドライン第 5.2 版において、事業者の選定基準の考え方等を示しておりますので、御参照ください。
6	現状のランサムウェア攻撃による影響として、オンラインバックアップシステムは殆ど役に立たない印象を持つ中で、二重三重のバックアップをとることが要求され、オフラインバックアップも定期的に行ってはいるが、有益性、また、費用対効果も危ぶまれる。対策に対策を重ねて、はたしてどれがどこまでの対策なのかが分からない状況に陥らないように、自然災害を含む、有事の際の ICT における BCP も併せた根本的な対策が必要な時期である。	御意見ありがとうございます。本改正では、医療機関の管理者が遵守すべき事項として、サイバーセキュリティの確保のために必要な措置を講じることを規定しています。 「必要な措置」については、令和５年３月 10 日付け審議官通知において、安全管理ガイドラインを御参照の上、適切な対応をしていただくようお願いしています。 なお、安全管理ガイドライン第 5.2 版本編 6.10.B.(3)において、自然災害やサイバー攻撃による IT 障害等の非常時に、医療情報システムが通常の状態で使用できない事態に陥った場合における医療

		情報システムの BCP や留意事項について記載していますので御参照ください。
7	○　追加する第 2 項を遵守するための最低限のガイドラインと、望ましい対応を示したガイドラインの、少なくとも 2 種類のガイドラインを明確に示してほしい。 ○　可能であればサイバーセキュリティー対策のレベル(基準)として、「医療情報システムの安全管理に関するガイドライン」に準拠する等を、省令の補足事項等として記載いただきたい。 ○　概要では第 2 項に何をどの程度追加されるのかが不明でコメントができない。改正案を作成されたら、再度パブリックコメントの機会を設けてほしい。	御意見ありがとうございます。 本改正では、医療機関の管理者が遵守すべき事項として、サイバーセキュリティの確保のために必要な措置を講じることを規定しています。 「必要な措置」については、令和５年３月 10 日付け審議官通知において、安全管理ガイドラインを御参照の上、適切な対応をしていただくようお願いしています。 なお、安全管理ガイドラインに記載されている内容のうち、優先的に取り組んでいただく事項については、今後チェックリストを作成し、お示しする予定です。
8	市民としては､個人情報保護･サイバーセキュリティの両方について、医療機関が問題ある状況を放置している事態（(特にインターネット上でのホームページや電子メールの扱い方などについて)幾分かは市民に見える所で事態が露見している)への対応についても厚生労働省に規則などにおいての記載いただきたい。 例えば、問題事態について、厚生労働省や地方公共団体に情報提供を行えば、それらからの連絡・指導・注意・勧告・命令などが行われるようにすると､規則はより実効性が高くなると考え､規則追加の際に、合わせて､問題事態が存在する場合の行政の対応を記載すると良いのではないか。（あるいは、行政指導がその様な記述を改めて行わなくても可能なのであれば､通知でその解釈提示と注意喚起を行うのが良いのではないか。）	御意見ありがとうございます。本改正により新設する規則第 14 条第２項の遵守状況を確認できる仕組みについては、今後検討してまいります。 また、安全管理ガイドラインでは、医療機関等がサイバー攻撃を受けた（疑い含む）等の場合は、厚生労働省等の所管省庁への連絡等、必要な対応を行うほか、そのための体制を整備する必要があることを示しています。
9	昨今のサイバー攻撃は IT 担当者が管理していない脆弱性のある機器（診療部門管理のネットワーク機器や PC 等）が狙われている事と、エンドポイントセキュリティでの対応として利用者のセキュリティーに対する認識が対策に必要である事から、100%守り切れない（起動していない、Version が古い、インストールできない等)。NISC のサイバーセキュリティーフレームワークにある”特定”の資産管理とリスクアセスメントを対策に入れ､現状やサイバーセキュリティーに対するリスクを常に管理することが必要。	御意見ありがとうございます。御指摘のとおり、今般のサイバー攻撃を踏まえ資産管理とリスクアセスメントは重要であると認識しており､「医療機関等におけるサイバーセキュリティ対策の強化(注意喚起)」（令和４年 11 月 10 日通知）においては、医療機関においては、自組織のみならずサプライチェーン全体を俯瞰し、発生が予見されるリスクを医療機関自身でコントロールできるようにする必要があることから、関係事業者のセキュリティ管理体制を確認した上で、関係事業者とのネットワーク接続点（特にインターネットとの接続点）をすべて管理下におき、脆弱性対策を実施するよう注意喚起を行ったところです。医療機関の対応状況については、今後

		確認してまいります。
10	○　サイバーセキュリティに関して医療法(施行規則)を変更することは重要であり、賛同する。 ○　電子カルテなど医療情報システムが導入されることが多くなったが､サイバーセキュリティ対策について基準がなく各医療機関側の担当者の努力に依存していた点を､管理者の責務であると省令に定めていただくのは非常に有意義でありがたい。 ○　本改正に賛成である。	御意見ありがとうございます。
11	現状の第 14 条から推測すると、医療機器、医療情報システム、その他の ICT 機器、設備において、サイバーセキュリティに関する対応とその体制確保が必要。 特に、医薬品医療機器等法の対象外の機器である医療情報システムや、その他の ICT 機器設備を対象として含めることが重要である。 例えば、EU の ENISA では、 Remote Care system, Mobile Client Devices, Identification Systems, Building Management Systems, Networking Equipment, Medical Devices, Clinical Information Systems, Industrial Control Systems, Professional Services, Cloud Services の類型(Type)に分類して、抜けが生じないような網羅性と、個々の類型に合わせた対応を示している。 本邦の実情に合わせて、医療機関で使用する機器等を網羅した分類と、対応が明確になるようにして欲しい。医療機器、医療情報システムだけで不足する例として､医療情報システムとして扱われていない ICT 機器の脆弱性が攻撃されたこと、クラウドを利用した外部委託先の ICT 機器の脆弱性が攻撃されたことが挙げられる。	御意見ありがとうございます。本改正では、医療機関の管理者が遵守すべき事項として、サイバーセキュリティの確保のために必要な措置を講じることを規定しています。 「必要な措置」については、令和５年３月 10 日付け審議官通知において、安全管理ガイドラインを御参照の上、適切な対応をしていただくようお示しており、当該ガイドラインにおいては、医療に関する患者情報(個人識別情報)を含む情報を扱うシステムについて、安全対策上求められる内容を整理しています。 なお、医療機関における医療機器についても、サイバーセキュリティを含むリスクマネジメントが求められ、使用者に対する情報提供や注意喚起を含めて最新の技術に立脚して医療機器の安全性を確保することを、その具体的な措置の内容とともに「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」において示し適切な対応を求めています。
12	医療機関でのセキュリティ対策が確実で強固なものになった場合は、個々の医療機器、医療情報システムのセキュリティは、下げられる可能性もある。 医療機関(さらにはネットワークセグメント)のセキュリティ確保レベルが表示できるようにして欲しい。これにより、あるレベル以下の施設又はネットワークセグメントに対しては､費用をかけてでも最重量のセキュリティ機能を確保した機器しか販売できないようにできる。	頂いた御意見については、改正案に関するものではございませんが、サイバーセキュリティ対策については、物理的安全対策、技術的安全対策、組織的安全管理対策及び人的安全対策の各観点から取り組むことが重要です。 また、御提案の「医療機関のセキュリティ確保レベルを表示すること」については、その必要性も含め慎重な検討が必要と考えていますが、医療機関のサイバーセキュリティの確保のために必要な対策に取り組んでまいります。
13	医療機器の部品に、外国製品を含むものは日本では禁止するべき。情	頂いた御意見については、改正案に関するものではございません

	報を抜き取られたり、自爆型の攻撃をされる可能性もある。	が、医療機関が必要なサイバーセキュリティの確保のために必要な措置を講じることができるように必要な取組を検討してまいります。