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

経営管理編
[Governance]

概略版

令和6年10月

一般社団法人　日本病院会
ICT推進委員会

※「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 経営管理編（Governance）」.

https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html. 厚生労働省医政局.令和5年5月を一部改変

概略版冊子配布にあたって

◇本冊子作成の経緯・目的

今般、診療報酬上にガイドライン第6.0版に準拠していることといった項目が増え、医療機関において各編（経営管理編、企画管理編、システム運用編）の内容についての理解が求められている。特に、理事長や病院長等の経営管理者は、万が一サイバー攻撃が発生した際に経営責任や法的責任等の責任を負うことから、日頃からサイバーセキュリティ対策やサイバー攻撃が発生した際のBCP（事業継続計画）策定・整備、BCP訓練など院内における関連事項の意思決定を行わなくてはならない。そのために経営管理編は作成されているが、本編全23ページの内容をくまなく読み込むことは、多忙を極める病院管理者にとっては現実的に容易ではない。

以上の経緯から、読者として想定される理事長や病院長等がガイドラインの内容を負担なく端的に理解するための一助として、概略版として本冊子を作成した。

◇本冊子の構成

ガイドライン経営管理編 について、ガイドライン本編の内容を一部改変した。具体的には、目次箇所に本編の遵守事項を複写した。

本冊子がガイドライン本編を読む前の足掛かりとなれば幸いである。

◇本冊子についてのお問い合わせ

一般社団法人日本病院会 政策課

TEL：03-5226-7749、E-mail：joho@hospital.or.jp

※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版本編に関するお問い合わせは、

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までお願いいたします。

TEL:03-6812-7837

https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html.

目次

【遵守事項】

①　医療情報システムの安全管理に関係する法令等を遵守すること。

②　医療機関等で業務に従事する職員や関係するシステム関連事業者等に対して、医療情報システムに関係する法令等を遵守させること。

【遵守事項】

＜説明責任＞

①　医療情報システムの安全管理に関して、原則として文書化し、管理する体制を整えること。

②　患者等への説明を適切に行うための窓口の設置等の対策を行うこと。

＜管理責任＞

①　医療情報システムの安全管理に関する管理責任を適切に果たすために必要な組織体制を整備すること。

②　定期的に管理状況に関する報告を受けて状況を確認するとともに、組織内において監査を実施すること。

＜定期的な見直し、必要に応じた改善を行う責任＞

①　医療情報システムに関する安全管理を適切に維持するための計画を策定すること。

②　医療情報に関する安全管理を適切に維持するために、定期的な見直しを実施し、必要に応じて、改善措置を講じるよう、企画管理者及びシステム運用担当者に指示すること。

【遵守事項】

＜説明責任＞

① 情報セキュリティインシデントが生じた場合、患者の生命・身体への影響を考慮し、可能な限りの医療継続を図るとともに、その原因や対策等について患者、関係機関等に説明する体制を速やかに構築すること。

＜善後策を講ずる責任＞

① 情報セキュリティインシデントが生じた場合、医療機関等内、システム関連事業者及び外部関係機関と協働して、インシデントの原因を究明し、インシデントの発生や経緯等を整理すること。

② 情報セキュリティインシデントが生じた場合、その原因を踏まえた再発防止策を講じること。

③ ①②の対応を可能とするため、通常時から非常時を想定し、システム関連事業者や外部関係機関と協働関係を構築するとともに、再発防止策を検討できるよう、通常時から非常時を想定した体制や措置を講じておくこと。

【遵守事項】

① 医療情報システムの安全管理について、システム関連事業者に委託する場合は、法令等を遵守し、委託先事業者の選定や管理を適切に行うこと。

【遵守事項】

① 業務等を委託する場合には、委託する業務等の内容及び責任範囲並びに役割分担等の責任分界を明確にし、認識の齟齬等が生じないよう、書面等により可視化し、適切に契約等の取決めを実施し、保管すること。

【遵守事項】

① 医療情報を第三者提供する場合、法令等を遵守し、手続き等の記録等を適切に管理する体制を整備すること。

② 医療情報を第三者提供する場合、医療機関等と第三者それぞれが負う責任の範囲をあらかじめ明確にし、認識の齟齬等が生じないよう、書面等により可視化し、適切に管理すること。

【遵守事項】
① 取り扱う医療情報に応じたリスク分析・評価を踏まえ、対応方針を策定し、リスク管理方針（リスクの回避・低減・移転・受容）を決定すること。
② リスク分析を踏まえたリスク管理が必要な場面の整理、対策として求められる体制、並びにルール等の企画、整備及び管理について、企画管理者に指示すること。
③ 経営層の方針及びリスク分析を踏まえ、具体的にシステム面からの最適なリスク管理措置を検討し、実装、運用するよう、企画管理者に指示すること。

【遵守事項】
① リスク評価を踏まえ、医療情報の重要性及び医療の継続性並びに経営資源の投入及びリスク管理対策の実施の継続可能性等を鑑みて、リスク管理方針を決定すること。
② リスク評価結果及びリスク管理方針に関する説明責任を果たすこと。

【遵守事項】
① リスク管理方針を踏まえ、医療情報及び医療情報システムといった医療機関等における情報資産のセキュリティに関する管理を、通常業務の一環として整え、ISMS を策定し、実施すること。

【遵守事項】
① 医療機関等のリスク管理方針に基づき、システム関連事業者による適切なリスク管理を実施し、医療機関等の要求仕様への適合性を確認し、管理すること。

【遵守事項】
① 統制の体系を理解し、医療機関等における情報セキュリティ対策に関する統制の実効性を確保するために必要な規程類、管理体制等を整備するとともに、適切に統制が機能しれているかを確認すること。

【遵守事項】
① 医療機関等の規模や組織構成、特性等を踏まえた統制の内容を検討すること。
② 医療機関等において安全管理を直接実行する医療情報システム安全管理責任者及び企画管理者を設置すること。
③ 情報セキュリティ対策に関する統制は、医療機関等内の組織や人事等の統制とは区別し、医療機関等全体における統制の一つと位置付けて、組織横断的に実施すること。
④ 情報セキュリティ対策に関する統制の対象には、医療機関等に直接雇用されている職員だけでなく、システム関連事業者の担当者や派遣社員など、医療機関等が直接雇用していない者も含むこと。

【遵守事項】
①　リスク評価及びリスク管理方針を踏まえて、情報セキュリティ方針を整備すること。
②　情報セキュリティ方針に基づき、自医療機関等の実態を踏まえて、実施可能な内容で、実効性のある、適切な情報セキュリティ対策を整備するよう、企画管理者に指示し、管理すること。

【遵守事項】
① 整備した規程類を適切に利用し、情報セキュリティ方針を遵守した対策が実施できるよう、通常時から情報セキュリティ対策に関する統制対象者すべてに対して定期的な教育・訓練を実施すること。

【遵守事項】
① 医療機関等において医療情報システムに関する安全管理対策が適切に実施されていることを確認するため、企画管理者やシステム運用担当者に定期的に自己点検を行うよう指示し、その結果報告を受け、必要に応じて改善に向けた対応を指示すること。

【遵守事項】
①　医療機関等内で、企画管理者及びシステム運用担当者から独立した組織による内部監査、または医療機関等とは異なる機関による外部監査を実施し、管理責任を果たすこと。
②　内部監査又は外部監査の結果を踏まえ、必要に応じて、安全管理措置の改善に向けた対応を企画管理者やシステム運用担当者に指示するとともに、その対応結果をフォローすること。

【遵守事項】
① 情報セキュリティインシデントの発生に備え、非常時における業務継続の可否の判断基準、継続する業務内容の選定等に係る意思決定プロセスを検討し、BCP 等を整備すること。
② 情報セキュリティインシデントにより、医療機関等内の医療情報システムの全部又は一部に影響が生じる場合に備え、医療情報システムの適切な復旧手順を検討するよう、企画管理者やシステム運用担当者に指示するとともに、当該復旧手順について随時自己点検を行うよう指示した上で、その結果報告を受け、必要に応じて、改善に向けた対応を指示すること。
③ 通常時に整備していた BCP が、非常時において迅速かつ的確に実施できるよう、通常時から定期的に訓練・演習を実施し、その結果を踏まえ、必要に応じて改善に向けた対応を企画管理者やシステム運用担当者に指示すること。

【遵守事項】
① 情報セキュリティインシデントの発生に備え、システム関連事業者又は外部有識者と非常時を想定した情報共有や支援に関する取決めや体制を整備するよう、企画管理者に指示すること。
② 情報セキュリティインシデントの未然防止策として、通常時から医療情報システムに関係する脆弱性対策や EOS（End of Sale, Support, Service：販売終了、サポート終了、サービス終了）等に関する情報を収集し、速やかに対策を講じることができる体制を整えるよう、企画管理者やシステム運用担当者に指示すること。

【遵守事項】
① 情報セキュリティインシデントの発生に備え、厚生労働省、都道府県警察の担当部署その他の所管官庁等に速やかに報告するために必要な手順や方法、体制などを整備するよう、企画管理者に指示すること。
② 情報セキュリティインシデントが発生した場合に、厚生労働省等への報告のほかに、患者等に対する公表・広報を適切に行える体制を、通常時から整備すること。

【遵守事項】
① 医療情報システムの安全管理に必要な対策項目の概要を認識した上で、企画管理者やシステム運用担当者に対して、それぞれの対策項目に係る具体的な方法について整理する旨を指示し、それぞれの対策事項が対応できている旨を確認すること。
② 対応ができてない対策項目がある場合、その理由を確認し、対応の要否を判断の上、必要に応じて対応を指示すること。

【遵守事項】
①　医療情報システムの安全管理対策項目の特徴を認識し、企画管理者やシステム運用担当者に、必要に応じて、対策項目に掲げられる措置をとるよう指示すること。

【遵守事項】
① 委託する事業者を選定する場合には、本ガイドライン及び法令等が求める要件を満たすシステム関連事業者を選定するよう指示すること。
② 委託する事業者を選定する場合には、JIS Q 15001、JIS Q 27001 又はこれと同等の規格の認証を受けているシステム関連事業者を選定するよう指示すること。

【遵守事項】
① 委託契約において、委託業務の内容やシステム関連事業者の体制、システム関連事業者との責任分界、システム関連事業者における情報の取扱い等、医療機関等が負う医療情報システムの管理に関して、協働する上で認識の齟齬等が生じないように、適切な契約の締結や管理を行うよう企画管理者に指示すること。

【遵守事項】
① 委託するシステム関連事業者に対して、業務実行体制を明確にし、医療情報の取扱い及び医療情報システムの管理に関して再委託を行う場合には、事前に医療機関等に情報を提供し、協議・合意形成を経た上で承認を得ること等を契約の内容に含めるよう、企画管理者に指示すること。

【遵守事項】
① 委託するシステム関連事業者に対して、業務実行体制を明確にし、医療情報の取扱い及び医療情報システムの管理に関して再委託を行う場合には、事前に医療機関等に情報を提供し、協議・合意形成を経た上で承認を得ること等を契約の内容に含めるよう、企画管理者に指示すること。