参考資料１－９

［特集］小規模医療機関等向けガイダンス

（案）

目次

１．はじめに

オンライン資格確認が医療機関等に導入される中で、医療情報システムに関する安全管理や情報セキュリティ対策は、今日、すべての医療機関等において必須の事項となっています。また、サイバー攻撃は巧妙化が進み、適切な対策を講じることが求められています。

一方で、具体的な安全管理対策は導入している医療情報システムの特性により異なります。例えば電子カルテをはじめとした多数の医療情報システムを医療情報システム・サービス事業者（以下「システム関連事業者」という。）に依頼して導入し、その運用を医療機関等のシステム運用担当者が自ら行っている場合と、主だった医療情報システムとしては電子カルテや医事会計システムほどで、かつ、医療機関等内にシステムのサーバ等主要な機器を設置するオンプレミス型とは異なり、システム利用者が使用する端末のみ医療機関等に設置、もしくは利用者自身の PC 等を利用し、システムは医療機関等の外部クラウドサービス上で稼働しており、サービスを利用しているクラウド型で、情報技術やシステム運用に関する知見のある担当者も特に登用しておらず、基本的にシステム関連事業者にシステムの導入や保守等の管理のかなりの部分を委ねている場合とでは、具体的な安全管理対策の内容は異なります。

特に、診療所や歯科診療所、薬局、訪問看護ステーション等の小規模医療機関等（以下「小規模医療機関等」という。）では、医療情報システムの安全管理を専任で対応する職員が不在で、医療機関等の経営層（院長や事務長等）が、医療情報システムの安全管理に関する企画管理を兼任することも多くみられます。このような医療機関等では、「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。）のすべてを詳細に理解し、自施設に関係する事項を選出して対策を講じることは難しく、システム関連事業者から多くの支援を受けながら安全管理対策を講じることも多いです。

本ガイダンスでは、このような観点から、小規模医療機関等において、安全管理ガイドラインに示されている安全管理対策を実施するために必要な内容の概略を簡易的に示すことを目的とします。

２．医療情報システムの安全管理

医療情報システムは、医療機関等において、患者に対する診療行為をはじめとする各種医療行為を円滑かつ効率的に行うために利用されるため、

・医療情報システムで保管する医療情報（患者に関する診療情報等）を適切に管理すること

・医療機関等の診療業務等に支障が生じないようにすること

・医療情報の取扱いや医療情報システムの管理に関係する各種法令等を遵守すること

などが医療情報システムの安全管理として求められます。

具体的に実施される安全管理対策として、適切な管理を実施するための組織運営やシステム運用に関する観点から医療機関等に課せられた責任を果たすために必要となる対策と、情報システムに関する技術的な観点に基づき、管理責任を適切に果たすために実装される技術的な対策が主に考えられます。

２．１　小規模医療機関等における安全管理

小規模医療機関等では、院長や事務長等の特定の職員が安全管理ガイドラインの各編で想定する役割のすべてまたは大半を担うことも少なくありません。この場合には、例えば組織図のようなものを作成する意義は低く、むしろ属人的な管理に関するリスクへの対策（緊急時に代理的に執行する体制を用意するなど）の方が重要となります。

管理責任を適切に果たすために求められる技術的な対策は、専門的な知見を有する者に委ねざるを得ないと厳しい状況であることが多いが、専門的な知見を有する外部のシステム関連事業者に安全管理ガイドラインを踏まえた対策を委ね、適切に当該事業者との関係を管理する方が、契約書類等によりサービス内容が技術的対策に関して具体的に安全管理対策の内容を把握でき、結果的に効果的な対策を講ずることが可能となることが期待されます。

２．２　小規模医療機関等における安全管理ガイドライン

安全管理ガイドラインに示す安全管理対策は、「概説編　３．２　医療機関等の特性に応じた読み方」にまとめているとおり、医療情報システムが稼働しているすべての医療機関等を対象としており、病床数や職員数、情報システム関連機器数などの医療機関等の規模ではなく、稼働している医療情報システムの構成、採用しているサービス形態等の特性に応じて、参照パターンを例示しています。

なお、医療情報の取扱いや医療情報システムの安全管理対策は、個々の医療機関等の実状に合わせて検討するものですが、医療機関等の規模等に応じて一律の組織運営やシステム運用、医療情報システム形態ではないことから、一概に規模別に分類して一律に安全管理対策を講じることは困難です。また、医療情報の機微性を考えると、保管する医療情報の多寡で、医療情報システムに関する安全管理対策の重要度合いや内容が変わるわけでもありません。

３．安全管理ガイドラインに基づく留意点

小規模医療機関等が、安全管理ガイドラインの「経営管理編」「企画管理編」「システム運用編」を通して、留意すべき事項の概要を以下に簡略的に示します。詳細は各編を参照してください。

３．１　安全管理に関する責任・責務

安全管理に関する責任・責務としては、

・医療情報の取扱いや医療情報システムの安全管理に関する法令上の遵守事項や義務など
・通常時や非常時における安全管理上の説明責任や管理責任
・医療情報や医療情報システムに関して委託や第三者提供を行う場合の責任

があります。

3．1．1　法令上の遵守事項や義務

医療情報は患者の個人情報であることから、個人情報の保護に関する法律（平成 15 年法律第 59 号。以下「個人情報保護法」という。）を遵守する必要があるほか、医療情報は基本医療従事者や医療機関等が作成することから、医師法等の各種医療関係の法令の規定を遵守する必要があり、医療従事者や医療機関等には法律上の責任が生じます。（表 1 ）

表 1　医療情報の取扱いに関する法律上の責任

責任分野	*関連法*	*情報に対する責任の内容の例*
行政法上の責任	個人情報保護法	個人情報取扱事業者責任
	各種医療関係法 ※	医療従事者・医療機関等における業法責任
刑事上の責任	刑法等	秘密漏洩罪など
民事上の責任	民法（契約）	診療契約（準委任）及びこれに関する安全配慮義務

※　医師法、歯科医師法、薬剤師法、医療法等を想定

医療機関等が遵守すべき法令の中には、特に医療情報システムで取り扱うデータ等に関係するものが含まれています。例えば、個人情報保護法では、利用目的による制限や不適正利用の禁止等の個人情報の保護に関する必要な対応のほか、安全管理措置義務や委託先の監督等の個人データの保護に関する必要な対応が求められています。

また、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（平成 16 年法律第 149 号。以下「e-文書法」という。）により電子化して保存することが認められる文書については、e-文書法及びその関係法令に従うことが求められています。

なお、関係する法令が求める内容に従って医療従事者が作成する文書等（例えば医師法における診療録）の電子媒体による保存については、「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」（平成 17 年 3 月 31 日付け医政発第 0331009 号・薬食発第 0331020 号・保発第 0331005 号厚生労働省医政局長・医薬食品局長・保険局長連名通知。平成 28 年 3 月 31 日最終改正。以下「施行通知」という。）に従うことが求められ、施行通知第二の 2（3）に掲げる 3 条件を満たす必要があります。

（施行通知 第二の２（３））

① 見読性の確保

必要に応じ電磁的記録に記録された事項を出力することにより、直ちに明瞭かつ整然とした形式で使用に係る電子計算機その他の機器に表示し、及び書面を作成できるようにすること。

（ア）情報の内容を必要に応じて肉眼で見読可能な状態に容易にできること。

（イ）情報の内容を必要に応じて直ちに書面に表示できること。

② 真正性の確保

電磁的記録に記録された事項について、保存すべき期間中における当該事項の改変又は消去の事実の有無及びその内容を確認することができる措置を講じ、かつ、当該電磁的記録の作成に係る責任の所在を明らかにしていること。

（ア）故意または過失による虚偽入力、書換え、消去及び混同を防止すること。

（イ）作成の責任の所在を明確にすること。

③ 保存性の確保

電磁的記録に記録された事項について、保存すべき期間中において復元可能な状態で保存することができる措置を講じていること。

また、診療録等を病院又は診療所等以外の場所に外部保存する場合は、「診療録等の保存を行う場所について」（平成 14 年 3 月 29 日付け医政発第 0329003 号・保発第 0329001 号厚生労働省医政局長、保険局長連名通知。平成 25 年 3 月 25 日最終改正。以下「外部保存通知」という。）に従うことが求められています。

さらに、医療従事者等が作成する医療情報を含むデータに対して電子署名を施す必要がある場合には、電子署名及び認証業務に関する法律（平成 12 年法律第 102 号。以下「電子署名法」という。）等に従うことが求められます。

３．１．２　通常時や非常時における説明責任や管理責任

医療機関等には、通常時においては、説明責任や管理責任、定期的な見直し、必要に応じた改善を行う責任があり、医療情報システムの安全管理上、情報漏洩や情報システム障害等の望ましくない事象、いわゆる、情報セキュリティインシデントが生じた非常時においては、説明責任や善後策を講じる責任があります。

通常時の責任を果たすためには、以下の取組が重要です。

【説明責任】

医療情報システムの機能や運用を、必要に応じて患者等に説明ができるように、システム機能仕様やシステム運用手順等について、システム関連事業者の協力を得ながら文書化し、管理しておく。

【管理責任】

個人情報保護法第 23 条において「個人情報取扱事業者は、その取り扱う個人データの漏洩、滅失又は毀損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない。」と規定されているとおり、医療機関等は、個人情報取扱事業者として、医療情報システムの管理実態や責任の所在を明確にする必要があり、システム関連事業者の協力を得ながら、システムの管理や運用が適切に行われているかどうかを監督する。

【定期的な見直し、必要に応じた改善を行う責任】

医療機関等で利用している医療情報システムを提供するシステム関連事業者の協力を得ながら、医療機関等として安全管理の改善に必要な情報を収集し、必要に応じて、文書化して管理しているシステム運用手順等を改善する。

また、非常時においては、以下の取組が重要となります。

【説明責任】

情報セキュリティインシデントの事態やその原因、影響、対応方針や対処方法等を、インシデントの事態に応じて、システム関連事業者の協力を得ながら、患者等への説明、ならびに、所管官庁への報告等を実施する。

【善後策を講じる責任】

情報セキュリティインシデントが生じた場合に、システム関連事業者や外部有識者の協力を得ながら、原因を究明し、再発防止策を講じる。

3．1．3　委託における責任

個人情報保護法第 25 条では、「個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない。」と規定されており、具体的内容については、「医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス」の「IV 医療・介護関係事業者の義務等　7．安全管理措置、従業者の監督及び委託先の監督（法第 23 条～第 25 条）」において示されている。個人情報取扱事業者である医療機関等は委託先の事業者を監督する責任を負い、委託先のシステム関連事業者による医療情報システムの管理も医療機関等の管理責任に含まれています。

利用する医療情報システム・サービスはじめネットワーク回線や情報機器設備など医療情報システムに関する導入や保守などについて、システム関連事業者などの委託先の事業者との間で締結する契約に

おいて、委託する内容や非常時も含めた役割分担、責任の所在を明確にして、委託先事業者との間で適切な協働体制を構築する必要があります。

双方の役割を分担し、責任の所在を明確にする、いわゆる責任分界には、

・法律上の責任の範囲を明確にする。

・具体的な運用及び対応の範囲を明確にする。

等の設定効果が期待されますので、システム関連事業者との間で認識の齟齬等が生じないよう、詳細に確認をし、書面等により可視化して、適切な契約等の取決めを実施することが重要です。

3．1．4　第三者提供における責任

医療機関等が外部の第三者に医療情報を提供する場合、医療機関等は、個人情報保護法や「医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス」に留意し、安全に医療情報を提供する責任を負っています。

医療機関等は、医療情報を提供する先の第三者との間で、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が必要です。

3．2　リスク評価を踏まえた管理

医療機関等は、医療情報システムの安全管理対策を講じるために、リスク分析・評価を実施し、リスク管理方針（リスクの回避・低減・移転・受容）を決定することが必要です。

3．2．1　リスク分析・評価

リスク分析・評価、いわゆるリスクアセスメントを実施するには、専門的な知見などが求められることがあるため、医療情報システム・サービス事業者に対して、例えば、総務省・経済産業省が定めている「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における安全管理ガイドライン」における「サービス仕様適合開示書」や日本画像医療システム工業会（JIRA）の工業会規格（JESRA：Japanese Engineering Standards of Radiological Apparatus）及び保健医療福祉情報システム工業会（JAHIS）のJAHIS 標準となっている「『製造業者/サービス事業者による医療情報セキュリティ開示書』ガイド」で示されているチェックリスト等を参考に、資料や情報の提供を依頼し、協働してリスクアセスメントを実施するようシステム関連事業者へ相談することは有意義です。

なお、リスクアセスメントを行うに当たっては、下記の資料等が参考になります。

「中小企業の情報セキュリティ対策ガイドライン」（独立行政法人情報処理推進機構：IPA）
https://www.ipa.go.jp/security/keihatsu/sme/guideline/

ならびに、上記の付録

「付録 3：5 分でできる！情報セキュリティ自社診断」

「付録 7：リスク分析シート」

３．２．２　リスク管理

リスク分析・評価を踏まえ、各リスクに対して「回避・低減・移転・受容」のいずれのリスク管理方針をとるか決定します。

リスク管理方針の検討を行う際には、情報セキュリティの３要素である「機密性(Confidentiality)」、「完全性（Integrity)」、「可用性（Availability)」のバランスを考慮しながら、医療機関等に求められる医療の提供の維持・継続等するために、どの程度の経営資源を投入し、どのような対策を講じるかなどの判断が求められます。

リスク管理方針を決定し、リスク管理対策を講じるに際しては、医療情報システム・サービス事業者とも協議を行い、助言を求めるなどしながら、認識の齟齬等が生じないようにすることは重要です。

３．３　安全管理全般（統制、設計、管理等）

３．３．１　統制（Governance）

医療機関等での医療情報システムの安全管理において、安全管理に関する経営層の意識や方針が、組織全体にしっかり浸透し、これに基づいて適切に運用され、その状況や改善すべき課題を経営層が管理できるように、統制が効いている状態となっていることが重要です。

小規模医療機関等では、限られた人数と医療情報システム・サービス事業者で手分けをして、適切な安全管理に行うこともあるかと思われます。

そのため、統制の効いた体制づくりとして、個々の職員やシステム関連事業者の役割分担を明確にすることが求められます。例えば、

・医療情報システムが利用できる機器の施錠管理を誰が行うのか

・医療情報システムに異常が生じた場合に誰がどのような連絡体制で対応するのか

・職員の情報セキュリティなどに関する教育や訓練の担当は誰がどのように行うのか　等

役割を明確にし、遂行した上で、病院長など経営層が管理できるようにすることが求められます。

なお、技術的な対応などは、医療情報システム・サービス提供事業者に委ねることも考えられるため、体制づくりに際してこうした事業者も組み込むことは重要です。

様々な医療情報システム・サービス事業者と協働しながら、医療情報システムの運営や利用をする場合、医療機関等においては、医療情報システムに求められる安全管理の水準に鑑み、安全管理ガイドラインに加えて、総務省・経済産業省が定めている「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における安全管理ガイドライン」、その他の法令等に掲げる基準を満たした医療情報システム・サービス事業者を選定し、当該事業者との契約等において、双方の認識の齟齬が生じないよう、提供される情報システムやサービスの内容、当該事業者が行う業務内容、当該事業者との責任分界、役割分担、協働体制などを明確にした上で合意形成を図ることが必要で、当該事業者に対して、必要に応じて、「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における安全管理ガイドライン」の遵守状況を確認するなど、当該事業者の管理も求められます。

3．3．2　設計

リスク分析・評価、そして、リスク管理方針の決定を踏まえ、医療情報システムの安全管理に関する情報セキュリティ方針を定め、具体的な情報セキュリティ対策を整備・実装する、医療情報システムの安全管理における設計を行います。

情報セキュリティ対策の整備に当たっては、運用ルールを定め、規程類を整備しますが、適宜、自医療機関等と同規模、同様の医療サービス提供形態、同じ医療情報システム・サービスを利用しているなどの条件に適合する他の医療機関等の運用ルールや規程類を参考にして、自医療機関等の実態と照らし合わせて策定することも効率的で効果的な進め方と考えられます。

医療情報システム・サービスを利用する上で講じた情報セキュリティ対策や適切なシステム運用のルール等を、医療情報システム・サービスを利用する職員などのすべての関係者が理解して、実践できる必要があるため、定期的に教育・訓練を行うこと必要があります。適切なシステム運用の周知などに際しては、医療情報システム・サービス事業者にも協力を得ながら実施すると有効だと考えられます。

3．3．3　管理（Management）

設計された医療情報システムの安全管理の対策が適切に行われていることを定期的に確認し、必要があれば更なる対策を講じることが求められており、点検や監査を行うことは必要です。

3．3．4　情報セキュリティインシデントへの対策と対応

災害、サイバー攻撃、システム障害といった情報セキュリティインシデントが発生したことによる非常時において、医療機関等としての事業継続計画等（以下「BCP 等」という。）に基づいて行動し、医療情報システムに関する対応も的確に実施できることが必要です。

医療機関等は、地域における医療の継続と、医療機関等の要員等の状況などを踏まえて、各医療機関等が自ら BCP 等を策定し、この BCP に基づいて非常時における医療情報システムの運用や通常時における対策等を整理する必要があります。例えば医療情報システムを構成する機器等の一部が損傷するなどにより機能しなくなった場合に、診療等の医療業務をどうするのか、損傷したものをどのように復旧させるのか、復旧した後に、機能しなくなった間に講じた措置をどのように反映させるのか、などをあらかじめ整理する必要があります。

BCP 等は策定するだけでなく、通常時でも訓練などを通じて、周知だけでなく、BCP 等の改善の要否を確認することが必要です。例えば非常時を想定して、連絡や対応の方法や手順、非常時に使用する機器等が適切に機能するかの確認などを定期的に行うことが求められます。

また、技術的な対応の多くを医療情報システム・サービス事業者に委ねることが多いことから、非常時における対応についても、当該事業者に十分に確認しておく必要があります。特に非常時のうち、サイバー攻撃などへの対応では、通常のシステム・サービス事業者だけでは対応できないこともあるので、通常のシステム関連事業者以外の事業者に関する情報収集や協力体制の構築なども重要です。

最後に、サイバー攻撃やそのおそれがある場合を含めて、非常時となった場合には、行政機関等に対する速やかな報告や警察等への連絡が必要となることがありますので、関係する官庁の連絡先や非常時に相談や依頼するシステム関連事業者や外部有識者についても、通常時から確認しておく必要があります。

３．４　安全管理に必要な対策全般

医療機関等は、利用している医療情報システム・サービスのシステム関連事業者に、利用しているシステム特性を踏まえた医療機関等として実施すべき安全管理対策に関する提案や情報提供を、前述のリスク分析・評価の際と同様に依頼し、協力を得ながら対策を講じることは有効です。

３．５　医療情報システム・サービス事業者との協働

３．５．１　事業者選定

小規模医療機関等では、医療情報システムの安全管理を実現するために、的確で専門的な知見を有する医療情報システム・サービス事業者と協働することが重要です。

当該事業者の選定に際して、費用面や機能面などを重視して選定することも多いとされますが、患者等の機微な情報である医療情報を適切に管理することが医療機関等の信頼にも直結することを考えると、情報セキュリティにおいて十分な対応をしていると確認できる事業者を選定することは重要です。

３．５．２　事業者管理

医療情報システム・サービス事業者との契約や当該事業者との協働体制の管理は、医療機関等の規模を問わず重要です。システム関連事業者との契約や協働体制の管理では、特に非常時における対応や、契約の更新・終了などの場面が重要となります。

医療機関等においては、

・医療機関等で導入している医療情報システム・サービスについて、どの事業者と、どのシステム・サービスについて、どのような契約を締結しているかいつでも確認できるようにすること。
・医療情報システム・サービス事業者の体制、連絡先などを整理し、非常時の対応内容や非常時の連絡体制や連絡手順もいつでも確認できるようにしておくこと。
・契約の更新時、特に継続する場合に、自動契約とされていることも多いですが、契約の詳細内容が変更となっていることもあります。契約内容（特に医療情報システムの運用に関する内容）の変更

時などは、システム関連事業者が変更内容について医療機関等に丁寧に説明することを定め、医療機関等はその内容を十分に確認すること。

・契約の終了時、システム関連事業者におけるデータの取扱い（返却、削除など）や手順について確認すること。

等は少なくとも実施することが求められます。

３．５．３　責任分界管理

医療情報システム・サービス事業者との責任分界を、当該事業者による業務内容や利用する医療情報システム・サービスの特性に応じて、具体的なセキュリティに関する責任の範囲を明確にする必要があります。また、通常時に加えて、非常時における対応内容などについても、それぞれ整理することが必要です。

複数の医療情報システム・サービスを導入している場合には、医療機関等のみでは、医療情報システムに不具合があった場合に、適切な対応ができないなどの事態も想定されますので、医療機関等が利用する医療情報システム全体について整理し、助言を受けられるような体制を整備することも重要です。