

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 用語集

用語		説明	概 O	経 G	企 M	シ C
あ	アプリケーション（アプリ）	コンピュータの OS 上で動作するソフトウェアのこと。ファイル管理やネットワーク管理、ハードウェア管理、ユーザー管理といった基本的な機能を持つ OS に対して、ワープロソフトや表計算ソフトといったソフトウェアのことをアプリケーションと呼ぶ。スマートフォンの場合は、ゲームを初め、辞書機能や動画再生、文書作成等、様々な目的に応じたアプリケーションがあり、「アプリ」と略されて使われる場合もある。			○	○
あ	暗号アルゴリズム	暗号化の手順のこと。主な暗号アルゴリズムは、鍵の扱い方によって共通鍵暗号方式（暗号化と復号とで共通の鍵を使用する方式）と公開鍵暗号方式（暗号化と復号とで別々の鍵を使用する方式）の二つに大別される。			○	
あ	暗号化	データを見てもその内容が分からないように定められた処理手順でデータを変えること。また、暗号化されたデータは、復号という処理によって元のデータに戻すことができる。			○	○
あ	安全管理措置	医療情報を安全に管理する（例えば、医療情報の漏えい、滅失又は毀損を防止する）ために必要かつ適切な内容で、講ずるべきこととされている措置。個人情報の保護に関する法律（平成 15 年法律第 57 号。以下「個人情報保護法」という。）により、これを講ずることが法的な責務として求められている。	○	○	○	○
い	委託	医療機関等が外部の事業者との間で業務委託契約（契約の形態・種類は問わない）を締結し、外部の事業者が医療情報の取り扱いや、医療情報を取り扱う情報システム・サービスの管理・運用を行わせること。	○	○	○	○
い	医療情報	医療に関する患者情報（個人識別情報）を含む情報。 具体的には、	○	○	○	○

用語		説明	概 ○	経 G	企 M	シ C
		①「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。）に含まれている文書 ②施行通知には含まれていないものの、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。）の対象範囲で、かつ、患者の医療情報が含まれている文書等（麻薬帳簿等） ③法定保存年限を経過した文書等 ④診療の都度、診療録等に記載するために参考にした超音波画像等の生理学的検査の記録や画像 ⑤診療報酬の算定上必要とされる各種文書（薬局における薬剤服用歴の記録等）等が対象となる。				
い	医療情報システム	医療に関する患者情報（個人識別情報）を含む情報を取り扱うシステム。 例えば、医療機関等のレセプト作成用コンピュータ（レセコン）、電子カルテ、オーダーリングシステム等の医療事務や診療を支援するシステムだけでなく、何らかの形で患者の情報を保有するコンピュータ、遠隔で患者の情報を閲覧・取得するコンピュータや携帯端末等も、範ちゅうとして想定される。また、患者情報の通信が行われる院内・院外ネットワークも含む。	○	○	○	○
い	医療情報連携ネットワーク	情報通信技術（ICT）を活用して関係医療機関等の間で効率的に患者の医療情報を共有することを目的とした、患者の同意のもと、医療機関等の間で、診療上必要な医療情報（患者の基本情報、処方データ、検査データ、画像データ等）を電子的に共有・閲覧できることを可能とする仕組みのこと。	○	○	○	

用語		説明	概 O	経 G	企 M	シ C
い	インタフェース	コンピュータ等と他のコンピュータ・周辺機器等を接続するための規格や仕様。				○
い	インフォームド・コンセント	医療の場合では、医療行為を受ける前に、医師および看護師から医療行為について、わかりやすく十分な説明を受け、それに対して患者さんは疑問があれば解消し、内容について十分納得した上で、その医療行為に同意すること。すべての医療行為について必要な手続き。もともとは米国で生まれた言葉で、「十分な説明と同意」と訳される場合もある。	○			
う	ウイルススキャン	コンピュータがウイルスに感染していないかどうかを検査すること。一般のウイルス対策ソフトは、通常の動作では、電子メールやファイルのコピー等で送受信されるデータについて、ウイルス感染を調査するようになっている。そのため、既にコンピュータに感染してしまったウイルスを検出するには、ウイルススキャンを実行する必要がある。				○
う	ウェアラブル端末	腕や頭部等の身体に装着して利用する ICT 端末のこと。				○
お	オンプレミス型	医療機関等自身が保有・管理する機材にソフトウェアを配備し、データを保管する形で情報システムを利用する形態のこと。 「クラウドサービス型」と対比されて用いられることが多い用語である。	○		○	○
か	仮想デスクトップ	サーバやパソコン等で複数の OS を動かし、ネットワーク経由で個々のデスクトップ端末へ割り当てて通常のデスクトップパソコン同様の機能を実現する技術のこと。端末側には、記憶装置を持たない「シンククライアント」を使うことが多い。ネットワークにさえ繋がっていれば、利用する環境の違いに関係なく同じ作業環境を提供できる。				○
か	可用性	情報に関して正当な権限を持った者が、必要時に中断することなく、情報にアクセスできること（Availability）。機密性、完全性、可用性は情報セキュリティの三大要素と呼ばれている。	○	○	○	○
か	監視装置	ネットワークの処理能力低下や障害の発生を定期的または常時監視する機器や				○

用語		説明	概 O	経 G	企 M	シ C
		システム。				
か	完全性	情報に関して破壊、改ざん又は消去されていないこと（Integrity）。機密性、完全性、可用性は情報セキュリティの三大要素と呼ばれている。	○	○		
き	機微性	個人の生命・身体・健康等に関わる情報をはじめとした、漏えいすることによって深刻なプライバシー侵害につながる危険性がある情報の特性。	○	○		
き	基本 4 情報	氏名、生年月日、性別、住所を指す。			○	
き	機密性	情報に関して正当な権限を持った者だけが、情報にアクセスできること（Confidentiality）。機密性、完全性、可用性は情報セキュリティの三大要素と呼ばれている。	○	○	○	○
き	脅威	情報の盗難や不正利用など、情報セキュリティリスクを発生、または、顕在化させる要因のことを指す。 脅威は、人に起因するものと作業環境に起因するものの 2 つに大別され、人に起因するものは、意図的脅威と偶発的脅威に分類される。 意図的脅威としては、標的型攻撃やマルウェア感染、Web サイトの改ざんなど、外部の人間による悪意ある行為や機密データを持ち出し、悪用するといった内部不正などが該当します。	○			
き	共通鍵	暗号化と復号に同じ暗号鍵を用いる暗号方式である共通鍵暗号方式において、暗号文の送信者と受信者の間で共有する暗号鍵。				○
く	クライアント	ネットワーク上で情報やサービスを利用するコンピュータのこと。通常は、一般利用者が使用するコンピュータがクライアントになる。なお、クライアントが要求した情報やサービスを提供するコンピュータは、サーバと呼ばれる。		○		○
く	クラウドサービス型	事業者によって定義されたインタフェースを用いた、拡張性、柔軟性を持つ共用可能な物理的又は仮想的なリソースにネットワーク経由でアクセスするモデルを通じて提供され、利用者によって自由にリソースの設定・管理が可能なサービ	○	○		○

用語		説明	概 O	経 G	企 M	シ C
		スであって、情報セキュリティに関する十分な条件設定の余地があるもの。提供形態から、IaaS（Infrastructure as a Service）、PaaS（Platform as a Service）及びSaaS（Software as a Service）に分かれる。また、実現形態から、プライベートクラウド、パブリッククラウド及びハイブリッドクラウドに分けることができる。 「オンプレミス型」と対比されて用いられることが多い用語である。				
く	クラッカー	コンピュータネットワークに不正に侵入するなど、破壊・改竄などの悪意を持った行為を行う者。				○
く	クリアスクリーン	情報セキュリティに関する対策の一つで、自席のコンピュータを意図せず第三者に操作されたり画面を盗み見されたりしないことを求めるもの。				○
こ	公衆無線 LAN	駅や街中等、公共の場所で利用できるように設定された無線 LAN の施設やサービスのこと。				○
こ	公的個人認証サービス（JPKI）	インターネット上での行政手続等に際して本人確認を行う場合に必要となる電子証明書を個人・法人が利用できるサービス。地方公共団体情報システム機構（J-LIS）が提供している。 作成・送信した電子文書が、利用者本人が作成した真正なものであり、利用者が送信したものであることを証明する署名用電子証明書と、インターネットサイト等にログインした者が利用者本人であることを証明する利用者証明用電子証明書の2種類の電子証明書をマイナンバーカードに搭載することでサービス提供がなされている。			○	
こ	互換性	部品や構成要素を置き換えても、従来通り使用できる性能を互換性という。IT分野では、特に、特定の製品向けのハードウェアやソフトウェア等を他のものに置き換えても利用できることをいう。			○	○
こ	コンピュータウイルス	他のコンピュータに勝手に入り込んで、意図的に何らかの被害を及ぼすように				○

用語		説明	概 O	経 G	企 M	シ C
		作られたプログラムのこと。ディスクに保存されているファイルを破壊したり、個人情報等を盗むこともある。また、感染経路として、ウイルスは、インターネットからダウンロードしたファイルや、他人から借りた CD メディアや、USB メモリ、電子メールの添付ファイル、ホームページの閲覧等を媒介して感染する。ウイルスにはウイルス対策ソフトでは検出・駆除できないものもあり、ウイルスに感染したことに気付かずにコンピュータを使用し続けるとウイルス自身が自分を複製する仕組みを持っていた場合には、他のコンピュータにウイルスを感染させてしまう危険性もある。				
さ	サーバ	ネットワーク上で情報やサービスを提供するコンピュータのこと。サーバに対して、情報やサービスを要求するコンピュータをクライアントという。		○	○	○
さ	サイバー攻撃	コンピュータシステムやネットワークに、悪意を持った攻撃者が不正に侵入し、データの窃取・破壊や不正プログラムの実行等を行うこと。	○			
し	死活監視／死活管理	機器やシステム、ソフトウェアなどの対象が動作しているかどうか外部から定期的・継続的に調べること。特に、専用の装置やソフトウェアなどによって自動的に調べ続けること。				○
し	実在性	対象の個人・組織等が間違いなく実在していること。			○	
し	証跡	情報システムが行った処理内容や処理対象、処理過程のデータ、利用者が行った操作などを時系列にそのまま電子的に記録したデータのこと。 「証跡管理」とは、不正アクセスや機密情報漏えい等、コンピュータ等に関する犯罪や法的紛争の発生時における原因究明や捜査に必要な機器やデータ、電子的記録を収集・分析し、その法的な証拠性を明らかにする手段や技術の総称を指す。		○	○	○
し	冗長化	システムの構成要素や機能の実現手段を複数用意することにより、一部に故障が発生しても上位系の障害に至らないよう配慮した設計を行うこと。			○	○

用語		説明	概 O	経 G	企 M	シ C
し	情報セキュリティインシデント	望まない又は予期しない、単独又は一連の情報セキュリティ事象であって、事業運営を危うくする確率及び情報セキュリティを脅かす確率が高いもの。		○	○	○
し	情報セキュリティ監査	情報システムについて、セキュリティ対策を正しく実施し、機能させることができているかを実際に検証・評価することで、組織が保有する情報資産を守るために正しく対策がとれているかを第三者の目線で確認すること。 組織内で監査人を立てる内部監査、組織外から監査人を呼ぶ外部監査の二通りの実施方法がある。		○		
し	情報セキュリティマネジメントシステム	個別の問題毎の技術対策の他に、組織のマネジメントとして、自らのリスクアセスメントにより必要なセキュリティレベルを決め、プランを持ち、資源配分して、システムを運用すること。	○	○	○	
し	証明書ポリシー（CP：Certificate Policy）	証明書発行（失効も含む）に関して「適用範囲」、「セキュリティ基準」、「審査基準」等の一連の規則を定めるもの。			○	
す	スマートフォン	従来の携帯電話に比べてパソコンに近い性質を持った情報機器。大きな画面でパソコン向けの Web サイトや動画を閲覧できたり、アプリケーションを追加することによって機能を自由に追加したりすることができる。また、タッチパネルを使い、画面の拡大やスクロールなど直感的な操作が可能。				○
せ	脆弱性	コンピュータの OS やソフトウェアにおいて、プログラムの不具合や設計上のミスが原因となって発生したサイバーセキュリティ上の欠陥のこと。セキュリティ・ホール（security hole）と呼ばれることもある。 セキュリティ上の設定に不備がある状態を指して、脆弱性があるといわれることもある。		○	○	○
せ	政府情報システムのためのセキュリティ評価制度（ISMAP）	政府が求めるセキュリティ要求を満たしているクラウドサービスを予め評価・登録することにより、政府のクラウドサービス調達におけるセキュリティ水準の確保を図り、もってクラウドサービスの円滑な導入に資することを目的とし			○	

用語		説明	概 O	経 G	企 M	シ C
		た制度。				
せ	責任分界	協働や提携、委託等する関係者間でそれぞれの責任の範囲を明確にして分けること。責任を分けて、責任の移行する点のことを責任分界点という。	○	○	○	○
せ	セキュリティ・デバイス	IC カード、USB キー等の認証用の個人識別情報を格納するデバイス。				○
せ	セキュリティ・パッチ	セキュリティ上の脆弱性・機能的不適合等を解消するためのプログラム。単に「パッチ」ともいう。				○
せ	セッション	コンピュータシステムやネットワーク通信において、接続/ログインしてから、切断/ログオフするまでの、一連の操作や通信のこと。				○
せ	セッション乗っ取り	ホームページの閲覧等、パソコンと Web サーバとの間で通信を行っている際に、その通信を利用者以外の者が乗っ取る攻撃のこと。通信が乗っ取られると、本来の利用者になり代わって通信が行われてしまう。「セッションハイジャック」と呼ばれることもある。				○
そ	ソフトウェア	コンピュータを構成する電子回路や装置などの物理的実体を指す「ハードウェア」と対比して、それ自体は形を持たないプログラムや付随するデータなどを指す言葉。 ソフトウェアは、コンピュータの中でファイル管理やネットワーク管理、ハードウェア管理、ユーザー管理といった基本的な機能を持つ OS と、その OS の上で動作する、ワープロソフトや表計算ソフト等に代表されるアプリケーションの 2 種類に大別される。	○	○	○	○
た	タイムスタンプ	電子文書がタイムスタンプが付与された時点で存在することを証明する技術。 作成された電子文書がその時点で存在したことだけでなく、その時点からいかなる人にも改ざんされていないことを証明するもの。		○	○	○
た	台帳管理	情報機器等（医療情報システムにおいて利用する物理的な資産、サービス、ライセンス等）や ID・パスワード、医療情報そのものといった、医療機関等におい			○	○

用語		説明	概 O	経 G	企 M	シ C
		て管理する情報資産を洗い出した上で、保存先や利用者範囲、保存期限等を台帳に記録して管理する方法のこと。				
た	立会人型電子署名	利用者の指示に基づきサービス提供者自身の署名鍵による暗号化等を行う電子契約サービス。			○	
た	タブレット PC	薄い板状（タブレット）の本体に、タッチして操作が可能な液晶画面が組み込まれたパソコン。				○
ち	チャネル・セキュリティ	ネットワーク回線を通して情報が伝送される途中で情報が盗み見られることのないよう、ネットワーク回線の経路を暗号化する等の措置をとること。				○
て	データ形式	プログラム上でデータを保存する形式をいう。また、補助記憶にデータを保存する形式、転送でデータを送る形式等を指す場合を含む。ファイルとして保存する場合はファイル形式という。代表的なものとして CSV 等が挙げられる。				○
て	データセンタ	サーバやネットワーク機器などの IT 機器を設置、運用する施設・建物の総称。			○	
て	データベース	複数の主体で情報を共有若しくは利用し、又は用途に応じ加工、再利用ができるように、一定の法則に基づき、作成、管理されたデータの集合をいう。				○
て	電子証明書	暗号化やデジタル署名に用いる公開鍵暗号の公開鍵が配送される際に添付され、受信者が鍵の所有者を確認するために利用する一連のデータセットのこと。信頼できる第三者（認証局）によって、間違いなく所有者本人であることを電子的に証明するために発行される。			○	○
て	電子署名	電子文書に付加される電子的な署名情報。電子文書の作成者の本人性確認や、改ざんが行われていないことを確認できるもの。	○	○	○	○
と	統制	一般的には、多くの物事を一つにまとめておさめることや国家などが一定の計画や方針に従って指導・制限することを指す。 情報セキュリティにおける統制としては、内部統制や情報セキュリティガバナンスとして用いられ、情報資産に係るリスクの管理を狙いとして、情報セキュリ	○	○	○	

用語		説明	概 O	経 G	企 M	シ C
		ティに関わる意識、取組及びそれらに基づく業務活動を組織内に徹底させるための仕組みを構築・運用することを指す。 (参照) 経済産業省「情報セキュリティガバナンスの概念・定義」 https://www.meti.go.jp/policy/netsecurity/secgov-concept.html				
と	トラフィック	通信回線やネットワーク上で送受信される信号やデータ、およびその量や密度のこと。				○
に	二要素認証	情報システムの利用者を認証する方式のうち、IC カード等のセキュリティ・デバイス+パスワードやバイオメトリクス+IC カード、ID・パスワード+バイオメトリクスのように、認証の3要素である「記憶」、「生体情報」、「物理媒体」のうち、2つの独立した要素を組み合わせることで認証を行う方式のこと。				○
ね	ネットワーク機器	ルータ、スイッチ、HUB 等の情報通信ネットワークを構築する際に用いられる機器。				○
は	パーソナルファイアウォール	個人向けファイアウォール製品。				○
は	パターンファイル	ウイルス対策ソフトがウイルスを発見するために使用するデータのこと。 ウイルスは日々新しいものが出現しているため、最新のウイルスに対応するためには、パターンファイルを常に最新のものに更新しておく必要がある。 ウイルス対策ソフトによっては、「ウイルス定義ファイル」や「ウイルス検知用データ」、「シグネチャ」等と呼び名が異なる。				○
は	バックドア	外部からコンピュータに侵入しやすいように、“裏口”を開ける行為、またはそれを実現するプログラムのこと。このプログラムが実行されると、攻撃者によってインターネットを通じてコンピュータを遠隔操作されてしまう可能性がある。 一部のウイルスでは、感染時にバックドアを埋め込むことがある。				○
は	パブリッククラウド	情報システムのインフラをサービスとして遠隔から利用できるようにしたクラウドコンピューティング環境のうち、インターネットを通じて事業者から一般				○

用語		説明	概 O	経 G	企 M	シ C
		の法人や個人に広く提供されているもの。Web サービス運営などによく用いられる。 限られた環境からのみアクセス可能なクラウドコンピューティング環境である「プライベートクラウド」と対をなす言葉である。				
ひ	秘密鍵	公開鍵暗号で使用される一対の暗号鍵の組のうち、相手方に渡したり、一般に公開したりせず、所有者が管理下に置いて秘匿する必要がある鍵。公開鍵暗号では一対の対応関係にある暗号鍵のペアを用い、公開鍵で暗号化した暗号文は秘密鍵でしか復号できないという仕組みになっている。			○	
ひ	標準時刻	国立研究開発法人情報通信研究機構の原子時計で生成・供給される協定世界時（UTC）をベースに定められた時刻。日本国内では、英国の標準時であるグリニッジ標準時（GMT）に対して 9 時間を加えた日本標準時（JST）が用いられる。				○
ふ	ファイアウォール	外部のネットワークと内部のネットワークを結ぶ箇所に導入することで、外部からの不正な侵入を防ぐことができるシステム、又はシステムが導入された機器。ファイアウォールには防火壁の意義があり、火災のときに被害を最小限に食い止めるための防火壁から、このように命名されている。				○
ふ	ファームウェア	ハードウェアの基本的な制御を行うために機器に組み込まれたソフトウェア。パソコンや周辺機器、家電製品等に搭載されており、機器に内蔵された ROM やフラッシュメモリに記憶されている。			○	○
ふ	フェイルセーフ	システムが故障した場合において、安全性が確保された状態で機能を停止させることで、被害を最小限に留めることを目指す考え方のこと。			○	
ふ	不可逆変換	ある文字列を他の文字列に変換する方法の一つで、変換後の文字列を使って変換前の文字列を特定することができないように変換する方法のこと。				○
ふ	不正アクセス	利用する権限を与えられていないコンピュータに対して、不正に接続しようと	○		○	○

用語		説明	概 O	経 G	企 M	シ C
		すること。実際にそのコンピュータに侵入したり、利用したりすることを不正アクセスに含むこともある。				
ふ	不正ソフトウェア	利用者の予期していない不利益をもたらす不正な活動を実行する、悪意を持ったソフトウェアのこと。マルウェアとも呼ばれる。 コンピュータウイルス、ワーム等、様々な形態がある。		○	○	○
ふ	振る舞い検知	ウイルス対策の方法の一つで、検査対象のプログラムを仮想環境で実行したり、実際の環境で監視したりするなどして、不審な挙動が行われていないかを確認し、それによってウイルスかどうか判断する方法。				○
ふ	プロトコル	ネットワークを介してコンピュータ同士がデータをやり取りするために定められた、データ形式や送受信の手順等の国際標準規則のこと。通信プロトコルとも呼ばれる。				○
ほ	ポート	外部とデータを入出力するための、ソフトウェアやハードウェアの末端部分（インタフェース）のこと。多くのパソコンは、周辺機器を接続するインタフェースとしての USB ポート、LAN ポート等を備えている。				○
ほ	保健医療福祉分野 PKI（HPKI）	「保健医療福祉分野の公開鍵基盤（Healthcare Public Key Infrastructure）」の略。医療現場において、本人確認だけでなく、公的資格の確認機能を有する電子署名や電子認証を行うための基盤。基盤の設置要件等は厚生労働省において策定されている。 現在は日本医師会、日本薬剤師会、医療情報システム開発センターにおいて、医師等の資格確認を行うための HPKI カードを発行している。			○	
ほ	本人性	申請等が行われる場面において、当該申請等の内容が、間違いなく当該申請等の対象者本人が作成した真正なものであること。			○	
ま	マイナンバーカード	マイナンバー制度導入により、平成 28 年 1 月から交付が開始された IC カードで、基本 4 情報と顔写真、電子証明書機能等が付されている。本人の申請に			○	

用語		説明	概 O	経 G	企 M	シ C
		より交付され、個人番号を証明する書類や本人確認の際の公的な本人確認書類として利用できる。				
ま	マクロ	アプリケーションソフトの操作を自動化する機能の一つで、利用者が関連する複数の操作や手順、命令を一連の手続きとして記録し、必要に応じて簡単な操作で繰り返し呼び出して実行することができる機能。表計算ソフトでよく利用される。				○
ま	マスターデータベース	情報システムにおいて、複数のデータベースで共通で用いられる情報群。医療分野では、医薬品や病名等に関するマスターが厚生労働省標準規格として、広く用いられている。				○
ま	マルウェア	「不正ソフトウェア」参照				○
む	無害化	無害化とは、攻撃者からの悪意のあるファイルの送付やファイル・データ等の利用に対して、利用者の PC 等の利用環境にマルウェア等が混入しないように行われる対策。これにより送付された悪意のあるマクロやコード等を削除し、送付先のシステム等の障害や情報漏えいを防止することが期待される。				○
む	無線 LAN	ケーブル線の代わりに無線通信を利用してデータ送受信を行う LAN システム。				○
ら	ランサムウェア	感染することにより PC をロックしたり、ファイルを暗号化したりすることによって使用不能にしたのち、元に戻すことと引き換えに「身代金」を要求する不正ソフトウェアをいう。				○
り	リスク	医療の場合でのリスクとは、健康や生命に被害や悪影響、危険を与える可能性のことを指す。 情報セキュリティにおけるリスクは、情報セキュリティを損ねる要因のことを指し、脅威と脆弱性の要素で構成される。 (参照) 日本ネットワークセキュリティ協会 (JNSA) https://www.jnsa.org/ikusei/01/02-03.html	○	○	○	○

用語		説明	概 ○	経 G	企 M	シ C
り	リスクアセスメント	現実に自組織が持つ情報資産（経営情報や預かり情報と、それを扱う情報システムや、紙を含む記録媒体）について、どのようなリスクが存在するのか、調査して洗い出し、そのインパクトを評価して、対応を決める必要があり、この一連の作業をリスクアセスメントという。 （参照）日本ネットワークセキュリティ協会（JNSA） https://www.jnsa.org/ikusei/01/02-04.html				○
り	リモート署名	クラウド上のサーバに利用者自身の署名鍵を格納し、利用者が当該サーバにリモートでログインした上で行う電子署名。			○	
り	リモートログイン	遠隔地から公衆回線網やインターネット等を利用して施設内のネットワークシステム（LAN）に接続し、ネットワーク上の情報資源を活用すること。				○
る	ルータ	ネットワーク上を流れるデータを他のネットワークに中継する機器。				○
ろ	ローカル署名	IC カードやパソコン等の媒体に格納された、本人が管理する鍵で署名するもの。			○	
わ	ワーム	ネットワークを通じてほかのコンピュータに拡散することを目的としたマルウェアのこと。他のファイルに寄生して増殖するのではなく、自分自身がファイルやメモリを使って自己増殖を行う。				○
わ	ワンタイムパスワード	接続する度に入力するパスワードが毎回変わり、一度使用されたパスワードは次回からは使用できないような方式のこと。実装にあたっては専用プログラムやハードウェアを利用するため、パスワードの盗み見等に対するリスクも軽減できる。				○
A	ANY 接続拒否	無線 LAN アクセスポイントの設定において ESSID が「ANY」や空欄の設定になっている無線 LAN クライアントを拒否する対策のこと。この対策により、不特定多数の無線 LAN 端末からの接続を防ぐことが可能となる。				○
A	ASP	「Application Service Provider」の略。ネットワークを通じて、アプリケーション				○

用語		説明	概 O	経 G	企 M	シ C
		ン・ソフトウェア及びそれに付随するサービスを利用させることを指す。SaaS（Software as a Service）もほとんど同様であるため、「ASP・SaaS」と連ねて呼称する。				
B	BCP	「Business Continuity Plan」の略。災害時、中でも大規模災害時には医療情報システムだけでなく、医療機関等の様々な機能や人的能力に変化が生じる。その一方で、そのような事態では医療の需要が高まり、平常時以上の対応が求められることもある。 このような事態に可能な限り対応するためには、普段からあらゆるレベルの異常時を想定し、対策を立て、文書化し、訓練を繰り返すことが有用である。このような対策を事業継続計画（Business Continuity Plan）と呼ぶ。		○		
B	BYOD	「Bring Your Own Device」の略。個人の所有する、あるいは個人の管理下にある端末の業務利用。			○	○
C	CISO	「Chief Information Security Officer」の略。最高情報セキュリティ責任者。施設や組織における情報セキュリティを統括する責任者を指す。			○	
C	CSIRT	「Computer Security Incident Response Team」の略。コンピュータセキュリティにかかるインシデントに対処するための組織の総称。インシデント関連情報、脆弱性情報、攻撃予兆情報を常に収集、分析し、対応方針や手順の策定などの活動をする。		○	○	
E	EDR	「Endpoint Detection and Response」の略。情報システムのネットワーク末端（エンドポイント）の端末に導入し、そこに存在する脅威を監視・検知することで、インシデント対応等を支援するセキュリティ対策システム・対策手法のこと。				○
H	HTTPS	「HTTP Security」の略。インターネット接続における情報通信プロトコル（HTTP：Hyper Text Transfer Protocol）に、TLS 技術による暗号化プロトコ				○

用語		説明	概 O	経 G	企 M	シ C
		ルを付加した通信プロトコル。				
I	IaaS	「Infrastructure as a Service」の略。CPU、メモリ、ストレージ、ネットワーク等のハードウェア資産をインターネット経由で利用できるサービスとして提供するクラウドサービス。			○	○
I	IDS	「Intrusion Detection System」の略。不正な攻撃を検知するシステム。ネットワークやサーバを監視し、不正なアクセスを検知する役割を担う。ファイアウォールで防ぐことのできない不正プログラムの侵入や行為を発見する仕組みであり、不正な通信を検知した場合、管理者に通知する機能を提供する。				○
I	IKE	「Internet Key Exchange」の略。ネットワーク上の機器や端末間で暗号鍵の交換及び管理を行うためのプロトコル。				○
I	Internet-VPN	「Internet-Virtual Private Network」の略。各事業所の LAN をインターネット経由で接続しながら、VPN 技術を使うことで盗聴や改ざんを未然に防止し、インターネット経由でも安全に情報を伝送することができる技術。インターネット VPN を提供するための選択肢としては、IPsec、SSL-VPN が代表的である。				○
I	IoT 機器	IoT は「Internet of Things」の略。物理的または仮想的なモノに通信機能を持たせ、インターネットに接続したり相互に通信したりすることにより、自動認識や自動制御、遠隔計測等の高度なサービスを実現するために配置する機器。				○
I	IPS	「Intrusion Prevention System」の略。不正な攻撃を遮断するシステム。不正な通信を検知した場合、管理者への通知に加え、その通信を遮断する機能を提供する。				○
I	IPsec	IP レイヤー（ネットワーク層）において暗号に基づくセキュリティサービスを提供する機能。インターネット規格の RFC 4301 で規定されている。				○
I	IP-VPN	「IP-Virtual Private Network」の略。電気通信事業者の閉域 IP 通信網を経由して構築された仮想私設通信網。IP-VPN を利用することにより、遠隔地のネット				○

用語		説明	概 O	経 G	企 M	シ C
		ワーク同士を LAN 同様に運用することが可能になる。				
I	IP アドレス	インターネット等の TCP/IP 環境に接続されているネットワーク関連機器の識別番号。				○
I	ISMS	「Information Security Management System」の略。「情報セキュリティマネジメントシステム」参照	○	○	○	
K	Kerberos	利用者のコンピュータ（クライアント）からネットワークを通じてサーバにアクセスする際に利用者の認証を行う方式の一つで、パスワードから一定の手順により生成した暗号鍵により、クライアントとサーバ間の通信経路を暗号化することで、認証情報を安全に送受信する仕組み。 複数のサーバにアクセスする際、共通に認証情報を利用することができる利点もある。				○
L	LAN	「Local Area Network」の略。企業内、ビル内、事業所内等の狭い空間においてコンピュータやプリンタ等の機器を接続するネットワーク。				○
M	MAC アドレス	「Media Access Control アドレス」の略。LAN カードの中で、イーサネット（特に普及している LAN 規格）を使って通信を行うカードに割り振られた一意の番号のこと。インターネットでは、IP アドレス以外にも、この MAC アドレスを使用して通信を行っている。LAN カードは、製造会社が出荷製品に対して厳密に MAC アドレスを管理しているため、全く同一の MAC アドレスを持つ LAN カードが2つ以上存在することはない。				○
M	MDM	「Mobile Device Management」の略。組織内の従業者に支給する携帯情報端末のシステム設定等を統一的・効率的に管理する手法、あるいはそれを実現するシステム。 利用できる機能、導入できるソフトウェアやデータに制限を加えたり、端末の紛失時に遠隔制御によってデータの消去や操作のロックを行ったりすることが可				○

用語		説明	概 O	経 G	企 M	シ C
		能となるものもある。				
N	Nonrepudiation（否認防止）	送信元（あるいは受信者）が、あとになってその送信事実（受信事実）またはその内容を否定する主張をすることができないように証拠を残すこと。			○	
O	OS	「Operating System」の略。コンピュータを動作させるための基本的な機能を提供するシステム全般のこと。例えば、メモリやディスク等のハードウェアの制御、キーボードやマウスといったユーザーインタフェースの処理、画面への表示とウィンドウの制御等、コンピュータが動作するための数多くの基本処理を行う。さらに、コンピュータシステムを管理するための数多くのツールが用意されている。				○
P	PaaS	「Platform as a Service」の略。オペレーティングシステムや、アプリケーションの実行環境（開発環境を含む）をインターネット経由で利用できるサービスとして提供するクラウドサービス。			○	○
P	PKI	「Public Key Infrastructure」の略。信用の起点となる最上位の認証局（ルート認証局）が自らの秘密鍵で署名した電子証明書に基づいて、他の認証局が提供する公開鍵を利用する形で、インターネットによる通信のみによって公開鍵暗号とデジタル署名サービスが運用される仕組みのこと。			○	○
R	REST-API	「Representational State Transfer Application Programming Interface」の略。Web システムを外部から利用するためのプログラムの呼び出し規約（API）の種類の一つで、「REST」（レスト）と呼ばれる設計原則に従って策定されたもの。				○
S	SaaS	「Software as a Service」の略。ソフトウェアをインターネット経由で利用できるサービスとして提供するクラウドサービス。			○	○
S	SLA	「Service Level Agreement」の略。書面にしたサービス提供者と顧客との合意であって、サービス及びサービス目標を特定した、サービス提供者と顧客との間の合意文書（JIS Q 20000-1:2020）。	○		○	○

用語		説明	概 O	経 G	企 M	シ C
S	SSL-VPN	「Secure Socket Layer-Virtual Private Network」の略。リモートアクセスでの通信経路上を TLS（SSL の後継技術）で保護する技術。IPsec を用いた VPN のような特定端末間だけで VPN を構成する、いわゆる拠点間 VPN とは異なる。				○
T	TLS	「Transport Layer Security」の略。インターネットにおいてデータを暗号化したり、なりすましを防いだりするためのプロトコルのこと。利用者は、認証機関により発行されたサーバ証明書によって、サーバの真正性を確認する。				○
V	VPN	「Virtual Private Network」の略。公衆回線網等の上に仮想的に構築された閉域網（イントラネットのように外部に対して非公開であるネットワーク）。				○
W	WPA2-AES、WPA2-TKIP	WPA2 は、無線 LAN 上で通信を暗号化して保護するための技術規格である WPA（Wi-Fi Protected Access）のセキュリティを向上させた技術規格であり、そのうち WPA2-AES は、共通鍵暗号方式として AES と呼ばれるアルゴリズムを用いた CCMP と呼ばれる暗号化方式を、WPA2-TKIP は、共通鍵暗号方式として RC4 と呼ばれるアルゴリズムを用いた TKIP と呼ばれる暗号化方式を、それぞれ採用している。				○

[特集] 小規模医療機関等向けガイドンス

目次

1. はじめに	- 1 -
2. 医療情報システムの安全管理	- 1 -
2. 1 小規模医療機関等における安全管理	- 2 -
2. 2 小規模医療機関等における安全管理ガイドライン	- 2 -
3. 安全管理ガイドラインに基づく留意点	- 3 -
3. 1 安全管理に関する責任・責務	- 3 -
3. 1. 1 法令上の遵守事項や義務	- 3 -
3. 1. 2 通常時や非常時における説明責任や管理責任	- 5 -
3. 1. 3 委託における責任	- 6 -
3. 1. 4 第三者提供における責任	- 6 -
3. 2 リスク評価を踏まえた管理	- 6 -
3. 2. 1 リスク分析・評価	- 7 -
3. 2. 2 リスク管理	- 7 -
3. 3 安全管理全般（統制、設計、管理等）	- 7 -
3. 3. 1 統制（Governance）	- 7 -
3. 3. 2 設計	- 8 -
3. 3. 3 管理（Management）	- 9 -
3. 3. 4 情報セキュリティインシデントへの対策と対応	- 9 -
3. 4 安全管理に必要な対策全般	- 10 -
3. 5 医療情報システム・サービス事業者との協働	- 10 -
3. 5. 1 事業者選定	- 10 -
3. 5. 2 事業者管理	- 10 -
3. 5. 3 責任分界管理	- 11 -
医療情報システム・サービス事業者との協働事項	- 12 -

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、自施設に係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。

本ガイドンスでは、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係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が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 57 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に、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に、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、適切な安全管理を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、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（略称：MDS/SDS：Manufacturer/Service Provider Disclosure Statement for Medical Information Security）』ガイド』で示されているチェックリスト等を参考に、当該事業者から情報提供していただく等をして選定し、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に、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・訓練を行うことが必要です。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、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（略称：MDS/SDS：Manufacturer / Service Provider Disclosure Statement for Medical Information Security）』ガイド』で示されているチェックリスト等を参考に、当該事業者から情報提供していただく等をして、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。

【別添】

医療情報システム・サービス事業者との協働事項

小規模医療機関等が本ガイダンスに基づいて医療情報システムの安全管理を実施する上で、専門的な知見を有し、技術的な対応を委ねることが多いシステム関連事業者からの協力を得ることが望ましいと考えられる事項を以下に示します。

- 医療機関等として、管理責任を果たすために求められる技術的な対策の具体的な内容
- 説明責任を果たすためのシステム機能仕様やシステム運用手順等の文書化及び当該資料の管理
- 管理責任を果たすためのシステムの管理実態や責任の所在に関する情報や資料の提供
- 医療情報システムの安全管理の改善に必要な、文書化し管理しているシステム運用手順等に関する情報や資料の提供
- 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おいて、非常時も含めた役割分担、責任の所在、協働体制をまとめた情報や資料の提供
- 医療情報システムに関するリスク分析・評価・管理を実施するために必要な情報や資料の提供（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（略称：MDS/SDS：Manufacturer / Service Provider Disclosure Statement for Medical Information Security）』ガイド」で示されているチェックリスト等を参考にしたもの。）

[特集] 医療機関等におけるサイバーセキュリティ

目次

1. はじめに	- 1 -
2. サイバーセキュリティとは.....	- 1 -
3. サイバーインシデント	- 2 -
3. 1 代表的な起因例	- 2 -
3. 2 サイバー攻撃の典型例.....	- 2 -
3. 3 必要最小限の対策：バックアップ（システム・データ）	- 3 -
4. 対策	- 5 -
4. 1 ガバナンス	- 5 -
4. 1. 1 構成管理	- 5 -
4. 1. 2 アカウント管理	- 6 -
4. 1. 3 監視	- 7 -
4. 2 バックアップ.....	- 7 -
4. 2. 1 BCP（Business Continuity Plan：事業継続計画）	- 7 -
4. 2. 2 システム・データ	- 7 -

1. はじめに

診療情報等の機微な情報を扱う電子カルテをはじめとする医療情報システムは、情報の利用性を高めて連携を容易にし、質の高い医療の提供に極めて有用ですが、短時間で大量の情報を処理できることが可能であるために、何かセキュリティ上の問題が起こると被害や業務影響が大きくなる可能性があります。セキュリティ上の問題としては、例えば、システム利用終了時にログアウトし忘れるといった運用上の問題から、停電や機器の故障、さらにはマルウェア（コンピュータウイルス）と呼ばれる悪意のある不正ソフトウェアの混入など様々な事象があります。「医療情報システムの安全管理に関するガイドライン」は、これらすべてに対応するためのガイドラインで、どうしても扱う項目が多くなります。一方でサイバー攻撃と呼ばれる外部からの不正ソフトウェアの混入による被害が昨今増えてきており、最悪の場合は診療機能停止に至るなど、社会的にも問題になっています。サイバー攻撃の脅威が近年増大していることに鑑み、医療法施行規則（昭和 23 年厚生省令第 50 号）第 14 条第 2 項では、病院、診療所又は助産所の管理者が遵守すべき事項として、医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律施行規則（昭和 36 年厚生省令第 1 号）第 11 条第 2 項において薬局の管理者が順守すべき事項として、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なければならないとしています。そこで、「医療情報システムの安全管理に関するガイドライン」の中で、サイバーセキュリティに関係する部分を要約し、できるだけ具体的な例などにも触れてまとめたものがこの特集です。一読いただいて、ご自身の所属する医療機関の対策に役立てていただければ幸いです。

最初に述べなければならないことは、サイバーセキュリティは導入している医療情報システムによって異なるということです。例えば、フルクラウドの電子カルテサービスを導入している診療所など小規模医療機関等の場合は、サイバーセキュリティを踏まえたシステムやデータ、サービスが用意された適切なシステム関連事業者のサービスを採用していれば、医療機関等が主に取り組むことは医療情報システムの利用者認証を適切に行うことと想定されますので、当該事業者がサイバーセキュリティに関して医療機関等側が取り組むべきことを確認し、認識の齟齬や漏れがないようにして、適切に医療情報システムを利用してください。

これ以降の記載はオンプレミス型の医療情報システムや、オンプレミス型とクラウド型の混在した医療情報システムを導入・利用している医療機関等を想定しており、地域において地域医療の基幹を担う医療機関は必要最小限の対策に留まることなく、地域で担っている役割を維持できるよう各種対策に注力してください。

2. サイバーセキュリティとは

不正ソフトウェアによる感染被害や、外部から不法に医療情報システムに侵入し、データを盗み取ったり、または破壊したりするような被害を受けるか、または被害には至らなくとも対応が必要になる事象をサイバーインシデントと呼び、これに対応する対策がサイバーセキュリティです。

外部からネットワーク等を介して、侵入または不正ソフトウェアの送り込みをサイバー攻撃と呼びますが、例えばユーザや保守事業者の自宅のパソコンが不正ソフトウェアに感染し、USB メモリや CD /DVD、外付け HDD 等の可搬媒体を介して医療情報システムに不正ソフトウェアが入り込むこともあります。

3. サイバーインシデント

3. 1 代表的な起因例

サイバーインシデントの代表的な起因例を以下に示します。

- (1) USB メモリ、CD/DVD、業務に使っているスマートフォンなどを介して不正ソフトウェアに感染する。(媒体感染)
- (2) 送られてきた電子メールに添付されたファイルやソフトウェアを、不用意にダブルクリック等を行い、開封または起動する、あるいはメール本文中にあるリンク情報 (URL) をクリックし、不正ソフトウェアを呼び込んでしまう。(メール攻撃)
- (3) 地域医療連携、オンライン保守作業 (リモートメンテナンス)、インターネット利用などの外部に接続する部分を攻撃されて、侵入または不正ソフトウェアを送り込まれる。(サイバー攻撃)

上記以外にもありますが、本特集では代表的なものにとどめます。しかし、サイバーセキュリティの観点から、基本的に講ずるべき対策などに変わりはありません。

3. 2 サイバー攻撃の典型例

サイバー攻撃被害と対応の典型的な例として、ランサムウェア*と呼ばれる不正ソフトウェアが保守回線から医療情報システムに侵入した場合をあげます。

*ランサムウェア： 身代金要求 (Ransom) 型の不正ソフトウェアで、典型的な場合はデータを暗号化し、復号するために暗号資産などで身代金を要求してきます。

[攻撃被害]

1. 最初に侵入するのはランサムウェアそのものではないことが多いです。最初に侵入した不正ソフトウェアは、医療情報システムを静かに観察します。どのファイルが良く使われて、システムがどのような構成になっているか調査し、急所となる部分に外部からランサムウェアを呼び込む不正ソフトウェアを配置します。この時点で検出することは不可能ではありませんが、比較的難しいです。
2. ランサムウェアを外部から呼び込みます。呼び込まれたランサムウェアは一斉に重要なファイルを暗号化します。さらに脅迫文書をプリンタから打ち出したり、画面に脅迫文などを表示したりします。この時点で正常な業務はできなくなります。最初の不正ソフトウェアの侵入から被害が表面化するまでに数日～数週間かかることが多いようです。

[被害対応]

3. 自機関の BCP (Business Continuity Plan：事業継続計画) に基づき、非常時における緊急的な情報アクセスを開始します。現状が BCP に記載されているどのフェイズにあるのかを確認することが重要です。
4. 被害を把握した場合、被害届けを警察に提出します。警察では、被害防止対策に必要な情報の提供・助言や被害の復旧への貢献が行われています。また、こうした対応や捜査に当たって

は、被害医療機関の意向が最大限尊重され、業務への影響が最小限となるよう早期被害復旧等に配慮されます。

5. 侵入経路に関係する通信ログの保全が完了すれば、医療情報システムの復旧に着手します。バックアップデータはすでに不正ソフトウェアが侵入している可能性があり、検出と適切な対応を行いながら復旧します。復旧が完了した医療情報システムの動作が確認できれば、必要に応じて緊急対応中のデータ復旧を行い、終了した時点で平常運用に戻り、BCP を終了します。
6. それまでの経過をレビューし、BCP の点検・検証・評価を行い、必要があれば改善し、すべての対応プロセスが完了します。

上記は比較的大規模な医療機関で最近見られた典型的な例を記載したもので、攻撃の種類や医療機関の規模によって被害や対応方法は変わってきます。

3. 3 必要最小限の対策：バックアップ（システム・データ）

媒体感染、メール攻撃、サイバー攻撃等のサイバーインシデントの被害に遭ったとしても、被害や業務影響を少しでも小さくし、業務や情報システムの復旧が少しでも早くなるための必要最小限の基本的な対策として、システムやデータのバックアップがあります。

医療情報システムを利用して、診療等の患者に対する医療サービスを行っている医療機関等においては、自施設が提供している医療サービスの特性を踏まえ、利用する医療情報システムや取り扱う医療情報の重要性に鑑み、対象とするシステムの範囲やデータの期間を定め、地域医療に与える影響や業務の復旧に要するコストが許容できる最小限に留まるよう、システム関連事業者とも協議をし、バックアップを整える必要があります。

システムやデータのバックアップの目的は下記の2つがあります。

1. 最低限の業務が継続できるように、最低限必要な情報へのアクセスをすばやく復旧させる。
2. 医療情報システムになにかあった場合に、元の正常な状態に戻し、復旧させる。

1. は、診療等の最低限の業務を継続するために最低限必要なデータへのアクセスをできるだけ早く回復させるためのものです。何が最低限必要であるかは医療機関等によって異なります。またデータが利用可能でもシステムの機能が回復できず、アクセスできないこともありますので、非常時における緊急のデータへの代替アクセス方法も考えておく必要があります。

また、このバックアップは毎営業日に行うべきです。典型的なサイバー攻撃の例で述べたように、不正ソフトウェアは観察してから暗号化していきますので、バックアップも狙われます。したがってバックアップを一つ用意するだけでは、対応できないこともあります。これを防ぐためには複数世代のバックアップを用意し、少なくともその一つは暗号化などのデータの変更不能に既に書き込まれたデータに対する追加の書き込みを禁止にする必要があります。

対策の例としては、テープカートリッジにバックアップし、次の日には前の日のバックアップをさらにコピーバックアップし、このバックアップカートリッジを外します。カートリッジを5セット用意してローテーションで使うと、常に3世代分は書き込みされる恐れのないバックアップが確保できます。

テープバックアップが利用できない場合は、複数世代のバックアップをディスク領域に保存した上で、OS の機能で書き込み禁止にしますが、不正ソフトウェアによって管理者権限が奪取されると、書き込み禁止の状態を解除される恐れがあります。完全に防止することは難しいですが、少なくとも医療情報システムの運用系とバックアップ系は管理者のパスワードを異なるものにするか、利用者の管理ドメインを変えるなどの措置を施すことで、リスクの軽減を講じることはできます。

2. におけるシステムの復旧には、データだけでなくシステムを動作させるためのプログラムや設定もバックアップしておく必要があります。フルバックアップと言ってもいいでしょう。一般的に医療機関等の判断と作業で実施できうるものではなく、医療情報システムを導入するシステム関連事業者がセットアップするものです。医療機関等はシステムを導入するときに、フルバックアップを適切に行うことを仕様を含め、検収の際に確認することになります。医療機関等の判断で、医療情報システムを複数のシステム関連事業者が構成することもあります。例えば放射線画像システムと電子カルテが異なる事業者が導入する場合で、LAN などのネットワークインフラは別事業者という場合もあります。複数のシステム関連事業者が関与する場合は、バックアップに抜け漏れや隙間があってははいけません。またシステムの稼働や利用に必要なサーバやクライアント PC 等の機器に障害が発生した場合で、同じ機器が手配・調達できない場合もあります。機器の設定等は、単純なバックアップと同時に、論理的な設定の記録も必要です。これがあるとないとでは復旧に要する時間や作業効率に差が出ます。

プログラムや設定のバックアップは変更した時に取ればいいですが、データはやはり毎日バックアップされると思います。こちらも 1. の場合と同じで、バックアップも不正ソフトウェアに狙われますので、1. と同様の対策を取る必要があります。また、被害の範囲や性格等によっては、ソフトウェアやデータばかりでなく、医療情報システムで利用する機器（ハードウェア）のバックアップが求められることがあります。例えばサイバー攻撃による刑事事件とされるような場合には、警察による捜査のため、サーバや端末、機器等について証拠として提供を求められることがあります。また機器等のファームウェア等が書き換えられているリスクが認められる場合には、交換等の対応も必要となります。このように犯罪による被害やその範囲・内容によっては、既存のシステムと互換性を保つことが可能なハードウェアを準備しておくことが必要なこともあります。

診療の継続性をできる限り早く回復させるためのバックアップについては、医療機関によって何が必要異なりますので、事前によく検討しておく必要があります。一般的に言って、情報が生成されてから時間が経てば経つほど、利用される頻度は低下します。もちろん過去の情報との比較は必要ですが、一般的な医療機関では、緊急事態である非常時では直近 1 年程度の期間の情報が比較できれば、緊急の診療としては可能なことが多いと思われます。したがって、バックアップ対象期間については、1 年を少し超える期間をバックアップ対象とすることが推奨されます。なお、放射線画像診断検査結果データのようにデータサイズが大きい画像情報については、バックアップの環境にかけられるコストの都合から、このような目的でのバックアップが難しい場合は、読影レポートを保存するか、カルテ自体に所見を記載するようにしておくといいでしょう。検査結果や処方データなどは、厚生労働省標準規格である SS-MIX 2 標準化ストレージの形式で保存されていれば必要なバックアップデータを容易に作成することができます。また、HL7 FHIR 化が進んでいる場合は SS-MIX 2 標準のデータを HL7 FHIR 化した HL7 FHIR 規格準拠サーバでも同じことが言えます。

また、システム機能が回復できないためにバックアップデータがあってもアクセスできなくなる可能性もあります。一年程度のデータであれば CD-R や DVD-R にコピーすることも可能ですので、非常用

のノート PC を用意して、SS-MIX2 ビューアや HL7 FHIR クライアントを用意することも考えられます。システム関連事業者と事前によく相談しておくことが必要です。

非常時における緊急用のデータアクセスで過去の記録まで用意することは一般的には難しく、対応も複雑になり経費もかかります。非常時はインシデント発生以前のデータは閲覧のみと割り切って、紙ベースで運用することも一つの方法です。その際、非常時の真っ只中や非常時からの復旧を急いで対応している中、データの事後入力や再入力が必要になりますが、非常時においては、診療の継続性の確保が優先すべき状況であるため、やむを得ないことだと考えられます。

4. 対策

サイバーセキュリティを確保するために医療情報システムの稼働を支えるサーバや端末、ネットワーク等の機器、様々なシステム群の構成管理、そして、システムを利用・管理する利用者・管理者をシステム関連事業者の担当者も含めてリストアップし、かつ、複数のシステムが互いに連携したり、制御し合ったりして稼働しているためシステム自体も管理対象としてリストアップして、医療情報システムの稼働に接するすべてのアカウントの管理を行うことが重要である。そして、これらの多数の構成とアカウントが正常な動作をしていることをモニタリングし、正常ではない動き等をするのがないように制御、または、異常な動き等を検知した際には、予防的措置を発動する、というような監視を含め、ガバナンスを働かせる必要がある。

次に、ガバナンスを働かせていたとしてもサイバーインシデントの被害に遭う、という非常時を想定して、システムとの共存環境において、非常時における運用面の方針や判断基準や手順等を BCP（Business Continuity Plan：事業継続計画）として定め、業務継続に必要なシステムやデータの冗長化や複製などの保管を行い、運用面からシステム面までトータルでのバックアップを策定しておく必要がある。

4. 1 ガバナンス

現在の医療情報システムは複雑で、外部サービスを利用することもありますし、機器やシステムの保守を外部からオンラインで行うこともあります。このような場合、外部接続するためのルータなどの機器や回線自体も外部事業者が管理している場合があります。この回線や通信機器あるいは外部事業者のシステムに脆弱性があると、ここが攻撃され、医療情報システム全体に被害が及びます。ガバナンスと言っても外部事業者を直接管理することはできませんので、医療機関としては接続の状況を把握し、契約等で、脆弱性が生じないように縛る必要があります。例えば、部門システムの保守は部門が業者と交渉し、契約も担当し、医療機関としては把握が不十分なことがあります。このような状況では患者に対して責任あるセキュリティ対策を行うことは不可能です。医療機関として接続状況を把握し、コントロールすることが必須です。

4. 1. 1 構成管理

医療情報システムの構成や利用するサービスの形態に応じて、システムやサービスを構成する機器や利用するネットワーク構成を一覧化し、システムが稼働するためのネットワークに接続する機器やネッ

トワーク経路を掌握し、不正な機器が接続されたり、不正なソフトウェアやデータが混入されたり、異常なデータ通信が発生したりすることがないように、管理する必要があります。

特に、セキュアなネットワークを整備する観点からは、ネットワークの論理的または物理的な構成の分割、接続機器の制御、通信するデータの制御等を実施し、セキュリティを確保することが重要です。

4. 1. 2 アカウント管理

医療情報システムを利用・管理する関係者をリストアップし、それぞれがどのような権限でどのようなシステムを操作するのかを掌握しておく必要があります。

特に、システム関連事業者を含めて、システムの管理を行う関係者のアカウントの管理は厳重に行う必要があります。

3. 3の項でも少し触れましたが、不正ソフトウェアはシステムを解析し、管理者権限を奪取し、防御を無力化します。管理者権限を奪取されると、アクティブディレクトリやLDAPのような利用者認証のコントロールは奪われますが、運用系とバックアップ系などのセキュリティ系の認証を分離しておくと、時間稼ぎにはなりますし、うまく行けばバックアップ系やセキュリティ系を守ることができます。

また、昨今の情報システムは複雑で、様々なシステムが互いに自動的に連携したり、支援・制御していたりします。アカウント管理に、システムやアプリケーション等のソフトウェアも含めて管理することが重要です。

WindowsのようなPCのOSでもサーバ系のLinux系のOSでも極めて多機能で、様々なプロセスがインストールされており、必要に応じて、あるいは自動的に起動されています。医療情報システムで利用しない機能は起動する必要はありません。起動していると、そのプロセスに脆弱性があればサイバー攻撃の侵入口になります。不要なプロセスやプログラムは削除あるいは起動しないようにシステム関連事業者に要求してください。また、実際に不要なプロセスが起動されていないかの監視も重要です。削除や起動静止していたプロセスが、セキュリティパッチによって再生することもあります。

4. 1. 3 監視

機器構成やアカウントを管理することで、システムやネットワークに対する不正な侵入が検知でき、不正アクセスを防止することが可能となり、さらには、不正な侵入等がなされた際においても、不正なソフトウェアやデータによる正常とは異なる振る舞いを検知する、監視の仕組みを整え、その効果を発揮することが可能となります。

不正侵入の検知や不正アクセスの防止を支援するシステムとしては、IDS（Intrusion Detection System：不正侵入検知システム）/IPS（Intrusion Prevention System：不正侵入防御システム）と称したセキュリティサービスが提供されています。

不正なソフトウェアやデータによる振る舞い検知によるセキュリティサービスとして、EDR（Endpoint Detective and Response）があります。最近の不正ソフトウェアの被害を見ると、従来のパターンマッチングによる不正ソフトウェア検出をすり抜ける不正ソフトウェアが多いと言えます（ゼロ・デイ攻撃）。100%検出できるわけではありませんが、不正ソフトウェアの異常な動きを検出して、被害が出る前に報告します。最近のコンピュータウイルス対策ソフトウェアには EDR 機能も持つものが増えていますが、ライセンス契約によっては活性化していないこともあります。EDR が導入されていればリスクを低下させることが可能です。

4. 2 バックアップ

ガバナンスを補完し、少しでもサイバーインシデントが発生した際に、混乱を最小限にとどめ、業務影響、復旧に要する時間等を最小限にするために、システムも含んだ運用面での方針等を定めた BCP の策定及びシステムやデータのバックアップの整備は重要です。

4. 2. 1 BCP（Business Continuity Plan：事業継続計画）

サイバーインシデントを 100%防止することは不可能ですし、大規模災害もないとは言えません。地域に一定の役割を担う医療機関としては BCP の策定と、BCP に基づく訓練、さらに BCP の持続的な見直しは必須です。昨今の状況を踏まえると、サイバーインシデントも BCP の重要なテーマです。大規模災害の BCP も重要ですが、サイバーインシデントも主要なテーマに入れて BCP を策定し運用してください。非常時には最悪の場合は紙運用や地域の他の医療機関等による支援も視野に含めることも必要です。

4. 2. 2 システム・データ

医療機関等の担う特性に応じて、「3. 3 必要最小限の対策：バックアップ（システム・データ）」を参照し、継続できる業務の範囲を広げ、サイバー攻撃による影響が少しでも軽減されるように、システムやデータのバックアップを策定する必要がある。

第5.2 版→第6.0 版 項目移行対応表

第5.2版記載内容			第6.0版								
項番	区分	内容	概説 (Overview)		経営管理編 (Governance)		企画管理編 (Management)		システム運用編 (Control)		Q&A
			記載の有無	記載箇所	記載の有無	記載箇所	記載の有無	記載箇所	記載の有無	記載箇所	記載の有無
1. はじめに	＝	(略)	レ	1、2.1							
2. 本ガイドラインの読み方	－	(略)	レ	3							
3. 本ガイドラインの対象システム及び対象情報	－	(略)	レ	2.2、2.3、4.7	レ	16					
4. 電子的な医療情報を扱う際の責任のあり方	－	(略)	レ	4.1	レ	1.1～1.4、5.3					
5. 情報の相互運用性と標準化について	－	(略)							レ	5	
6.1. 方針の制定と公表	C.最低限のガイドライン	1. 個人情報保護に関する方針を策定し、公開すること。	レ	4.4	レ	1.1	レ	1、2、2			
		2. 医療情報システムの安全管理に関する方針を策定すること。その方針には、次に掲げる事項を定めること。 ・ 理念（基本方針と管理目的の表明） ・ 医療情報システムで扱う情報の範囲 ・ 情報の取扱いや保存の方法及び期間 ・ 不要・不法なアクセスを防止するための利用者識別の方法 ・ 医療情報システム安全管理責任者 ・ 苦情・質問の窓口	レ	4.4	レ	1.1	レ	1、④			
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	B.考え方	(略)	レ	4.2							
6.2.1 ISMS構築の手順	B.考え方	(略)			レ	2.2	レ	6.2			
6.2.2 取扱い情報の把握	B.考え方	(略)					レ	6.1.2			
6.2.3. リスク分析	C.最低限のガイドライン	1. 医療情報システムで扱う情報を全てリストアップすること。	レ	4.5	レ	2.2	レ	6、②			
		2. リストアップした情報を、安全管理上の重要性に応じて分類し、常に最新の状態を維持すること。			レ	2.2	レ	6、②			
		3. リストアップした情報は、医療情報システム安全管理責任者が必要に応じて速やかに確認できる状態で管理すること。			レ	2.2	レ	6、1、2			
		4. リストアップした情報に対してリスク分析を実施すること。脅威に関してはリスク分析に関する解説（別冊）を参照	レ	4.5	レ	2.2	レ	6、⑤			
		5. 医療情報システムベンダ及びサービス事業者から技術的対策等の情報を収集すること。例えば、「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」（総務省・経済産業省 令和2年8月21日）における「サービス仕様適合開示書」を利用することが考えられる。	レ	4.5	レ	2.2	レ	6、⑥	レ	4②	
		6. 医療情報システムに関する全体構成図（ネットワーク構成図・システム構成図等）、及びシステム責任者一覧（設置事業者等含む）を作成し、常に最新の状態を維持すること。例えば、前述の「サービス仕様適合開示書」を利用することが考えられる。	レ	4.5	レ	2.2	レ	6、⑥	レ	2②	
		7. リスク分析により得られたリスクに対して、6.3章～6.12章に示す対策を実施すること。			レ	2.2	レ	6、⑧			
	D.推奨されるガイドライン	1. 上記1から7の結果を系統的に文書化して管理すること。			レ	2.2	レ	6、⑦			
6.3 組織的安全管理対策（体制、運用管理規程）	B.考え方	(略)			レ	3.2					
	C.最低限のガイドライン	1. 医療情報システム安全管理責任者を設置するとともに、医療情報システム運用担当者を限定すること。ただし、小規模医療機関等で役割が自明の場合は、明確な規程を定めなくとも良い。			レ	3.2	レ	3① 3③			
		2. 個人情報が参照可能な場所においては、来訪者の記録・識別、入退制限等の入退管理を定めること。			レ	3.2	レ	8③			
		3. 医療情報システムへのアクセス制限、記録、点検等を定めたアクセス管理規程を作成すること。	レ	4.4	レ	3.2	レ	8①			
		4. 個人情報の取扱いを委託する場合、委託契約において安全管理に関する条項を含めること。	レ	4.4	レ	3.2	レ	7⑤			
		5. 運用管理規程等において次の内容を定めること。 ・ 医療機関等の体制 ・ 契約書・マニュアル等の文書の管理方法 ・ リスクに対する予防措置、発生時の対応の方法 ・ 機器を用いる場合は機器の管理方法 ・ 個人情報の記録媒体の管理（保管・授受等）の方法 ・ 患者等への説明と同意を得る方法 ・ 監査 ・ 苦情・質問の受付窓口	レ	4.4	レ	3.2	レ				
6.4 物理的安全対策	B.考え方	(略)			レ	4.1					
	C.最低限のガイドライン	1. 個人情報が保存されている機器の設置場所及び記録媒体の保存場所には施錠すること。					レ	8③			
		2. 個人情報を入力・参照できる端末が設置されている区画は、業務時間帯以外は施錠するなど、運用管理規程等に基づき許可された者以外の者が立ち入ることができないようにするための対策を実施すること。ただし、上記の対策と同等レベルの他の対策がある場合はこの限りではない。					レ	15②			
		3. 個人情報が保存されている機器が設置されている区画への入退管理を実施すること。例えば、次に掲げる対策を実施すること。 ・ 入退者に名札等の着用を義務付ける。 ・ 台帳等によって入退者を記録する。 ・ 入退者の記録を定期的にチェックし、妥当性を確認する。					レ	15②			レ
		4. 個人情報が保存されている機器等の重要な機器に盗難防止用チェーン等を設置すること。					レ	8③	レ	12.3.1	
		5. 個人情報が入力・参照できる端末の覗き見防止対策を実施すること。							レ	1 2.3.2	
	D.推奨されるガイドライン	1. 情報管理上重要な区画に防犯カメラ、自動侵入監視装置等を設置すること。							レ	12②	レ
6.5 技術的安全対策	B.考え方	(略)			レ	4.1					
	C.最低限のガイドライン	1. 医療情報システムへのアクセスにおける利用者の識別・認証を行うこと。	レ	4.6	レ	4.1	レ	13①	レ	14①	
		2. 利用者の識別・認証にユーザIDとパスワードの組み合わせを用いる場合、それらの情報を、本人しか知り得ない状態に保つよう対策を実施すること。	レ	4.6			レ	13②	レ	14②	
		3. 利用者の識別・認証にICカード等のセキュリティ・デバイスを用いる場合、ICカードの破損等、セキュリティ・デバイスが利用できないときを想定し、緊急時の代替手段による一時的なアクセスルールを用意すること。							レ	14③	
		4. 利用者が個人情報を入力・参照できる端末から長時間離席する際に、正当な利用者以外の者による入力のおそれがある場合には、クリアスクリーン等の対策を実施させること。					レ	8③	レ	12.3.2	
		5. 動作確認等で個人情報を含むデータを使用するときは、漏えい等に十分留意すること。	レ	4.4			レ	15⑨	レ	10①	
		6. 利用者の職種・担当業務ごとに、アクセスできる診療録等の範囲（アクセス権限）を定め、アクセス権限に沿ったアクセス管理を行うこと。また人事異動等による利用者の担当業務の変更等に合わせて、アクセス権限の変更を行うことを、運用管理規程で定めること。なお、複数の職種の利用者がアクセスするシステムでは職種別のアクセス管理機能があることが求められるが、そのような機能がない場合は、システム更新までの期間、運用管理規程でアクセス可能範囲を定め、次項の操作記録を行うことでアクセス管理を実施する必要がある。			レ	4.2	レ	13③	レ	14.2	
		7. アクセスログを記録するとともに、定期的にログを確認すること。アクセスログは、少なくとも利用者のログイン時刻、アクセス時間及びログイン中に操作した医療情報が特定できるように記録すること。医療情報システムにアクセスログの記録機能があることが前提であるが、ない場合は、業務日誌等により操作者、操作内容等を記録すること。			レ	4.2	レ	5③	レ	17①	
		8. アクセスログへのアクセス制限を行い、アクセスログの不当な削除／改ざん／追加等を防止する対策を実施すること。	レ	4.4	レ	4.2	レ	5②	レ	17②	
		9. アクセスログの記録に用いる時刻情報は、信頼できるものを利用すること。利用する時刻情報は、医療機関等の内部で同期させるとともに、標準時刻と定期的に一致させる等の手段で診療事実の記録として問題のない範囲の精度を保つ必要がある。					レ	5①	レ	17③	
		10. システム構築時、適切に管理されていない記録媒体の使用時、外部からの情報受領時には、コンピュータウイルス等の不正なソフトウェアが混入していないか確認すること。適切に管理されていないと考えられる記録媒体を利用する際には、十分な安全確認を実施し、細心の注意を払って利用すること。					レ	9⑥	レ	8①	
		11. 常時不正なソフトウェアの混入を防ぐ適切な措置をとること。また、その対策の有効性・安全性の確認・維持（例えばパターンファイルの更新の確認・維持）を行うこと。	レ	4.4	レ	4.2	レ	15⑥	レ	8②	

第5.2版記載内容			第6.0版								
項番	区分	内容	概説 (Overview)		経営管理編 (Governance)		企画管理編 (Management)		システム運用編 (Control)		Q&A
		12. 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。なお、保守等でやむを得ずファイル送付等を行う場合、送信側で無害化処理が行われていることを確認すること。					レ	15⑥	レ	8④	
		13. 令和9年度時点で稼働していることが想定される医療情報システムを、今後、新規導入又は更新に際しては、二要素認証を採用するシステムの導入、又はこれに相当する対応を行うこと。					レ	15②	レ	14⑤	
		14. パスワードを利用者認証に使用する場合、次に掲げる対策を実施すること。 (1) 医療情報システム内のパスワードファイルは、パスワードを暗号化（不可逆変換によること）した状態で、適切な手法で管理・運用すること。また、利用者識別にICカード等其他の手段を併用した場合はシステムに応じたパスワードの運用方法を運用管理規程にて定めること。 (2) 利用者のパスワードの失念や、パスワード漏えいのおそれなどにより、医療情報システムの運用担当者がパスワードを変更する場合には、利用者の本人確認を行うとともに、どのような手法で本人確認を行ったのかを台帳に記載（本人確認を行った書類等のコピーを添付）すること。また、変更したパスワードは、利用者本人以外が知り得ない方法で通知すること。なお、パスワード漏えいのおそれがある場合には、速やかにパスワードの変更を含む適切な処置を講じること。 (3) 医療情報システムの運用担当者であっても、利用者のパスワードを推定できないようにすること（設定ファイルにパスワードが記載される等があってはならない）。 (4) パスワードは以下のいずれかを要件とする。 a. 英数字、記号を混在させた13文字以上の推定困難な文字列 b. 英数字、記号を混在させた8文字以上の推定困難な文字列を定期的に変更させる（最長でも2ヶ月以内） c. 二要素以上の認証の場合、英数字、記号を混在させた8文字以上の推定困難な文字列。ただし他の認証要素として必要な電子証明書等の使用にPIN等が設定されている場合には、この限りではない。 いずれのパスワードを設定した場合でも、他に講じられているセキュリティ対策等の内容を勘案して、全体として安全なパスワード漏えい対策が講じられていることを確認すること。 (5) 類推されやすいパスワードを使用させないこと。また、類似のパスワードを繰り返し使用させないこと。 なお、類推されやすいパスワードには、利用者の氏名や生年月日、辞書に記載されている単語等が含まれるものがある。				レ	15②	レ	14⑥	レ	
		15. 無線LANを利用する場合、次に掲げる対策を実施すること。 (1) 適切な利用者以外に無線LANを利用されないようにすること。例えば、ANY接続拒否等の対策を実施すること。 (2) 不正アクセス対策を実施すること。少なくともMACアドレスによるアクセス制限を実施すること。 (3) 不正な情報の取得を防止するため、WPA2-AES、WPA2-TKIP等により通信を暗号化すること。 (4) 電波を発する機器（携帯ゲーム機等）による電波干渉に留意すること。			レ	4.2	レ	15⑦	レ	13⑬	
		16. IoT機器を利用する場合、次に掲げる対策を実施すること。検査装置等に付属するシステム・機器についても同様である。 (1) IoT機器により医療情報を取り扱う場合は、製造販売業者から提供を受けた当該医療機器のサイバーセキュリティに関する情報を基にリスク分析を行い、その取扱いに係る運用管理規程を定めること。 (2) セキュリティ対策を十分に行うことが難しいウェアラブル端末や在宅設置のIoT機器を患者等に貸し出す際は、事前に、情報セキュリティ上のリスクと、患者等が留意すべきことについて患者等へ説明し、同意を得ること。また、機器に異常や不都合が発生した場合の問い合わせ先や医療機関等への連絡方法について、患者等に情報提供すること。 (3) IoT機器には、製品出荷後にファームウェア等に関する脆弱性が発見されることがある。システムやサービスの特徴を踏まえ、IoT機器のセキュリティ上重要なアップデートを必要なタイミングで適切に実施する方法を検討し、運用すること。 (4) 使用が終了した又は不具合のために使用を停止したIoT機器をネットワークに接続したまま放置すると不正に接続されるリスクがあるため、対策を実施すること。			レ	4.2	レ	9④	レ	8⑥	
	D.推奨されるガイドライン	1. 情報の区分管理を実施し、区分単位でアクセス管理を実施すること。	レ	4.6	レ	4.2	レ		レ	14.2	レ
		2. 個人情報を入力・参照できる端末から離席する場合、クローズ処理等（クリアスクリーン、ログオフ、パスワード付きスクリーンセーバーの起動等）を実施させること。					レ		レ		レ
		3. 外部のネットワークとの接続点やDBサーバ等の安全管理上の重要部分には、ファイアウォール（ステートフルインスペクションやそれと同等の機能を含む。）を設置し、ACL（アクセス制御リスト）等を適切に設定すること。					レ		レ		レ
		4. パスワードを利用者認証に使用する場合、次に掲げる対策を実施すること。 (1) パスワード入力が不成功に終わった場合、再入力に対して一定の不応時間を設定すること。 (2) パスワード再入力の失敗が一定回数を超えた場合、再入力を一定期間受け付けない仕組みとすること。					レ		レ		レ
		5. 利用者認証には、ID・パスワード＋バイオメトリクス又はICカード等のセキュリティ・デバイス＋パスワード若しくはバイオメトリクスのように、2つの独立した要素を用いて行う方式（二要素認証）等、より認証強度が高い方式を採用すること。ただし、医療情報システムを利用する端末に二要素認証が実装されていないとしても、端末操作を行う区画への入場に当たって利用者の認証を行う等して、入場時・端末利用時を含め二要素以上（記憶・生体計測・物理媒体のいずれか2つ以上）の認証がなされていれば、二要素認証に相当すると考えてよい。					レ	13②	レ	14②	レ
		6. 許可された者以外の無線LANの利用を防止するため、例えば802.1xや電子証明書を組み合わせるなどして、無線LANのセキュリティを強化すること。	レ	4.6			レ	13.4	レ		レ
		7. IoT機器を含む医療情報システムの接続状況や異常発生を把握するため、IoT機器・医療情報システムそれぞれの状態や他の機器との通信状態を収集・把握し、ログとして適切に記録すること。			レ	4.2	レ	13.4	レ		レ
6.6 人的安全対策	B.考え方	(略)			レ	3.2					
	C.最低限のガイドライン	1. 従業者に対する人的安全管理措置 (1) 法令上の守秘義務のある者以外の者を従業者等として採用するに当たって、雇用契約に守秘・非開示に関する条項を含める等の安全管理対策を実施すること。	レ	4.4	レ	3.2	レ	7①			
		1. 従業者に対する人的安全管理措置 (2) 従業者に対し個人情報の安全管理に関する教育訓練を定期的に実施すること。	レ	4.4	レ	3.2	レ	7②			
		1. 従業者に対する人的安全管理措置 (3) 従業者の退職後の個人情報保護規程を定めること。	レ	4.4	レ	3.2	レ	7①			
		2. 事務取扱委託業者の監督及び守秘義務契約 (1) 医療機関等の事務、運用等を外部の事業者に委託する場合は、個人情報保護のため、次に掲げる対策を実施すること。 a 受託する事業者に対する罰則を定めた就業規則等で裏付けられた包括的な守秘契約を締結すること。 b 保守作業等の医療情報システムに直接アクセスする作業の際には、作業者、作業内容及び作業結果を確認すること。 c 清掃等の直接医療情報システムにアクセスしない作業の場合でも、作業結果を定期的に確認すること。 d 受託する事業者が再委託を行うか否かを明確にすること。受託する事業者が再委託を行う場合は、受託する事業者と同等の個人情報保護に関する対策及び契約がなされることを条件とすること。			レ	3.2	レ	1② 7③④			
		2. 事務取扱委託業者の監督及び守秘義務契約 (2) ソフトウェアの異常等でデータを救済する必要があるとき等、やむを得ない事情で受託する事業者の保守要員が医療情報にアクセスする場合は、罰則のある就業規則等で裏付けられた守秘契約等の秘密保持の対策を行うこと。			レ	3.2	レ	7③④			
	D.推奨されるガイドライン	1. サーバ室等の安全管理上重要な場所では、モニタリング等により従業者の行動を管理すること。					レ	8③	レ	12	レ
6.7 情報の破壊	B.考え方	(略)			レ	4.1					
	C.最低限のガイドライン	3. 6.2章C.1で把握した情報種別ごとに破壊の手順を定めること。手順には破壊を行う条件、破壊を行うことができる従業者、具体的な破壊方法を含めること。					レ	8①	レ	7⑨	
		2. 情報処理機器自体を破壊する場合、必ず専門的な知識を有するものが行うこと。また、破壊終了後に、残存し、読み出し可能な情報がないことを確認すること。					レ	8⑨	レ	7⑩	
		3. 外部保存を受託する事業者等に破壊を委託した場合は、6.6章C.2に従うとともに、確実に情報が破壊されたことを確認すること。					レ	8⑩	レ	7⑪	
		4. 運用管理規程において、不要になった個人情報を含む媒体の破壊に関する規定を定めること。					レ	8⑨			
6.8 情報システムの改造と保守	B.考え方	(略)			レ	4.1					
	C.最低限のガイドライン	1. 動作確認で個人情報を含むデータを使用するときは、明確に守秘義務を設定するとともに、終了後は確実にデータを消去させること。 2. メンテナンスを実施するためにサーバに保守事業者の作業員（保守要員）がアクセスする際には、保守要員の専用アカウントを使用させ、個人情報へのアクセスの有無並びに個人情報にアクセスした場合の対象個人情報の及び作業内容を記録すること。なお、これは利用者を模して操作確認を行う際の識別・認証についても同様である。					レ	15⑨	レ	10①	
							レ	13⑤	レ	10③	

第5.2版記載内容			第6.0版									
項番	区分	内容	概説 (Overview)		経営管理編 (Governance)		企画管理編 (Management)		システム運用編 (Control)		Q&A	
		3. 保守要員の専用アカウントについて、外部流出等による不正使用の防止の観点から適切に管理することを求めること。					レ	13⑤			レ	
		4. 保守要員の離職や担当替え等に応じて速やかに保守要員の専用アカウントを削除できるよう、保守事業者に報告を義務付けるとともに、それに対応できるアカウント管理体制を整備すること。			レ	4.1	レ	13⑤⑦	レ	10③	レ	
		5. 保守事業者がメンテナンスを実施する際には、日単位で作業申請書を事前提出させるとともに、終了時に速やかに作業報告書を提出させること。提出された書類は、医療情報システム安全管理責任者が承認すること。なお、作業申請書の承認は、原則として保守作業の実施前に行う必要があるが、事前に承認を得ずに実施可能なものとして保守事業者と合意したメンテナンスについては、事後承認とすることができる。					レ	15⑧	レ	10.1	レ	
		6. 保守事業者と守秘義務契約を締結し、これを遵守させること。			レ	4.1	レ	7③				
		7. 原則として、保守事業者に個人情報を含むデータを医療機関等外等に持ち出させないこと。やむを得ず医療機関等外に持ち出さなければならない場合は、置き忘れ等に対する十分な対策を含む運用管理規程を定めることを求め、医療情報システム安全管理責任者がそれを承認すること。					レ	8⑤	レ	7.1		
		8. リモートメンテナンスによるシステムの改造・保守作業が行われる場合には、必ずアクセスログを収集するとともに、当該作業の終了後速やかに医療機関等の責任者が確認すること。					レ	15⑧	レ	10④		
		9. リモートメンテナンスにおいて、やむを得ずファイルを医療機関等へ送付等を行う場合、送信側で無害化処理が行われていることを確認すること。					レ	15⑧	レ	10⑤		
		10. 再委託が行われる場合は、再委託を受ける事業者に対しても、保守事業者の責任で同等の義務を課させること。	レ	4.4	レ	5	レ	1②	レ	3.3		
		D.推奨されるガイドライン	1. 詳細なオペレーション記録を保守操作ログとして記録すること。									レ
		2. 保守作業は医療機関等の関係者の立会いの下で行わせること。										レ
	3. 保守要員と保守事業者との守秘義務契約を求めること。										レ	
	4. 保守要員の持ち込む機器や記憶媒体に対して、不正ソフトウェアがないことを確認すること。										レ	
	5. 保守事業者がやむを得ず個人情報を含むデータを医療機関等外に持ち出さなければならない場合には、詳細な作業記録を残すよう求めること。また、必要に応じて、医療機関等の監査に応じるよう求めること。										レ	
	6. 保守作業に関わるログの確認の際に、アクセスした診療録等の識別情報を時系列順に並べて表示し、かつ指定時間内でどの患者の診療録等に何回アクセスされたか確認できる仕組みを備えること。										レ	
	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	B.考え方	(略)			レ	2.2、3、4					
		C.最低限のガイドライン	1. 組織としてリスク分析を実施し、情報及び情報機器の持ち出しや、BYODの実施に関する方針を運用管理規程で定めること。	レ	4.4	レ	3.2	レ	9⑥	レ	7.1 8.4	
			2. 運用管理規程には、持ち出した情報及び情報機器の管理方法を定めること。					レ	8①			
			3. 情報を格納した可搬媒体又は情報機器の盗難、紛失時の対応を運用管理規程に定めること。					レ	8⑦			
			4. 運用管理規程で定めた盗難、紛失時の対応に従業者等に周知徹底するとともに、教育を実施すること。					レ	7②			
			5. 情報が格納された可搬媒体及び情報機器の所在を台帳等により管理すること。					レ	9①②	レ	7⑦	
6. 情報機器に対して起動パスワード等を設定すること。設定に当たっては推定しやすいパスワード等の利用を避けるとともに、定期的なパスワードの変更等の対策を実施すること。			レ	4.6	レ	3.2	レ	13⑥	レ	8⑤		
7. 盗難、置き忘れ等に対応する措置として、情報に対する暗号化やアクセスパスワードの設定等、容易に内容を読み取られないようにすること。							レ	8⑤	レ	7③		
8. 持ち出した情報機器について、外部のネットワークや他の外部媒体に接続したりする場合は、コンピュータウイルス対策ソフトやパーソナルファイアウォールの導入等により、情報端末が情報漏えい、改ざん等の対象にならないような対策を実施すること。なお、ネットワークに接続する場合は6.11章の規定を遵守すること。特に、スマートフォンやタブレットのようなモバイル端末では公衆無線LANを利用できる場合があるが、公衆無線LANは6.5章C.15.の基準を満たさないことがあるため、利用できない。ただし、非常時等でやむを得ず公衆無線LANしか利用できない環境である場合に限り、利用を認める。利用する場合は6.11章で述べている基準を満たした通信手段を選択すること。							レ	8⑤	レ	7④		
9. 持ち出した情報を取り扱う情報機器には、必要最小限のアプリケーションのみをインストールすること。業務に使用しないアプリケーションや機能については削除又は停止するか、業務に対して影響がないことを確認すること。							レ	8⑤	レ	7⑥		
10. 個人所有の情報機器（ノートパソコン、スマートフォン、タブレット等）であっても、業務上、医療機関等の情報を持ち出して取り扱う場合は、医療情報システム安全管理責任者は1～5の対策を行うとともに、医療情報システム安全管理責任者の責任において上記の6、7、8、9と同様の要件を遵守させること。			レ	3.2	レ	9⑥	レ	8.4				
D.推奨されるガイドライン	1. 外部での情報機器の覗き見による情報の漏えいを避けるため、ディスプレイに覗き見防止フィルタ等を張ること。							レ	12⑥	レ		
	2. 情報機器のログインや情報へのアクセス時には複数の認証要素を組み合わせて用いること。							レ		レ		
	3. 情報格納用の可搬媒体や情報機器は全て登録し、登録されていない機器による情報の持ち出しを禁止すること。	レ	4.4	レ	3	レ	9⑥	レ	8⑨	レ		
	4. ノートパソコン、スマートフォン、タブレット等を持ち出して使用する場合、次に掲げる対策を実施すること。 (1) 紛失、盗難の可能性を十分考慮し、可能な限り端末内に医療情報を置かないこと。やむを得ず医療情報が端末内に存在する場合や、当該端末を利用すれば容易に医療情報にアクセスできる場合は、一定回数パスワード入力を誤った場合に端末を初期化する等の対策を行うこと。 (2) BYODを行う場合は、管理者以外による端末のOSの設定の変更を技術的あるいは運用管理上で制御する等、適切な技術的対策や運用による対策を選択・採用し、十分な安全性が確保された上で行うこと。					レ	9⑥	レ	8⑨	レ		
6.10 災害、サイバー攻撃等の非常時の対応	B.考え方	(略)			レ	3.4						
	C.最低限のガイドライン	1. 医療サービスを提供し続けるためのBCPの一環として、“非常時”と判断するための基準、手順、判断者等及び正常復帰時の手順をあらかじめ定めておくこと。	レ	4.4	レ	3.4	レ	11①				
		2. 非常時における対応に関する教育及び訓練に従業者に対して行うこと。なお、医療情報システムの障害時の対応についても同様に行うこと。	レ	4.4	レ	3.4	レ	11⑥				
		3. 正常復帰後に、代替手段で運用した間のデータ整合性を図るための規約を用意すること。					レ	11①				
		4. 非常時の医療情報システムの運用について、次に掲げる対策を実施すること。 (1) 「非常時のユーザアカウントや非常時用機能」の管理手順を整備すること。 (2) 非常時機能が定常時に不適切に利用されることがないようにするとともに、もし使用された場合に使用されたことが検知できるよう、適切に管理及び監査すること。 (3) 非常時用ユーザアカウントが使用された場合、正常復帰後は継続使用ができないように変更すること。 (4) 医療情報システムに不正ソフトウェアが混入した場合に備えて、関係先への連絡手段や紙での運用等の代替手段を準備すること。 (5) 重要なファイルは数世代バックアップを複数の方式で取得し、その一部は不正ソフトウェアの混入による影響が波及しない手段で管理するとともに、バックアップからの重要なファイルの復元手順を整備すること。					レ	11④⑤	レ	11①		

第5.2版記載内容			第6.0版								
項番	区分	内容	概説 (Overview)		経営管理編 (Governance)		企画管理編 (Management)		システム運用編 (Control)		Q&A
		5. 不正ソフトウェアの混入などによるサイバー攻撃を受けた（疑い含む）場合や、サイバー攻撃により障害が発生し、個人情報の漏洩や医療提供体制に支障が生じる又はそのおそれがある事案であると判断された場合には、「医療機関等におけるサイバーセキュリティ対策の強化について」（医政総発1029 第1号 医政地発1029 第3号 医政研発1029 第1号 平成30年10月29日）に基づき、所管官庁への連絡等、必要な対応を行うほか、そのための体制を整備すること。また上記に関わらず、医療情報システムに障害が発生した場合も、必要に応じて所管官庁への連絡を行うこと。 厚生労働省連絡先 https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryou/iryou/johoka/cyber-security.html ※ 独立行政法人等においては、各法人の情報セキュリティポリシー等に基づき所管課へ連絡すること。 なお、情報処理推進機構は、5. 不正ソフトウェアや不正アクセスに関する技術的な相談を受け付ける窓口を開設している。標的型メールを受信した、Webサイトが何者かに改ざんされた、不正アクセスを受けた等のおそれがある場合は、下記連絡先に相談することが可能である。 連絡先 情報処理推進機構 情報セキュリティ安心相談窓口（03-5978-7509）	レ	4.4	レ	3.4	レ	11⑧			
6.11 外部と個人情報を含む医療情報を交換する場合の安全管理	B.考え方 C.最低限のガイドライン	(略) 1. ネットワーク経路でのメッセージ挿入、不正ソフトウェアの混入等の改ざん及び中間者攻撃等を防止する対策を実施すること。 施設間の経路上においてクラッカーによるパスワード盗聴、本文の盗聴を防止する対策を実施すること。 セッション乗っ取り、IPアドレス詐称等のなりすましを防止する対策を実施すること。 上記を満たす対策としては、①クローズドなネットワークを選択する、又は②オープンなネットワークを選択する場合、例えばIPsecとIKEを利用する等してセキュアな通信路を確保すること又は、IPsecによるVPN接続等を利用せず医療情報システムへ接続する場合は、後述の11.に示す方法等により実施すること。 チャネル・セキュリティの確保を開域ネットワークに期待してネットワークを構成する場合には、選択するサービスの閉域性の範囲を電気通信事業者を確認すること。 2. クローズドなネットワーク、オープンなネットワークのいずれを選択する場合であっても、データ送信元と送信先での、ルータ等の拠点の出入り口・使用機器・使用機器上の機能単位・利用者等の選択するネットワークに応じた必要な単位で、相手の確認を行う必要がある。採用する通信方式や運用管理規程により、採用する認証手段を決めること。採用する認証手段は、PKIによる認証、Kerberosのような鍵配布、事前配布された共通鍵の利用、ワンタイムパスワード等、容易に解読されない方法が望ましい。 3. 施設内において、正規利用者へのなりすまし、許可機器へのなりすましを防ぐ対策を実施すること。これに関しては、6.5章で包括的に述べているので、それを参照すること。 4. クローズドなネットワーク、オープンなネットワークのいずれを選択する場合であっても、ルータ等のネットワーク機器は、安全性が確認できる機器を利用すること。VPN接続による場合は、施設内のルータを経由して異なる施設間を結ぶ通信経路の間で送受信ができないように経路を設定すること。安全性が確認できる機器とは、例えば、ISO 15408で規定されるセキュリティターゲット又はそれに類するセキュリティ対策が規定された文書が本ガイドラインに適合していることを確認できるものをいう。 5. クローズドなネットワーク、オープンなネットワークのいずれを選択する場合であっても、送信元と相手先の当事者間で当該情報そのものに対する暗号化等のセキュリティ対策を実施すること。例えば、S/MIMEの利用、ファイルに対する暗号化等の対策が考えられる。その際、暗号化の鍵については電子政府推奨暗号のものを使用すること。 6. 医療機関等間の情報通信には、医療機関等だけでなく、電気通信事業者やシステムインテグレータ、運用を受託する事業者、遠隔保守を行う機器保守事業者等の多くの組織が関連する。そのため、次に掲げる事項について、これら関連組織の責任分界点、責任の所在を契約書等で明確にすること。 ・診療録等を含む医療情報を、送信先の医療機関等に送信するタイミングと一連の情報交換に関わる操作を開始する動作の決定 ・送信元の医療機関等がネットワークに接続できない場合の対処 ・送信先の医療機関等がネットワークに接続できなかった場合の対処 ・ネットワークの経路途中が不通の場合又は著しい遅延が発生している場合の対処 ・送信先の医療機関等が受け取った保存情報を正しく受信できなかった場合の対処 ・伝送情報の暗号化に不具合があった場合の対処 ・送信元の医療機関等と送信先の医療機関等の認証に不具合があった場合の対処 ・障害が起こった場合に障害部位を切り分ける責任 ・送信元の医療機関等又は送信先の医療機関等が情報交換を中止する場合の対処 また、医療機関等内においても、次に掲げる事項を契約や運用管理規程等で定めておくこと。 ・通信機器、暗号化装置、認証装置等の管理責任（外部事業者へ管理を委託する場合は、責任分界点も含めた整理と契約の締結） ・患者等に対する説明責任 ・事故発生時における復旧作業・他施設やシステムベンダ及びサービス事業者との連絡に当たる専任の管理者の設置 ・交換した医療情報等に対する管理責任及び事後責任（個人情報の取扱いに関して患者から照会等があった場合の送信元、送信先双方の医療機関等への連絡に関する事項、またその場合の個人情報の取扱いに関する秘密事項） 7. 医療情報システムを内部ネットワークを通じて外部ネットワークに接続する際には、なりすまし、盗聴、改ざん、侵入及び妨害等の脅威に留意したうえで、ネットワーク、機器、サービス等を適切に選定し、監視を行うこと。 8. リモートメンテナンスを実施する場合は、必要に応じて、適切なアクセスポイントの設定、プロトコルの限定、アクセス権限管理等、不必要なログインを防止するための対策を実施すること。 また、サイバー攻撃への対策については、PCやVPN機器等の脆弱性対策をはじめとする6.5章及び6.6章に記載されている内容や、NISCから示されている「政府機関等のサイバーセキュリティ対策のための統一基準群（令和3年度版）」、2021年4月30日の「ランサムウェアによるサイバー攻撃に関する注意喚起について」も参照すること。メンテナンス自体は6.8章を参照すること。 9.電気通信事業者やオンラインサービス提供事業者と契約を締結する際には、脅威に対する管理責任の範囲や回線の可用性等の品質を確認すること。また、上記1及び4を満たしていることを電気通信事業者やオンラインサービス提供事業者を確認すること。 10.患者等に情報を閲覧させる場合、情報を公開しているコンピュータシステムを通じて、医療機関等の内部のシステムに不正な侵入等が起こらないように、例えば、システムやアプリケーションを切り分け、ファイアウォール、アクセス監視、通信のTLS暗号化、PKI個人認証等の対策を実施すること。また、情報の主体者となる患者等へ危険性や提供目的についての納得できる説明を行い、ITに係る以外の法令等の遵守の体制等も含めた幅広い対策を立て、それぞれの責任を明確にすること。 11.オープンなネットワークにおいて、IPsecによるVPN接続等を利用せずHTTPSを利用する場合、TLSのプロトコルバージョンをTLS1.3以上に限定した上で、クライアント証明書を利用したTLSクライアント認証を実施すること。ただしシステム・サービス等の対応が困難な場合にはTLS1.2の設定によることも可能とする。その際、TLSの設定はサーバ/クライアントともに「TLS暗号設定ガイドライン3.0.1版」に規定される最も安全性水準の高い「高セキュリティ型」に準じた適切な設定を行うこと。なお、SSL-VPNは利用する具体的な方法によっては偽サーバへの対策が不十分なものが含まれるため、使用するには適切な手法の選択及び必要な対策を行うこと。また、ソフトウェア型のIPsec又はTLS1.2以上により接続する場合、セッション間の回り込み（正規のルートではないクローズドセッションへのアクセス）等による攻撃への適切な対策を実施すること。 12. クローズドなネットワークで接続する場合でも、内部トラフィックにおける脅威の拡散等を防止するために、不正ソフトウェア対策ソフトのパターンファイルやOSのセキュリティ・パッチ等、リスクに対してセキュリティ対策を適切に適用すること。 13. 電子署名に用いる秘密鍵の管理は、認証局が定める「証明書ポリシー」（CP）等で定める鍵の管理の要件を満たして行うこと。			レ	4			レ	13⑨	
							レ	15⑦	レ	13④	
							レ				
							レ	15⑦	レ	13⑤	
									レ	13⑦	レ
					レ	4	レ	2①	レ	13①	
					レ	4	レ	7⑥	レ	13⑪	
					レ	4	レ	12⑤	レ	10.1 18.1	
					レ	4	レ	15⑩	レ	10.1	
							レ	8⑧	レ	7④	
							レ	15⑦	レ	13⑥	
							レ	15⑦	レ	13③	
							レ	14②	レ	15.1	
	D.推奨されるガイドライン	1. やむを得ず従業者による外部からのアクセスを許可する場合は、PCの作業環境内に仮想的に安全管理された環境をVPN技術と組み合わせて実現する仮想デスクトップのような技術を用いるとともに、運用等の要件を設定すること。 2. 共通鍵、秘密鍵を格納する機器、媒体については、FIPS140-2レベル1相当以上の対応を図ること。					レ	8⑧	レ	7.2.1	レ
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	B.考え方 C.最低限のガイドライン	(略) 法令で署名又は記名・押印が義務付けられた文書において、記名・押印を電子署名に代える場合、以下の条件を満たす電子署名を行う必要がある。			レ	4	レ	14①			

第5.2版記載内容			第6.0版							
項番	区分	内容	概説 (Overview)	経営管理編 (Governance)	企画管理編 (Management)	システム運用編 (Control)	Q&A			
		1. 以下の電子証明書を用いて電子署名を施すこと (1) A項の要件を満たす電子署名を施すこと。なお、これはローカル署名のほか、リモート署名、立会人型電子署名の場合も同様である。 (2) 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については、以下の（a）～（c）のいずれかにより、医師等の国家資格の確認が電子的に検証できる電子署名等を用いること。 (a) 厚生労働省の定める準拠性監査基準を満たす保健医療福祉分野PKI認証局の発行する電子証明書を用いて電子署名を施すこと。 保健医療福祉分野PKI認証局は、電子証明書内に医師等の保健医療福祉に係る資格を格納しており、その資格を証明する認証基盤として構築されている。したがって、この保健医療福祉分野PKI認証局の発行する電子署名を活用すると電子的な本人確認に加え、同時に、医師等の国家資格を電子的に確認することが可能である。ただし、当該電子署名を施された文書を受け取る者が、国家資格を含めた電子署名の検証を正しくできることが必要である。 (b) 認定認証事業者（電子署名法第2条第3項に定める特定認証業務を行う者として主務大臣の認定を受けた者をいう。以下同じ。）又は認証事業者（電子署名法第2条第2項の認証業務を行う者（認定認証事業者を除く。）をいう。）の発行する電子証明書を用いて電子署名を施すこと。その場合、当該電子署名を施された文書を受け取る者が、医師等の国家資格の確認を電子的に検証でき、電子署名の検証を正しくできることが必要である。事業者（認証局あるいは立会人型電子署名の場合は電子署名サービス提供事業者をいう。以下6.12.において同じ）を選定する際には、事業者が次に掲げる事項を適切に実施していることについて確認すること（ローカル署名のほか、リモート署名、立会人型電子署名の場合も同様）。				レ	14①			
		・ 事業者による利用者の実在性、本人性及び利用者個人の申請意思の確認に当たっては、オンラインの場合、「電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律」（平成14年法律第153号）第3条第1項に規定する署名用電子証明書に係る電子署名により確認を行うこと。マイナンバーカードによる確認が行えない場合は、身分証明書と住民票等の公的証明書をスキャンしたデータ（いずれも本項と同等の電子署名（資格確認を除く）を施すこと）により確認を行うこと。郵送の場合は、身分証明書のコピー（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））、住民票等の公的証明書により確認を行うこと。対面の場合は、身分証明書と住民票等の公的証明書により確認を行うこと。なお、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。 ※ 身分証明書の確認は、公的な写真付きの身分証明書であればマイナンバーカード、運転免許証、パスポート等のいずれか1種類により、又はその他の身分証明書であれば2種類以上により行うこと。 ・ 事業者による利用者の医師等の国家資格保有の確認は、①利用者が保健医療福祉分野PKI認証局の発行する署名用証明書をを用いた電子署名を事業者へ提供することによりオンラインで行う方法、②利用者が官公庁の発行した国家資格を証明する書類（以下「国家資格免許証等」という。）の原本又はコピー等（紙媒体の場合は、国家資格免許証等のコピーに署名又は押印（実印が捺印され、印鑑登録証明書が添えてあること）があること。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。）を事業者へ持参、郵送又は送信する方法、③利用者が電子署名による確認方法以外の電子的に国家資格等情報と連携して提示できる仕組みを用いて事業者へ提示する方法、④利用者の所属又は運営する医療機関等が利用者の国家資格保有の事実の立証を事業者へ行う方法、のいずれかによって利用者の登録時において確認すること（電子署名を行う都度、事業者による医師等の国家資格保有の確認を求めるものではない）。なお、①～③の場合、事業者は、資格確認に用いた国家資格免許証等のコピーや証明書等について、保存年限を定めて保存し				レ	14①			
		－ 医療機関等の管理者が、自組織の実在性を事業者に対して立証すること。 － 医療機関等の管理者が国家資格保有の確認を行った者の「氏名、生年月日、性別、住所」（以下「基本4情報」という。）を事業者へ提出すること（これによって、利用者が実在性、本人性及び利用者個人の申請意思を立証した際に、国家資格保有の立証もなされたものとみなすこととする）。 － 医療機関等による医師等の国家資格保有の立証に当たって、医療機関等が責任の主体としての説明責任を果たすため、資格確認を行った実施記録の作成を行うとともに、資格確認を実施した国家資格免許証等のコピーや利用者の基本4情報を提出した書類のコピー等について保存年限を定めて保存し、さらに医療機関等の内部の独立した監査部門による定期的な監査を行うこと。 ・ 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。 ※ ①～④のいずれかによって資格確認を行った後、利用可能となった当該電子署名を利用者が他の事業者に提供した場合、提供を受けた事業者が別途資格の確認を行う必要はない。なお、この場合であっても以下の事項を行うこと。 ・ 適切な外部からの評価を受けること。 ・ 資格確認に用いた証明書等について、保存年限を定めて保存しておくこと。 (c) 「電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律」（平成14年法律第153号）に基づき、平成16年1月29日から開始されている公的個人認証サービスを用いることも可能であるが、その場合、その署名用電子証明書に係る電子署名に紐づく医師等の国家資格が検証時に電子的に確認できること、当該電子署名を施された文書を受け取る者が公的個人認証サービスを用いた電子署名を検証することが必要である。				レ	14①			
		2. 電子署名を含む文書全体にタイムスタンプを付与すること (1) タイムスタンプは、第三者による検証を可能にするため、「タイムビジネスに係る指針－ネットワークの安心な利用と電子データの安全な長期保存のために－」（総務省、平成16年11月）等で示されている時刻認証業務の基準に準拠し、一般財団法人日本データ通信協会が認定した時刻認証事業者のものを使用すること。 (2) 法定保存期間中、タイムスタンプの有効性を継続できるようにするための対策を実施すること。 (3) タイムスタンプの利用や長期保存に関しては、今後も、関係府省の通知や指針の内容や標準技術、関係ガイドラインに留意しながら適切に対策を実施すること。				レ	14①			
		2. 法定保存期間等の必要な期間、電子署名の検証を継続して行うことができるよう、必要に応じて電子署名を含む文書全体にタイムスタンプを付与すること (1) タイムスタンプは、第三者による検証を可能にするため、「時刻認証業務の認定に関する規程」（令和3年4月1日、総務省告示第146号）に基づき認定された事業者（認定事業者）が提供するものを使用すること。なお、一般財団法人日本データ通信協会が認定した時刻認証事業者（「タイムビジネスに係る指針」（総務省、平成16年11月）等で示されている時刻認証業務の基準に準拠し、一般財団法人日本データ通信協会が認定した時刻認証事業者。以下「認定時刻認証事業者」という。）については、令和4年以降、国による認定制度に順次移行する予定であることから、当面の間、認定時刻認証事業者によるものを使用しても差し支え無い。 (2) 法定保存期間中、タイムスタンプの有効性を継続できるようにするための対策を実施すること。 (3) タイムスタンプの利用や長期保存に関しては、今後も、関係府省の通知や指針の内容や標準技術、関係ガイドラインに留意しながら適切に対策を実施すること。 (4) タイムスタンプを付与する時点で有効な電子証明書を用いること。 当然ではあるが、有効な電子証明書を用いて電子署名を行わなければならない。本来法定保存期間は電子署名自体が検証可能であることが求められるが、タイムスタンプが検証可能であれば電子署名を含めて改変の事実がないことが証明されるため、タイムスタンプ付与時点で電子署名が検証可能であれば、電子署名付与時点での有効性を検証することが可能である。具体的には、電子署名が有効である間に、電子署名の検証に必要なとなる情報（関連する電子証明書や失効情報等）を収集し、署名対象文書と署名値とともにその全体に対してタイムスタンプを付与する等の対策が必要である。				レ	14①			
7.1 真正性の確保について	B.考え方	(略)		レ	1.1					
	C.最低限のガイドライン 【医療機関等に保存する場合】	1. 入力者及び確定者の識別・認証 (1) 電子カルテシステム等でPC等の汎用入力端末により記録が作成される場合 a 入力者及び確定者を正しく識別し、認証を行うこと。 b システムへの全ての入力操作について、対象情報ごとに入力者の職種や所属等の必要な区分に基づいた権限管理（アクセスコントロール）を定めること。また、権限のある入力者以外による作成、追記、変更を防止すること。 c 業務アプリケーションが稼動可能な端末を管理し、権限を持たない者からのアクセスを防止すること。 (2) 臨床検査システム、医用画像ファイリングシステム等、特定の装置又はシステムにより記録が作成される場合 a 装置の操作者を運用管理規程で明確にするとともに操作者以外のものによる機器の操作を運用上防止すること。 b 当該装置による記録をいつ・誰が行ったか、システム機能と運用の組み合わせにより明確にすること。		レ	1.1	レ	13.⑧ 15⑬			

第5.2版記載内容			第6.0版								
項番	区分	内容	概説 (Overview)		経営管理編 (Governance)		企画管理編 (Management)		システム運用編 (Control)		Q&A
		2. 記録の確定手順の確立と、識別情報の記録 (1) 電子カルテシステム等でPC等の汎用入力端末により記録が作成される場合 a 診療録等の作成・保存を行おうとする場合、確定された情報を登録できる仕組みをシステムに備えること。その際、登録する情報に、入力者及び確定者の氏名等の識別情報、信頼できる時刻源を用いた作成日時を含めること。 b 「記録の確定」を行うに当たり、内容を十分に確認できるようにすること。 c 「記録の確定」は、確定を実施できる権限を持った確定者に実施させること。 d 確定された記録に対する故意の虚偽入力、書換え、消去及び混同を防止するための対策を実施するとともに、原状回復のための手順を検討しておくこと。 e 一定時間経過後に記録が自動確定するような運用の場合は、入力者及び確定者を特定する明確なルールを運用管理規程に定めること。 f 確定者が何らかの理由で確定操作ができない場合における記録の確定の責任の所在を明確にすること。例えば、医療情報システム安全管理責任者が記録の確定を実施する等のルールを運用管理規程に定めること。 (2) 臨床検査システム、医用画像ファイリングシステム等、特定の装置又はシステムにより記録が作成される場合 a 運用管理規程等に当該装置により作成された記録の確定ルールを定義すること。その際、当該装置の管理責任者や操作者の氏名等の識別情報（又は装置の識別情報）、信頼できる時刻源を用いた作成日時を記録に含めること。 b 確定された記録が、故意の虚偽入力、書換え、消去及び混同を防止するための対策を実施するとともに、原状回復のための手順を検討しておくこと。			レ	1.1	レ	13.⑧ 15⑬	レ	14⑧	
		3. 更新履歴の保存 (1) 一旦確定した診療録等を更新する場合、更新履歴を保存し、必要に応じて更新前と更新後の内容を照らし合わせることができるようにすること。 (2) 同じ診療録等に対して複数回更新が行われた場合でも、更新の順序性が識別できるようにすること。			レ	1.1	レ	13.⑧ 15⑬	レ	14⑧	
		4. 代行入力の承認機能 (1) 代行入力を実施する場合、具体的にどの業務等に代行入力を認めるか、誰が誰を代行してよいかを運用管理規程で定めること。 (2) 代行入力が行われた場合には、誰の代行がいつ誰によって行われたかの管理情報を、代行入力の都度記録すること。 (3) 代行入力により記録された診療録等は、できるだけ速やかに確定者による「確定操作（承認）」が行われるようにすること。この際、内容の確認を行わずに確定操作を行ってはならない。			レ	1.1	レ	13.⑧ 15⑬	レ	14⑧	
		5. 機器・ソフトウェアの品質管理 (1) システムがどのような機器、ソフトウェアで構成され、どのような場面、用途で利用されるのかを明らかにするとともに、システムの仕様を明確に定義すること。 (2) 機器、ソフトウェアの改訂履歴、その導入の際に実際に行われた作業の妥当性を検証するためのプロセスを規定すること。 (3) 機器、ソフトウェアの品質管理に関する作業内容を運用管理規程で定めるとともに、従業者等への教育を実施すること。 (4) システム構成やソフトウェアの動作状況に関する内部監査を定期的に実施すること。			レ	1.1	レ	15⑬	レ	9.2	
	C.最低限のガイドライン 【ネットワークを通じて医療機関等の外部に保存する場合】	6. 通信の相手先が正当であることを認識するための相互認証を行うこと 診療録等のオンライン外部保存を受託する事業者と委託する医療機関等が、互いに通信目的とする正当な相手かどうかを認識するための相互認証機能が必要である。					レ	15⑦	レ	13⑫	
		7. ネットワーク上で「改ざん」されていないことを保証すること ネットワークの転送途中で診療録等が改ざんされていないことを保証できるようにすること。なお、可逆的な情報の圧縮・解凍、セキュリティ確保のためのタグ付け、暗号化・復号等は改ざんにはあたらない。					レ	15⑦ 15⑬	レ	13⑧	
		8. リモートログイン機能を制限すること 保守作業等のどうしても必要な場合を除いてリモートログインを行うことができないように、適切に管理されたリモートログインのみに制限する機能を設けなければならない。					レ	8⑧ 15⑬	レ	7⑫	
7.2 見読性の確保について	B.考え方	(略)			レ	1.1					
	C.最低限のガイドライン	1. 情報の所在管理 紙管理された情報を含め、各種媒体に分散管理された情報であっても、患者ごとの全ての情報の所在が日常的に管理されていること。					レ	8④ 15⑬	レ	4①	
		2. 見読化手段の管理 電子媒体に保存された全ての情報とそれらの見読化手段を対応付けて管理すること。また、見読化手段である機器、ソフトウェア、関連情報等は常に整備された状態にすること。					レ	15⑬	レ	5④	
		3. 見読目的に応じた応答時間 目的に応じて速やかに検索表示又は書面に表示できるようにすること。					レ	15⑬	レ	9④	
		4. システム障害対策としての冗長性の確保 システムの一系統に障害が発生した場合でも、通常の診療等に差し支えない範囲で診療録等を見読可能とするため、システムの冗長化（障害の発生時にもシステム全体の機能を維持するため、平常時からサーバやネットワーク機器等の予備設備を準備し、運用すること）を行う又は代替的な見読化手段を用意すること。			レ	1.1	レ	15⑬	レ	11.2	
	D.推奨されるガイドライン 【医療機関等に保存する場合】	1. バックアップサーバ システムが停止した場合でも、バックアップサーバと汎用的なブラウザ等を用いて、日常診療に必要な最低限の診療録等を見読できるようにすること。									レ
		2. 見読性確保のための外部出力 システムが停止した場合でも、見読目的に該当する患者の一連の診療録等を汎用のブラウザ等で見読できるように、見読性を確保した形式で外部ファイルへ出力できるようにすること。									レ
		3. 遠隔地のデータバックアップを使用した見読機能 大規模火災等の災害対策として、遠隔地に電子保存記録をバックアップするとともに、そのバックアップデータ等と汎用的なブラウザ等を用いて、日常診療に必要な最低限の診療録等を見読できるようにすること。									レ
		4. 緊急に必要なことが予測される診療録等の見読性の確保 緊急に必要なことが予測される診療録等は、内部に保存するか、外部に保存しているものの複製又は同等の内容の情報を医療機関等の内部に保持すること。									レ
		5. 緊急に必要なこととまではいえない診療録等の見読性の確保 緊急に必要なこととまではいえない情報についても、ネットワークや外部保存を受託する事業者の障害等に対応できるような対策を実施しておくこと。									レ
7.3 保存性の確保について	B.考え方	(略)			レ	3、4					
	C.最低限のガイドライン 【医療機関等に保存する場合】	1. 不正ソフトウェアによる情報の破壊、混同等の防止 (1) 不正ソフトウェアによる情報の破壊、混同等が起こらないように、システムで利用するソフトウェア、機器及び媒体を適切に管理すること。	レ	4.4	レ	3、4	レ	15⑥ 15⑬	レ	8.1	

第5.2版記載内容			第6.0版									
項番	区分	内容	概説 (Overview)		経営管理編 (Governance)		企画管理編 (Management)		システム運用編 (Control)		Q&A	
		2. 不適切な保管・取扱いによる情報の滅失、破壊の防止 (1) 記録媒体及び記録機器の保管及び取扱いについて、運用管理規程を作成し、適切な保管及び取扱いを行うよう関係者に周知徹底するとともに、教育を実施すること。また、保管及び取扱いに関する作業履歴を残すこと。 (2) システムが情報を保存する場所（内部、可搬媒体）を明示し、その場所ごとの保存可能容量（サイズ）、期間、リスク、レスポンス、バックアップ頻度、バックアップ方法等を明確にすること。これらを運用管理規程に定めて、その運用を関係者全員に周知徹底すること。 (3) 記録媒体の保管場所やサーバの設置場所等には、許可された者以外が入室できないような対策を実施すること。 (4) 電子的に保存された診療録等の情報に対するアクセス履歴を残すとともに、その履歴を適切に管理すること。 (5) 各保存場所における情報が毀損したときに、バックアップされたデータ等を用いて毀損前の状態に戻せるようにすること。もし、毀損前と同じ状態に戻せない場合には、毀損された範囲が容易に分かるようにしておくこと。			レ	3、4	レ	15②③ 15⑬	レ	12.2 18.1		
		3. 記録媒体、設備の劣化による情報の読み取り不能又は不完全な読み取りの防止 (1) 記録媒体が劣化する前に、当該記録媒体に保存されている情報を新たな記録媒体又は記録機器に複写すること。記録媒体及び機器ごとに劣化が起これずに正常に保存が行える期間を明確にするとともに、使用開始日、使用終了予定日を管理して、月に一回程度の頻度でチェックを行うこと。使用終了予定日が近づいた記録媒体又は記録機器は、そのデータを新しい記録媒体又は記録機器に複写すること。これらの一連の運用の流れを運用管理規程に定めるとともに、関係者に周知徹底すること。					レ	15⑬	レ	12.2		
		4. 媒体・機器・ソフトウェアの不整合による情報の復元不能の防止 (1) システム更新の際の移行を迅速に行えるように、診療録等のデータについて、標準形式が存在する項目は標準形式で、標準形式が存在しない項目は変換が容易なデータ形式で、それぞれ出力及び入力できる機能を備えること。 (2) マスタデータベースの変更の際に、過去の診療録等の情報に対する内容の変更が起これない機能を備えること。					レ	15⑬	レ	5①		
		C.最低限のガイドライン 【ネットワークを通じて医療機関等の外部に保存する場合】	5. データ形式及び転送プロトコルのバージョン管理と継続性の確保を行うこと 保存義務のある期間中に、データ形式や転送プロトコルがバージョンアップ又は変更されることが考えられる。その場合、外部保存を受託する事業者は、以前のデータ形式や転送プロトコルを使用している医療機関等が存在する間に対応を維持しなくてはならない。			レ	3、4	レ	15⑬	レ	5③	
		6. ネットワークや外部保存を受託する事業者に設備の劣化対策の実施を求めること ネットワークや外部保存を受託する事業者の設備の条件を考慮し、回線や設備が劣化した際にそれらを更新する等の対策を実施するよう求めること。			レ	3、4	レ	15⑬	レ	12.2		
		D. 推奨されるガイドライン 【医療機関等に保存する場合】	1. 不適切な保管・取扱いによる情報の滅失・破壊の防止 (1) 記録媒体、記録機器及びサーバは、許可された者しか入ることができない部屋に保管するとともに、その部屋の入室履歴を残し、保管及び取扱いに関する作業履歴と関連付けて保存すること。 (2) サーバ室には、許可された者以外が入室できないよう、鍵等の物理的な対策を施すこと。 (3) 診療録等のデータのバックアップを定期的に取得するとともに、その内容に対する改ざん等が行われていないことを検査する機能を備えること。 2. 記録媒体、設備の劣化による情報の読み取り不能又は不完全な読み取りの防止 診療録等の情報をハードディスク等の記録機器に保存する場合は、RAID-1又はRAID-6相当以上のディスク障害に対する対策を行うこと。					レ	8③	レ	12②	レ
	8 診療録及び診療諸記録を外部に保存する際の基準	－						レ	7			
	8.1 電子保存の3基準の遵守							レ	1.1.2			
	8.2 運用管理規程	B.考え方	(略)			レ	3.2	レ	16			
	8.3. 外部保存を受託する事業者の選定基準及び情報の取扱いに関する基準	C.最低限のガイドライン	1. 病院、診療所、医療法人等が適切に管理する場所に保存する場合 (1) 病院や診療所、医療法人等が適切に管理する場所に診療録等を保存すること。 (2) 委託した医療機関等及び患者等の許可なく、保存を受託した診療録等を分析等の目的で取り扱わせないこと。 (3) 保存を受託した診療録等の分析等は、不当な利益を目的としない場合に限って許可すること。 (4) 匿名化した情報であっても、匿名化の妥当性の検証を行う、及び院内掲示等を使って取扱いをしている事実を患者等に知らせるなどして、個人情報保護に配慮した上で取り扱わせること。 (5) 保存を受託する医療機関等に患者がアクセスし、自らの記録を閲覧できるような仕組みを提供する場合は、外部保存を受託する事業者に適切なアクセス権を設定し、情報漏えいや、誤った閲覧（異なる患者の情報を見せてしまう又は患者に見せてはいけない情報が見えてしまう等）が起これないように配慮するよう求めること。 (6) 情報の提供は、原則、患者が受診している医療機関等と患者間の同意に基づいて実施すること。 2. 医療機関等が外部の事業者との契約に基づいて確保した安全な場所に保存する場合 (1) 保存した情報の取扱いに関して監督できるようにするため、外部保存を受託する事業者及びその管理者、電子保存作業従事者等に対する守秘に関連する事項やその事項に違反した場合のペナルティを契約書等で定めること。 (2) 医療機関等と外部保存を受託する事業者を結ぶネットワーク回線に関しては6.11章を遵守させること。 (3) 総務省・経済産業省の定めた「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」を遵守することを契約等で明確に定め、少なくとも定期的に報告を受ける等で確認をすること。 (4) 外部保存を受託する事業者の選定に当たっては、事業者のセキュリティ対策状況を示す資料を確認すること。例えば、「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」の提供を求めて、確認することなどが挙げられる。 (5) 外部保存を受託する事業者は、契約書等で合意した保守作業に必要な情報以外の情報を閲覧させないこと。なお保守に関しては、6.8章を遵守すること。 (6) 保存した情報（Cookie、匿名加工情報等、個人を特定しない情報を含む。本項において以下同じ。）を独断で分析、解析等を実施してはならないことを契約書等に明記するとともに、外部保存を受託する事業者に遵守させること。 (7) 保存した情報を、外部保存を受託する事業者が独自に提供しないように、契約書等で情報提供について定めること。外部保存を受託する事業者が提供に係るアクセス権を設定する場合は、適切な権限を設定させ、情報漏えいや、誤った閲覧（異なる患者の情報を見せてしまう又は患者に見せてはいけない情報が見えてしまう等）が起これないようにさせること。 (8) 保存された情報を格納する機器等が、国内法の適用を受けることを確認すること。			レ	5	レ	7⑤			

第5.2版記載内容			第6.0版								
項番	区分	内容	概説 (Overview)		経営管理編 (Governance)		企画管理編 (Management)		システム運用編 (Control)		Q&A
		(9) 外部保存を受託する事業者を選定する際は、(1)から(8)のほか、少なくとも次に掲げる事項について確認すること。 a 医療情報等の安全管理に係る基本方針・取扱規程等の整備状況 b 医療情報等の安全管理に係る実施体制の整備状況 c 不正ソフトウェア等のサイバー攻撃による被害を防止するために必要なバックアップの取得及び管理の状況 d 実績等に基づく個人データ安全管理に関する信用度 e 財務諸表等に基づく経営の健全性 f プライバシーマーク認定又はISMS認証を取得していること g 「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」の「セキュリティクラウド認証等」に示す下記のいずれかの認証等により、適切な外部保存に求められる技術及び運用管理能力の有無 ・政府情報システムのためのセキュリティ評価制度（ISMAP） ・JASAクラウドセキュリティ推進協議会CSゴールドマーク ・米国 FedRAMP ・AICPA SOC2（日本公認会計士協会 IT7号） ・AICPA SOC3（SysTrust/WebTrust）（日本公認会計士協会 IT2号） 上記認証等が確認できない場合、下記のいずれかの資格を有する者による外部監査結果により、上記と同等の能力の有無を確認すること ・システム監査技術者 ・Certified Information Systems Auditor ISACA認定 h 医療情報を保存する機器が設置されている場所(地域、国) i 受託事業者に対する国外法の適用可能性			レ	5	レ	7⑥			
	D. 推奨されるガイドライン	1. ISMS認証を取得している事業者の選定に際しては、選定対象となる事業者に管理しているリスクに応じて、適合性を示す資料の提供を求めること。 2. 医療機関等が外部の事業者との契約に基づいて確保した安全な場所に保存する場合では、技術的な方法として、例えばトラブル発生時のデータ修復作業等緊急時の対応を除き、原則として委託する医療機関等のみがデータ内容を閲覧できることを担保するよう求めること。 3. 外部保存を受託する事業者に保存される個人識別に係る情報の暗号化を行い適切に管理することや、外部保存を受託する事業者の管理者といえども通常はアクセスできない制御機構をもつこと。具体的には、「暗号化を行う」、「情報を分散保管する」という方法が考えられる。その場合、非常時等の通常とは異なる状況下でアクセスすることも想定し、アクセスした事実が医療機関等で明示的に識別できる機構を備えるよう求めること。					レ				レ
											レ
8.4. 個人情報の保護	B.考え方 C.最低限のガイドライン	(略) 1. 診療録等の外部保存を受託する事業者内における個人情報保護 (1) 委託先を適切に監督すること 診療録等の外部保存を受託する事業者内の個人情報保護については、本ガイドライン6章を参照し、適切な管理を行わせる必要がある。 2. 外部保存実施に関する患者への説明 外部保存の委託に当たり、あらかじめ患者に対して、必要に応じて個人情報が特定の外部の施設に送付・保存されることについて、その安全性やリスクを含めて院内掲示等を通じて説明し、理解を得る必要がある。 (1) 診療開始前の説明 患者から、病態、病歴等を含めた個人情報を収集する前に行われるべきであり、外部保存を行っている旨を、院内掲示等を通じて説明し理解を得た上で診療を開始すること。 (2) 患者本人に説明をすることが困難であるが、診療上の緊急性がある場合 意識障害や認知症等で本人への説明をすることが困難な場合で、診療上の緊急性がある場合は必ずしも事前の説明を必要としない。意識が回復した場合には事後に説明を行い、理解を得る必要がある。 (3) 患者本人に説明することが困難であるが、診療上の緊急性が特にない場合 乳幼児の場合も含めて本人に説明し理解を得ることが困難で、緊急性のない場合は、原則として親権者や保護者に説明し、理解を得ること。ただし、親権者による虐待が疑われる場合や保護者がいない等、説明をすることが困難な場合は、診療録等に、説明が困難な理由を明記しておくことが望まれる。			レ レ	4 5	 レ	 7⑧			
					レ	1.1、1.2	レ	7⑨			
9.1. 共通の要件	C.最低限のガイドライン	1. 医療に関する業務等に支障が生じることのないよう、スキャンによる情報量の低下を防ぎ、保存義務を満たす情報として必要な情報量を確保するため、光学解像度、センサ等の一定の規格・基準を満たすスキャナを用いること。また、スキャンによる電子化で情報が欠落することがないよう、スキャン等を行う前に対象書類に他の書類が重なって貼り付けられていたり、スキャナ等が電子化可能な範囲外に情報が存在しないか確認すること。 (1) 診療情報提供書等の紙媒体の場合、診療等の用途に差し支えない精度でスキャンを行うこと。 (2) 放射線フィルム等の高精細な情報をスキャンする場合、日本医学放射線学会電子情報委員会が公表した「デジタル画像の取り扱いに関するガイドライン3.0版（平成27年4月）」を参考にすること。 (3) このほか心電図等の波形情報やボラロイド撮影した情報等、様々な対象が考えられるが、医療に関する業務等に差し支えない精度でスキャンする必要があるため、その点に十分配慮すること。 (4) 一般の書類をスキャンした画像情報は、汎用性が高く可視化するソフトウェアに困らない形式で保存すること。また非可逆的な圧縮は画像の精度を低下させるため、非可逆圧縮を行う場合は医療に関する業務等に支障がなく、スキャンの対象となった紙等の破損や汚れ等の状況も判定可能な精度を保つよう留意する必要がある。放射線フィルム等の医用画像をスキャンした情報はDICOM等の適切な形式で保存すること。 2. 改ざんを防止するため、次に掲げる対策を実施すること。 (1) スキャナによる読み取りについて運用管理規程に定めること。 (2) スキャナにより読み取った電子情報と元の文書等から得られる情報と同等であることを担保する情報作成管理者を配置すること。 (3) スキャナによる読み取りの際の責任を明確にするため、作業責任者（実施者又は情報作成管理者）が電子署名法に適合した電子署名を遅滞なく行うこと。なお、電子署名については6.12章を参照すること。 3. 情報作成管理者は、運用管理規程に基づき、スキャナによる読み取り作業が、適正な手続で確実に実施される措置を講じること。					レ レ	16① 16①②③	レ	16①	レ
					レ	4.1	レ	16①②③			
							レ	16④			
9.2. 診療等の都度スキャナ等で電子化して保存する場合	C.最低限のガイドライン	1. 9.1章の対策に加えて、情報が作成されてから又は情報を入手してから一定期間以内にスキャンを行うこと。 (1) 運用管理規程において、改ざんの動機が生じないと考えられる期間（長くとも1～2日程度以内）を定めるとともに、その期間内に遅滞なくスキャンを行わなければならない。時間外診療等で機器の使用ができない等のやむを得ない事情がある場合は、スキャンが可能になった時点で遅滞なく行う必要がある。			レ	4.1	レ	16⑤			
9.3. 過去に蓄積された紙媒体等をスキャナ等で電子化保存する場合	C.最低限のガイドライン	1. 対象となる患者等に、スキャナ等で電子化して保存することを事前に院内掲示等で周知すること。異議の申立てがあった場合、その患者等の情報は電子化を行わないこと。			レ	4.1	レ	16⑥			

第5.2版記載内容			第6.0版								
項番	区分	内容	概説 (Overview)		経営管理編 (Governance)		企画管理編 (Management)		システム運用編 (Control)		Q&A
		2. 必ず実施前に実施計画書を作成すること。実施計画書には次に掲げる事項を含めること。 (1) 運用管理規程の作成と妥当性の評価方法（評価は、大規模医療機関等にあっては、外部の有識者を含む公正性を確保した委員会等で行うこと（倫理委員会を用いることも可）） (2) 作業責任者 (3) 患者等への周知の手段と異議の申立てに対する対応方法 (4) 相互監視を含む実施体制 (5) 実施記録の作成と記録項目（次項の監査に耐え得る記録を作成すること） (6) 事後の監査人と監査項目 (7) スキャン等で電子化を行ってから紙やフィルムの破棄までの期間及び破棄方法			レ	4.1	レ	16⑥			
		3. 医療機関等の保有するスキャナ等で電子化を行う場合、事後の監査は、システム監査技術者やCertified Information Systems Auditor（ISACA認定）等の適切な能力を持つ外部監査人によって実施すること。					レ	16⑥			
		4. 外部事業者に委託する場合は、9.1章の対策と同等以上の安全性を満たすことができる適切な事業者を選定すること。適切な事業者とみなすためには、少なくともプライバシーマークを取得しており、過去に情報の安全管理や個人情報保護上の問題を起こしていない事業者であることを確認する必要がある。また、実施に際しては、システム監査技術者やCertified Information Systems Auditor（ISACA認定）等の適切な能力を持つ外部監査人の監査を受けることを含め、安全管理に関する条項を契約書等に具体的に明記すること。			レ	4.1	レ	16⑥			
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	C.最低限のガイドライン	1. 紙の調剤済み処方箋の電子化のタイミングに応じて、9.2章又は9.3章の対策を実施すること。					レ	16⑦			
		2. 「電子化した紙の調剤済み処方箋」を修正する場合、「『元の』電子化した紙の調剤済み処方箋」を電子的に修正し、「『修正後の』電子化した紙の調剤済み処方箋」に対して薬剤師の電子署名が必須となる。電子的に修正する際には、「『元の』電子化した紙の調剤済み処方箋」の電子署名の検証が正しく行われる形で修正すること。					レ	16⑦	レ	16.1	
9.5（補足） 運用の利便性のためにスキャナ等で電子化を行うが、紙等の媒体もそのまま保存を行う場合	C.最低限のガイドライン	1. 医療に関する業務等に支障が生じることのないよう、スキャンによる情報量の低下を防ぐため、光学解像度、センサ等の一定の規格・基準を満たすスキャナを用いること。 (1) 診療情報提供書等の紙媒体の場合、診療等の用途に差し支えない精度でスキャンすること。これは、紙媒体を別途保存する場合でも、紙媒体は電子化情報に比べてアクセスの容易さが低く、電子化情報が主に使用される可能性があるため、電子化情報について元の文書等の見読性を可能な限り保つことが求められるからである。ただし、元々プリンタ等で印字された情報等、スキャン精度をある程度落としても見読性が低下しない場合は、診療に差し支えない見読性が保たれることを前提にスキャン精度を下げることもできる。 (2) 放射線フィルム等の高精細な情報をスキャンする場合、日本医学放射線学会電子情報委員会が公表した「デジタル画像の取り扱いに関するガイドライン3.0版（平成27年4月）」を参考にすること。 (3) このほか心電図等の波形情報やボラロイド撮影した情報等、様々な対象が考えられるが、医療に関する業務等に差し支えない精度でスキャンする必要があるため、その点に十分配慮すること。 (4) 一般の書類をスキャンした画像情報は、汎用性が高く可視化するソフトウェアに困らない形式で保存すること。また非可逆的な圧縮は画像の精度を低下させるために、非可逆圧縮を行う場合は医療に関する業務等に支障がなく、スキャンの対象となった紙等の破損や汚れ等の状況も判定可能な精度を保つよう留意する必要がある。放射線フィルム等の医用画像情報をスキャンした情報はDICOM等の適切な形式で保存すること。					レ	16⑧	レ	16②	
		2. 情報作成管理者は、運用管理規程を定めて、スキャナによる読み取り作業が、適正な手続で確実に実施される措置を講じること。					レ	16⑧			
		3. 緊急に閲覧が必要になったときに迅速に対応できるよう、保存している紙媒体等の検索性も必要に応じて維持すること。					レ	16⑧			
		4. 電子化後の元の紙媒体やフィルムの安全管理を行うこと。					レ	16⑧			
10. 運用管理について	C.最低限のガイドライン	以下の項目を運用管理規程に含めること。本ガイドラインの4章から9章において「D. 推奨されるガイドライン」に記載されている項目は省略しても差し支えない。 1. 一般管理事項 2. 電子保存のための運用管理事項 3. ネットワークによる外部保存に当たっての「医療機関等としての管理事項」 可搬媒体による外部保存、紙媒体による外部保存に当たっては、本項を参照して管理事項を作成すること。			レ	4.1	レ	4.2、8.2.5など			
					レ	4.1	レ	15③～⑤			
					レ	4.1	レ	15④			
		4. スキャナ等により電子化して保存する場合			レ	4.1	レ	16①、③～⑥			
		5. 運用管理規程の作成に当たって			レ	4.1	レ	4.2			

各編間相関表

経営管理編				企画管理編				システム運用編					
記載箇所				記載箇所				備考					
遵守事項				遵守事項				遵守事項					
1.1安全管理に関する法令の遵守			① 医療情報システムの安全管理に関する法令等を遵守すること。	52版のA項に関する前掲を対策として新設	1. 管理体系	① 医療情報システムの管理に関する法令等について理解し、医療機関等の組織全体として法令等を遵守できるよう、必要な措置を講じること。	1. 情報セキュリティの基本的な考え方	① 法令上求められる医療情報システムに関する要件等について、企画管理者の整理に基づいて、必要な技術的な対応を抽出し、各システムの整備において措置を行うほか、必要な手順、資料の作成を行うこと。	10C2-4				
			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。	52版のA項に関する前掲を対策として新設	1. 管理体系	② 委託先の医療情報システム・サービス事業者等に対して①に関連して必要な措置を講じよう契約において求め、その対応状況を定期的に把握すること。委託先事業者が再委託を用いる場合も同様の対応をすること。							
					1. 管理体系	③ 医療機関等内における法令の遵守状況について経営層に報告し、経営層の承認を得ること。また、遵守状況に応じて必要な改善措置を講じること。							
					11. 非常時（災害、インシデント、サイバー攻撃被害）対応とBCP策定	③ 非常時において、法令で求められる対応を事前に整理し、非常時に速やかに対応できる体制を講じること。							
						④ 法令で署名又は記名・押印が義務付けられた文書において、記名・押印を電子署名に代える場合、以下の条件を満たす電子署名を行うこと。 1. 以下の電子証明書を用いて電子署名を施すこと (1) 「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）第2条第1項に規定する電子署名を施すこと。なお、これはローカル署名のほか、リモート署名、立会人型電子署名の場合も同様である。 (2) 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については、以下の（a）～（c）のいずれかにより、医師等の国家資格の確認が電子的に検証できる電子証明書を用いた電子署名等を用いること。【以下略】 2. 法定保存期間等の必要な期間、電子署名の検証を継続して行うことができるよう、必要に応じて電子署名を含む文書全体にタイムスタンプを付与すること (1) タイムスタンプは、第三者による検証を可能にするため、「時刻認証業務の認定に関する規程」に基づき認定された事業者（認定事業者）が提供するものを使用すること。なお、一般財団法人日本データ通信協会が認定した時刻認証事業者（タイムビジネスに係る指針等で示されている時刻認証業務の基準に準拠し、一般財団法人日本データ通信協会が認定した時刻認証事業者、以下「認定時刻認証事業者」という。）については、令和4年以降、国による認定制度に順次移行する予定であることから、当面の間、認定時刻認証事業者によるものを使用しても差し支え無い。 (2) 法定保存期間中、タイムスタンプの有効性を継続できるようにするための対策を実施すること。 (3) タイムスタンプの利用や長期保存に関しては、今後も、関係府省の通知や指針の内容や標準技術、関係ガイドラインに留意しながら適切に対策を実施すること。 (4) タイムスタンプを付与する時点で有効な電子証明書を用いること。							
					14. 法令で定められた記名・押印のための電子署名								
1.2 医療機関等における責任		通常時における責任	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。	52版第4の趣旨を踏まえて新設	4. 医療情報の安全管理において必要な規程・文書類の整備	① 医療機関等が医療情報システムの安全管理に関して定める各種方針等を実現するために必要な規程等の整備を行い、経営層の承認を得ること。							
					4. 医療情報の安全管理において必要な規程・文書類の整備	② 規程等に基づいて、医療情報の取扱いや医療情報システムの構築、運用を行うために必要な規程等の整備を行うこと。規則類は必要に応じて見直しを行うこと。							
					4. 医療情報の安全管理において必要な規程・文書類の整備	③ 医療情報システムの構築、運用における通常時の対応に必要なマニュアル類や各種資料の整備を担当者に指示し、確認すること。	2. システム設計・運用に必要な規程類と文書体系			③ 医療情報システムの維持及び運用に必要な手順を整備し、常に最新の状態を維持すること。	10C1-4		
					4. 医療情報の安全管理において必要な規程・文書類の整備	④ 非常時における医療情報システムの運用等に関するマニュアル類や各種資料の整備を担当者に指示し、整備状況を確認の上、経営層に報告すること。	2. システム設計・運用に必要な規程類と文書体系			④ 医療情報システムの利用者が適切に医療情報システムの利用ができるよう、マニュアル等の整備を行うこと。	10C1		
							2. システム設計・運用に必要な規程類と文書体系			① 医療情報システムにおいて採用するシステム、サービス、情報機器等の機能仕様及び利用方法に関する資料を整備し、常に最新の状態を維持すること。	6.2C4 6.9C5		
							2. システム設計・運用に必要な規程類と文書体系			② 医療情報システムに関する全体構成図（ネットワーク構成図・システム構成図等）、及びシステム責任者・関係者一覧（設置事業者、保守事業者等含む）を作成し、常に最新の状態を維持すること。	6.2C4		
			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。	52版第4の趣旨を踏まえて新設	1. 管理体系	⑦ 患者等からの問い合わせに対応するために必要な医療情報システムの安全管理に関する窓口等を整備すること。							
					3. 医療機関等における安全管理のための体制と責任・権限	⑨ 患者等からの相談や苦情への対応を行うための体制を構築すること。							
					7. 安全管理のための人的管理（従業員管理、委託先管理、教育・訓練、委託先選定・契約）	⑩ 外部保存の委託に当たり、あらかじめ患者に対して、必要に応じて個人情報が特定の外部の施設に送付・保存されることについて、その安全性やリスクを含めて院内掲示等を通じて説明し、理解を得ること。							
					8. 情報管理（管理、持出し、破棄等）	⑪ 患者等に情報を閲覧させるために医療情報システムへのアクセスを許可する場合には、患者等に対して、情報セキュリティに関するリスクや情報提供目的について説明を行い、それぞれの責任範囲を明確にすること。							
			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、6.3C1-5に必要な組織体制を整備すること。	6.3C1-5 第10章	1. 管理体系	④ 医療情報システムの安全管理に係る法令等が求める内容を把握した上で、対応策を整備すること。必要に応じて、システム運用担当者具体的な対策について検討を求めて、その結果を反映すること。							
			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。	6.3C1-5 第10章	3. 医療機関等における安全管理のための体制と責任・権限	⑤ 医療情報の取扱いの安全性が確保できるよう、内部検査及び監査等の体制を構築すること。							
			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。	52版第5章の趣旨を踏まえて新設	10. 運用に対する点検・監査	④ 医療情報システムの取扱いの安全管理の状況を客観的に把握するために、定期的に、医療機関等内の企画管理者や担当者から独立した組織又は第三者による監査を実施すること。監査の実施に際しては、監査方針と監査計画を策定の上、経営層の承認を得ること。また、監査結果について、経営層に報告し、承認を得ること。監査結果における指摘事項を踏まえて、適宜管理の見直し等を図ること。							
					11. 非常時（災害、インシデント、サイバー攻撃被害）対応とBCP策定	⑤ 医療機関等が定める非常時の定義やBCP（Business Continuity Plan：事業継続計画）との整合性を確認して対応方針を策定すること。							
					12. サイバー攻撃対策	⑥ サイバーセキュリティ事象による非常時対応が生じた場合には、その状況について、定期的に経営層に報告すること。また、当該事象を踏まえ、サイバーセキュリティ対応計画の検証・見直しを実施し、必要に応じて改善を行うこと。							
【定期的に見直し必要に応じて改善を行う責任】		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。	52版6.2の趣旨を踏まえて新設	4. 医療情報の安全管理において必要な規程・文書類の整備	⑤ 規程等に基づいて、医療情報の取扱いや医療情報システムの構築、運用を行うために必要な規程等の整備を行うこと。規則類は必要に応じて見直しを行うこと。								
					10. 運用に対する点検・監査	④ 医療情報システムの取扱いの安全管理の状況を客観的に把握するために、定期的に、医療機関等内の企画管理者や担当者から独立した組織又は第三者による監査を実施すること。監査の実施に際しては、監査方針と監査計画を策定の上、経営層の承認を得ること。また、監査結果について、経営層に報告し、承認を得ること。監査結果における指摘事項を踏まえて、適宜管理の見直し等を図ること。							
					12. サイバー攻撃対策	⑥ サイバーセキュリティ事象による非常時対応が生じた場合には、その状況について、定期的に経営層に報告すること。また、当該事象を踏まえ、サイバーセキュリティ対応計画の検証・見直しを実施し、必要に応じて改善を行うこと。							
					15. 技術的な対策の管理	⑥ システム運用に関する安全管理対策として必要な項目を担当者と協議して検討すること。特に医療情報システムの脆弱性（不正ソフトウェア対策ソフトウェアやサイバー攻撃含む）への対策に関する項目については、定期的に見直しを図ること。							
			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。	6.10C5	52版4.1(B)(2)①の趣旨を加味	⑧ 非常時の事象が生じた場合、安全管理の状況を適宜把握し、経営層に報告すること。							
					11. 非常時（災害、インシデント、サイバー攻撃被害）対応とBCP策定	⑨ 非常時の事象が生じた場合、関係者に対する説明責任等を果たすため、報告対応や広報対応を行うこと。							
					12. サイバー攻撃対策	① サイバーセキュリティに関する組織的対策、医療機関等の職員等や委託先事業者などの対策を検討し、整理すること。技術的な対応・措置については、担当者にリスク評価を踏まえた対策の検討を指示し、状況を確認すること。							
					12. サイバー攻撃対策	⑦ サイバー攻撃を受けた（疑い含む）場合や、サイバー攻撃により障害が発生し、個人情報の漏洩や医療サービスの提供体制に支障が生じる又はそのおそれがある事業であると判別された場合には、「医療機関等におけるサイバーセキュリティ対策の強化について」（医政総発1029第1号）（医政総発1029第3号 医政研発1029第1号 平成30年10月29日）に基づき、所管官庁への連絡等の必要な対応を行うほか、そのために必要な体制を整備すること。また、上記に関わらず、医療情報システムに障害が発生した場合は、必要に応じて所管官庁への連絡を行うこと。							
			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。	52版6.10B(4)の趣旨を踏まえて新設	11. 非常時（災害、インシデント、サイバー攻撃被害）対応とBCP策定	⑧ 非常時の事象が生じた場合、安全管理の状況を適宜把握し、経営層に報告すること。							
					11. 非常時（災害、インシデント、サイバー攻撃被害）対応とBCP策定	⑩ 非常時の事象発生に伴い対応した内容について、事後検証を行い、その内容を経営層に報告し、承認を得ること。その検証結果や評価を、適宜、非常時の対応手順等に反映させること。							

1. 安全管理に関する責任・業務

[illegible]

[illegible]

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

[illegible]

[illegible]

5. 医療情報システム・サービス事業者との協働																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																											</
-------------------------	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	----

参照文書リンク集

	文書名	制定・公表	主体	最新	参照先リンク①	参照先リンク②	参照先リンク③
1	個人情報の保護に関する法律	平成15年法律第57号	法律	令和3年法	https://elaws.e-gov.go.jp/document?lawid=415AC0000000057		
2	行政機関の保有する個人情報の保護に関する法律	平成15年法律第58号	法律	令和3年法律第37号による廃止	https://elaws.e-gov.go.jp/document?lawid=415AC0000000058		
3	独立行政法人等の保有する個人情報の保護に関する法律	平成15年法律第59号	法律	令和3年法律第37号による廃止	https://elaws.e-gov.go.jp/document?lawid=415AC0000000059		
4	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	法律	令和3年法律第36号による改正	https://elaws.e-gov.go.jp/document?lawid=416AC0000000149		
5	電子署名及び認証業務に関する法律	平成12年5月	法律	令和4年法律第68号による改正	https://elaws.e-gov.go.jp/document?lawid=412AC0000000102		
6	電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律	平成14年法律第153号	法律	令和4年法律第68号による改正	https://elaws.e-gov.go.jp/document?lawid=414AC0000000153		
7	医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律	昭和35年法律第145号	法律	令和4年法律第47号による改正	https://elaws.e-gov.go.jp/document?lawid=335AC0000000145		
8	厚生労働省の所管する法令の規定に基づく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省令	平成17年3月25日発出	厚生労働大臣	令和4年厚生労働省令第75号による改正	https://elaws.e-gov.go.jp/document?lawid=417M60000100044		
9	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	令和4年9月30日初版決定	デジタル社会推進会議幹事会決定	令和4年12月28日最終改定	https://www.digital.go.jp/resources/standard_guidelines/	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/17ef852e/2022	
10	良質な医療を提供する体制の確立を図るための医療法の一部を改正する法律の一部の施行について	平成19年3月30日発出	厚生労働省	平成19年3月30日発出	https://www.mhlw.go.jp/web/t_doc?dataId=00tb3561&dataType=1&page		
11	「診療録等の保存を行う場所について」の一部改正について	平成25年3月25日発出	厚生労働省	平成25年3月25日発出	https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryuu/iryuu/johoka/index.html		
12	「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」の一部改正について	平成28年3月31日発出	厚生労働省	平成28年3月31日発出	https://www.mhlw.go.jp/file/05-Shingikai-12601000-Seisakutoukatsukan-Sanjikanshitsu_Shakaihoshoutantou/0000120128.pdf		
13	医療機器におけるサイバーセキュリティの確保について	平成27年4月28日発出	厚生労働省	平成27年4月28日発出	https://www.pmda.go.jp/files/000204891.pdf		
14	医療機関等におけるサイバーセキュリティ対策の強化について	平成30年10月29日発出	厚生労働省	平成30年10月29日発出	https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryuu/iryuu/johoka/cyber-security.html	https://www.mhlw.go.jp/content/10808000/001011697.pdf	
15	ランサムウェアによるサイバー攻撃に関する注意喚起	令和3年4月30日発出	内閣官房内閣サイバーセキュリティセンター（NISC）	令和3年4月30日発出	https://www.nisc.go.jp/pdf/policy/infra/ransomware20210430.pdf		
16	時刻認証業務の認定に関する規程	令和3年4月1日制定	総務省	令和3年4月1日制定	https://www.soumu.go.jp/main_sosiki/joho_tsusin/top/ninshou-law/timestamp.html	https://www.soumu.go.jp/main_content/000742664.pdf	
17	個人情報の保護に関する法律についてのガイドライン（通則編）	平成29年5月公表	個人情報保護委員会	令和4年9月改正	https://www.ppc.go.jp/personalinfo/legal/guidelines_administrative/		

18	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	平成29年4月14日	個人情報保護委員会 厚生労働省	令和4年3月一部改正	https://www.mhlw.go.jp/content/000909511.pdf	https://www.ppc.go.jp/personalinfo/legal/iryoukaigo_guidance/	
19	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	令和2年8月21日策定	経済産業省 総務省	令和3年8月31日改定	https://www.meti.go.jp/policy/mono_info_service/healthcare/teikyoujigiyousyagl.html		
20	政府機関等のサイバーセキュリティ対策のための統一基準群（令和3年度版）	令和3年7月7日策定	内閣官房内閣サイバーセキュリティセンター（NISC）	令和4年12月12日一部改定	https://www.nisc.go.jp/policy/group/general/kijun.html		
21	利用者の指示に基づきサービス提供事業者自身の署名鍵により暗号化等を行う電子契約サービスに関するQ&A（電子署名法2条1項に関するQ&A）	令和2年7月17日公表	総務省 法務省 経済産業省	令和2年7月17日公表	https://www.meti.go.jp/covid-19/denshishomei_qa.html	https://www.moj.go.jp/MINJI/denshishomeihou.html	
22	利用者の指示に基づきサービス提供事業者自身の署名鍵により暗号化等を行う電子契約サービスに関するQ&A（電子署名法3条に関するQ&A）	令和2年9月4日公表	総務省 法務省 経済産業省	令和2年9月4日公表	https://www.meti.go.jp/covid-19/denshishomei3_qa.html		
23	タイムビジネスに係る指針－ネットワークの安心な利用と電子データの安全な長期保存のために－	平成16年11月5日公表	総務省	平成16年11月5日公表	https://www.soumu.go.jp/main_sosiki/joho_tsusin/top/ninshou-law/timestamp.html	https://www.soumu.go.jp/main_content/000485112.pdf	
24	医療機器のサイバーセキュリティの確保に関するガイダンス	平成30年7月24日発出	厚生労働省	平成30年7月24日発出	https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryou/iryou/johoka/cyber-security.html	https://www.mhlw.go.jp/content/10808000/001011666.pdf	
25	クラウドサービス提供における情報セキュリティ対策ガイドライン（第3版）	平成26年に初版公表	総務省	令和3年9月公表	https://www.soumu.go.jp/main_news/s-news/01cyber01_02000001_0121.html	https://www.soumu.go.jp/main_content/000771516.pdf	
26	クラウドサービス提供・利用における適切な設定に関するガイドライン	令和4年10月策定	総務省	令和4年10月策定	https://www.soumu.go.jp/main_news/s-news/01cyber01_02000001_0149.html	https://www.soumu.go.jp/main_content/000843318.pdf	
27	厚生労働省標準規格	平成22年3月31日医政発0331第1号	厚生労働省	令和4年3月24日改正	https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryou/iryou/johoka/index.html	http://helics.umin.ac.jp/helicsStdList.html	
28	JIS Q 27001（情報セキュリティマネジメントシステム）	平成18年5月20日制定	経済産業大臣	平成26年3月20日最終改正	https://www.jisc.go.jp/app/jis/general/GnrJISNumberNameSearchList?toGnrJISStandardDetailList		
29	ISO14533-1：2014CMS利用電子署名(CAdES)の長期署名プロファイル	平成26年12月策定	ISO/TC154	ISO 14533-1:2022が最新（令和4年6月策定）	https://www.iso.org/standard/64756.html	https://www.iso.org/standard/81814.html	
30	ISO14533-2:2021XML署名利用電子署名(XAdES)の長期署名プロファイル	令和3年8月策定	ISO/TC154	令和3年8月策定	https://www.iso.org/standard/79129.html		
31	ISO14533-3:2017PDF長期署名プロファイル(PAdES)	平成29年9月策定	ISO/TC154	平成29年9月策定	https://www.iso.org/standard/67937.html		
32	JIS Q 15001（個人情報保護マネジメントシステム）	平成11年3月20日制定	（原案作成）一般財団法人日本情報経済社会推進協会（JIPDEC）	2017年12月20日改正	https://webdesk.jsa.or.jp/books/W11M0090/index/?bunsho_id=JIS+Q+15001%3A2017		
33	「医療情報システムの安全管理に関するガイドライン」の実装事例に関する報告書	平成19年2月公表	保健・医療・福祉情報セキュリティネットワーク基盤普及促進コンソーシアム（HEASNET）	平成19年2月公表	http://www.heasnet.jp/open/report.php?data=report_documents		
34	TLS暗号設定ガイドライン3.0.1版	平成27年5月8日初版発行	独立行政法人情報処理推進機構	令和2年7月8日改定	https://www.cryptrec.go.jp/openssl_guidelines.html		
35	『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	令和3年3月公表	一般社団法人保健医療福祉情報システム工業会（JAHIS）	令和3年3月公表	https://www.jahis.jp/standard/detail/id=779		

36	IoT セキュリティガイドライン ver1.0（IoT 推進コンソーシアム、総務省、経済産業省；平成 28 年 7 月）	平成28年7月5日公表	IoT 推進コンソーシアム 総務省 経済産業省	平成28年7月5日公表	https://www.ipa.go.jp/security/iot/	http://www.iotac.jp/wg/security/	
37	標的型攻撃メールへの対処について	平成28年4月28日公表	日本医療情報学会	平成28年4月28日公表	https://www.jami.jp/medicalFields/	https://www.jami.jp/medicalFields/Documents/targetedmailattack.pdf	
38	IPA対策のしおりシリーズ	平成24年1月30日第1版策定	情報処理推進機構（IPA）	令和2年9月4日最終更新	https://www.ipa.go.jp/security/antivirus/shiori.html		
39	デジタル画像の取り扱いに関するガイドライン 3.0 版（平成 27 年 4 月）	平成11年4月公表	日本医学放射線学会電子情報委員会	平成27年4月改定	http://www.radiology.jp/member_info/guideline/20150417.html	http://www.radiology.jp/content/files/20150417.pdf	http://www.radiology.jp/member_info/guideline/20060402.html
40	個人情報保護に役立つ監査証跡ガイド～あなたの病院の個人情報を守るために～（医療情報システム開発センター）	平成19年3月発行	一般財団法人医療情報システム開発センター（MEDIS）	平成19年3月発行	https://www.medis.or.jp/7_kikaku/hanbai/hanbai.html		

安全管理ガイドラインの改定の経緯に関する年表

- 個人情報保護法及びその関連法令等
- e-文書法及びその関連法令等
- 総務省・経済産業省ガイドライン（3省4ガイドライン→3省3ガイドライン→3省2ガイドライン）
- 外部保存通知

	年度	法改正・政府の動き等		安全管理ガイドライン策定のための会議体での検討	医療情報システムの安全管理に関するガイドライン（安全管理ガイドライン）の改定
作成以前	1988（昭和63）年	個人情報関係	e-文書法及びその関連法令等	その他	
	1994（平成6）年		1988（昭和63）年 診療録等の記載方法等について		
	1999（平成11）年		1994（平成6）年4月 エックス線写真等の光磁気ディスク等への保存について		
	2002（平成14）年		1999（平成11）4月 厚生省通知「診療録等の電子媒体による保存について」及び「法令に保存義務が規定されている診療録及び診療諸記録の電子媒体による保存に関するガイドライン」		
	2004（平成16）年	2004（平成16）年 個人情報保護法成立 2004（平成16）年12月 「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ドライン」	2002（平成14）年3月 厚生労働省通知「診療録等の保存を行う場所について」（外部保存通知）		
			2002（平成14）年5月 厚生労働省「診療録等の外部保存に関するガイドライン」 →診療録等の電子保存及び保存場所に関する要件等が明確化		
			2004（平成16）年11月 「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」（e-文書法）		
第1版	2005（平成17）年	2005（平成17）年3月 厚生労働省令「厚生労働省の所管する法令の規定に基づく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省令」（e-文書法省令）			2005（平成17）年3月 第1版公開 e-文書法・省令、個人情報保護法への対応としてガイドラインを新設 （e-文書法令の別添として） 「法令に保存義務が規定されている診療録及び診療諸記録の電子媒体による保存に関するガイドライン」及び「診療録等の外部保存に関するガイドライン」を見直し、さらに、個人情報保護に資する情報システムの運用管理に関わる指針と e-文書法への適切な対応を行うための指針を統合して作成
		2005（平成17）年4月 「個人情報の保護に関する法律」施行（個人情報保護法）			
第2版	2006（平成18）年		2005（平成17）年9月 情報セキュリティ政策会議「重要インフラの情報セキュリティ対策に係る基本的考え方」発表 →医療を「重要インフラ」として位置づけ	2006（平成18）年度 医療情報ネットワーク基盤検討会検討事項 （1）医療機関等で用いるのに適したネットワークに関するセキュリティ要件定義 （2）自然災害・サイバー攻撃によるIT障害対策等	
	2007（平成19）年		2006（平成18）年1月 高度情報通信技術戦略本部（IT戦略本部）から、「IT新改革戦略」が発表 →「安全なネットワーク基盤の確立」を掲げる		2007（平成19）年3月 第2版公開 ネットワーク基盤の安全性、災害・サイバー攻撃への対応を追加 ●ネットワークの要件を定義し、「6.10 外部と個人情報を含む医療情報を交換する場合の安全管理」を新設 ●医療における災害、サイバー攻撃対策に対する指針として「6.9災害等の非常時の対応」を新設 ●「6.2 医療機関における情報セキュリティマネジメント（ISMS）」の実践でISMSの概念を導入 ・その他関連する箇所の修正
第3版	2007（平成19）年3月	「IT新改革戦略評価専門調査会2006年度報告書」公表 →処方箋の電子化について言及		2007（平成19）年度 医療情報ネットワーク基盤検討会検討事項 （1）医療情報の取扱いに関する事項 →医療従事者とそれ以外の事業者等との責任分界 （2）処方箋の電子化に関する事項 →医療情報ネットワーク基盤検討会提言「処方せんの電子化について」（第4.2版でガイドラインに対応） （3）無線・モバイルを利用する際の技術的要件に関する事項	
	2008（平成20）年				2008（平成20）3月 第3版公開 責任分界の追加 ●医療従事者その他の関係者が医療・健康情報を取り扱う際の責任のあり方を定め「4 電子的な医療情報を扱う際の責任のあり方」を取りまとめ →「8.1.2 外部保存を委託する事業者の選定基準及び情報の取扱いに関する基準」を改定 無線・モバイルといった新技術への対応 ●無線・モバイルを利用する際の脅威や技術的要件について6章を加筆 →特にネットワークのあり方については「6.11 外部と個人情報を含む医療情報を交換する場合の安全管理」に取りまとめ →盗難や紛失といった新たなリスクについて、「6.9 情報及び情報機器の持ち出しについて」を新設
第4版					2009（平成21）年3月 第4版公開 体系的な見直し ●本ガイドラインに準じて取り扱うものとして、「3.3 取扱いに注意を要する文書等」を新設 ●「5 情報の相互運用性と標準化について」を全面改定 ●「6.1 方針の制定と公表」について、JIS Q 15001:2006をもとに説明しC項を新設 ●「6.2 医療機関における情報セキュリティマネジメントシステム（ISMS）」の実践においてC、D項を新設 ●「6.11 外部と個人情報を含む医療情報を交換する場合の安全管理」においてB、D項に従業者による外部からのアクセスに関する事項を追加 ●7章の大幅改定 「7.1 真正性の確保について」：B項簡略化、C項見直し、D項削除 「7.2 見証性の確保について」：B項簡略化、C項・D項の整理 「7.3 保存性の確保について」：C項、D項で大幅な見直し ●8章「診療録及び診療諸記録を外部の保存する際の基準」：2省ガイドラインとの整合を明確化
		2008（平成20）年1月 総務省「ASP・SaaSにおける情報セキュリティ対策ガイドライン」（「ASP・SaaSセキュリティガイドライン」） 2008（平成20）年7月 経済産業省「医療情報を委託管理する情報処理事業者における安全管理ガイドライン」（「情報処理事業者ガイドライン」） 2009（平成21）7月 総務省「ASP・SaaS事業者が医療情報を取り扱う際の安全管理に関するガイドライン」（「ASP・SaaS事業者ガイドライン」）策定 →外部保存に対する対応方法が明確化		2008（平成20）年度 医療情報ネットワーク基盤検討会検討事項 （1）医療分野における電子化された情報管理の在り方に関する事項 →体系的な見直し （2）個人が自らの医療情報を管理・活用するための方策等に関する事項	
第4.1版	2009（平成21）年			2009年11月 医療情報ネットワーク基盤検討会議 「診療録等の保存を行う場所に関する提言」	
	2010（平成22）年	2010（平成22）年2月 厚生労働省外部保存通知の一部改正（民間事業者が設置するデータセンターへの保存を解禁）		2009年11月 医療情報ネットワーク基盤検討会議 「診療録等の保存を行う場所に関する提言」	
第4.2版		2010（平成22）年6月 「規制・制度改革に係る対処方針」（「国民の声を集中受付月間（第1回）」において提出された提案等への対処方針について）閣議決定 2010（平成22）年6月 「新たな情報通信技術戦略工程表」IT戦略本部決定 2011（平成23）年8月 「情報通信技術利活用のための規制・制度改革に係る対処方針」IT戦略本部決定		2009（平成21）年度 医療情報ネットワーク基盤検討会検討事項 ・診療録等の保存を行う場所について ・「医療情報システムの安全管理に関するガイドライン」等の改正について	2010（平成22）年2月 第4.1版公開 総務省・経済産業省ガイドラインの策定と外部保存通知の改正に合わせた対応 ●「4.3 明細による責任分界点の考え方の整理」：（4）オンライン外部保存を委託する場合」を追加 ●「8.1.2 外部保存を委託する事業者の選定基準及び情報の取扱いに関する基準」 ●10章：4章、8章に合わせて修正
	2011（平成23）年				
	2012（平成24）年			2012（平成24）年4月 医療情報ネットワーク基盤検討会提言 「処方箋の電子化に向けて」 2012（平成24）年度 医療情報ネットワーク基盤検討会検討事項 ・処方箋の電子化について	
	2013（平成25）年	2013（平成25）年3月 厚生労働省外部保存通知の一部改正（調剤済み処方箋及び調剤録等の外部保存を解禁）		2013（平成25）年3月 医療情報ネットワーク基盤検討会提言 「電子処方箋の実現について」	2013（平成25）年10月 第4.2版公開 調剤済み処方箋及び調剤録等の外部保存への対応 ●3章：調剤録の外部保存に関する事項を追加、「3.3 調剤済み処方箋と調剤録の電子化・外部保存について」追加 ●9章：紙の処方箋を電子化する方法について追加
第4.3版	2015（平成27）年			2015（平成27）年度 医療情報ネットワーク基盤検討会検討事項 （1）電子処方せんの運用ガイドライン（案）について	
	2016（平成28）年	2016（平成28）3月 厚生労働省e-文書法省令の一部改正		2016（平成28）年3月 電子処方せんの運用ガイドラインの策定	2016（平成28）年3月 第4.3版公開 処方箋の電磁的記録による取扱いの運用は「電子処方せんの運用ガイドライン」を参照するものとする ●関連する3、8、9省の一部を修正

	個人情報保護法及びその関連法令等
	e-文書法及びその関連法令等
	総務省・経済産業省ガイドライン（3省4ガイドライン→3省3ガイドライン→3省2ガイドライン）
	外部保存通知

	年度	法改正・政府の動き等			安全管理ガイドライン策定のための会議体での検討	医療情報システムの安全管理に関するガイドライン（安全管理ガイドライン）の改定
第5版	2017（平成29）年	2017（平成29）年 改正個人情報保護法施行				2017（平成29）年5月 第5版公開 改正個人情報保護法等への対応 ●1章：本ガイドラインの対象に、病院、一般診療所、歯科診療所、助産所、薬局、訪問看護ステーション、介護事業者、医療情報連携ネットワーク運営事業者等における電子的な医療情報の取扱いに係る責任者が含まれることを明確化 ●3章：1章を踏まえて、介護事業者が取り扱う文書で7章及び9章の対象となる文書を列挙 ●4章「4.2.2 第三者提供における責任分界」：改正個人情報保護法で新たに規定された義務について関係資料を参照 4.2版公表以降に追加された標準規格等への対応 ●5章：厚生労働省標準規格・JAHIS標準規約を追加。日本 IHE 協会の「地域医療連携における情報連携基盤技術仕様」について記述を新設 ●6章：「6.1 方針の制定と公表」及び「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」において所要の改定 新たなセキュリティリスクへの対応 ●6章 ・6.2 章：「『製造業者による医療情報セキュリティ開示書』ガイド」に関する記述の追加 ・「6.5 技術的安全対策」：できるだけ早期に二要素認証を実装することを求め、かつパスワード要件について追記、 「（6）医療等分野における IoT 機器の利用」を新設 ・「6.6 人的安全対策」及び「6.10 災害、サイバー攻撃等の非常時の対応（改題）」：サイバー攻撃等への事前及び事後の対応や連絡先等について規定を新設 ・「6.9 情報及び情報機器の持ち出しについて」：公衆無線LAN、BYODについて追記 ・「6.11 外部と個人情報を含む医療情報を交換する場合の安全管理」：オープンなネットワークを介した SSL/TLS 接続における遵守事項や留意点を追記 その他 ●「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」：国家資格の証明が求められる文書に対する考え方や取扱いについて追記 ●「7.1 真正性の確保について」：電子カルテ等の入力における関係者の役割や責任をより明確にするとともに、代行入力を行う場合の記録確定に当たって遵守すべき事項を追記 ●「7.3 保存性の確保について」において、医療機関等が文書を保存する際の将来の互換性の確保について、規定を設けた。 ●10章他、上記に合わせた修正
		2017（平成29）年 「個人情報の保護に関する法律についてのガイドライン（通則編）」（通則ガイドライン）施行			2017（平成29）年度 医療情報ネットワーク基盤検討会検討事項 （1）「医療情報システムの安全管理に関するガイドライン」の改定について	
		2017（平成29）年4月 「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」				
		2017（平成29）年5月 平成27年改正個人情報保護法施行				
第5.1版	2018（平成30年）年	2018（平成30年）年7月 総務省「クラウドサービス提供における情報セキュリティ対策ガイドライン（第2版）」改定 （初版策定は2014年（平成26）年4月）				
		2018（平成30年）年7月 総務省「クラウドサービス事業者が医療情報を取り扱う際の安全管理に関するガイドライン」 （「クラウド事業者ガイドライン」）（総務省の2ガイドラインを統合） ASP・SaaSセキュリティガイドラインにおける医療情報に関する内容と ASP・SaaS 事業者ガイドラインの内容を1つのガイドラインに統合するとともに、ガイドラインの対象を ASP・SaaS 事業者だけでなく PaaS や IaaS 等のクラウドサービス事業者も対象とする				
	2019（平成31年／令和元年）				健康・医療・介護情報利活用検討会医療等情報利活用ワーキンググループ検討事項 ・保健医療情報を全国の医療機関等で確認できる仕組み及び標準的な医療情報システムについて ・電子処方箋について ・医療情報システムの安全管理に関するガイドライン改定素案について	
	2020（令和2）年	2020（令和2）年8月 総務省・経済産業省「医療等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」（2省ガイドライン）策定				
第5.2版	2021（令和3）年					令和3年1月 第5.1版公開 サイバー攻撃の多様化・巧妙化への対応 ●6章：以下の追記 ・「6.2.3 リスク分析」（管理されていない機器やソフトウェア、サービス等の利用等のリスク） ・「6.5 技術的安全対策」及び「6.11 外部と個人情報を含む医療情報を交換する場合の安全管理」（ネットワークの監視等の措置やネットワークの構築のあり方、外部からのデータ取り込みにおける対応措置等の必要性） ・「6.5 技術的安全対策」（二要素認証導入を促す方針をさらに進めるため、B、C 項の改定、暗号鍵の管理に関する内容も新規に規定） ・「6.10 災害、サイバー攻撃等の非常時の対応」（非常時の体制構築） 新技術への対応（スマホの普及、クラウドサービス、ネットワークサービス） ●4章：クラウドサービスの概要を示すとともに、「4.3 列示による責任分界点の考え方の整理」に追記 ●「8.1.2 外部保存を委託する事業者の選定基準及び情報の取扱いに関する基準」：行政機関等又は民間事業者が設置するデータセンターに関する選定の在り方、受託事業者の選定（Cookie 等の取扱いに関する事項、受託事業者に対する国内法の適用、求められる認証や提供すべきセキュリティ情報）について追記 関連ガイドライン等との整合 ●関連法規の改正に伴う部分の修正
	2022（令和4）年	2021（令和3）年4月 総務省告示「時刻認証業務の認定に関する規程（令和3年総務省告示第146号）」→タイムスタンプ認定制度開始			健康・医療・介護情報利活用検討会医療等情報利活用ワーキンググループ検討事項 ・データヘルス集中改革プラン等の主な論点と検討の方向性について ・データヘルス改革に関する工程表について ・医療情報ネットワークの基盤に関するワーキンググループの設置について ・医療情報システムの安全管理に関するガイドラインについて ・電子処方箋の仕組みの構築について ・医療機関等事業者による機密等情報の取扱いに関する基本的指針について	
		2022（令和4）年3月 「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」一部改正				2022（令和4）年3月 第5.2版公開 本編と別冊編に分離 ●本ガイドラインについての理解をより促す観点から、安全対策として実施すべき内容に直接関係する部分と、安全対策を行う上での背景となる考え方や判断などの部分を分けて記述 ランサムウェアに代表される攻撃への対策 ●6.2章医療情報システムに関する全体構成図（ネットワーク構成図、システム構成図等）、及びシステム責任者一覧（設置事業者等含む）を整備する旨追記 ●6.10 章：サイバー攻撃対応としてのバックアップのあり方等の対策を示す 関連する制度等の状況の反映 ●6.12章：電子署名が求められる文書の長期保存に必要なタイムスタンプについて、総務大臣の認定制度が創設されたことに伴う修正、JIS から ISO に準拠規格を変更、リモート署名や立会人型電子署名など新たな利用形態が普及しつつあることを踏まえて、電子署名に関する 6.12 章の記載を整理 ●6.3章：2省ガイドラインとの整合（外部保存を行う際の事業者の選定） その他 ●6.9章：BYOD利用時の安全な環境について追記 ●全体的な表現の修正
		2022（令和4）年4月 改正個人情報保護法施行				