令和５年〇月

「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」

に関するＱ＆Ａ　（案）

本 Q&A の参照箇所の使い方

企[1] 2 章第[2]①条

[1] 各編の名称　概…概説編　経…経営管理編　企…企画管理編　シス…システム管理編

[2] 本編【遵守事項】の「条」です。

概説編

概説編

概２章

概Ｑ－１ ① このガイドラインは、医療機関等の関係者が読むもので、医療情報システムに関係するベンダや事業者は読む必要はないのか。 ② ベンダや事業者が遵守すべきガイドラインにはどのようなものがあるのか。

Ａ 医療情報システムの管理上の一次責任は医療機関側にありますので、医療機関等の関係者は、このガイドラインの内容をよく理解し、遵守していただく必要があります。

ただし、情報システムの安全管理は運用と技術とが相まって一定のレベルを達成するものです。特に、情報化が進み、多様なシステムが導入され、利用されている医療機関等においては、システムの構築はじめ安全管理を医療機関等の関係者のみで実施することは少なく、システムに関係するベンダや事業者の協力を得て、情報システムの安全管理を実施することが多いです。そのため、医療情報システムを安全に管理・運用するのは、医療機関側の責任ですが、システムに関係するベンダや事業者にも本ガイドラインを読んでいただき、医療機関等側が負う責任や遵守すべき内容について理解を深め、より安全な情報システムの管理・運用が果たされるような協働を働きかけることは有用です。

協働するベンダや事業者には、医療情報システムの安全管理の観点ではこのガイドラインを、医療情報システムで取り扱う個人情報の保護の観点では「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」を理解していただくことが望ましいです。

なお、ベンダや事業者といった医療情報システム・サービスに関係する事業者に対しては、総務省・経済産業省が「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」を策定しています。ベンダや事業者はそのガイドラインの内容をよく理解していただく必要があります。

概２．１章

概Ｑ－２ どのような場合に、介護事業者は本ガイドラインの内容を遵守する必要があるか。

Ａ 下記のような事例等が想定されます。

介護事業者が取り扱う e-文書法の対象範囲となる文書に、医師等から提供を受けた患者の医療情報を記入し、電子保存を行う場合。

上記のほか、医師等が作成した患者の医療情報を情報システムにより取り扱う場合。

概２．２章

概Ｑ－３　他の医療機関等から提供された電子化された情報の取扱いは、このガイドラインの対象となるのか。

Ａ　このガイドラインは、医療に関わる情報を扱う全ての情報システムと、それらのシステムの導入、運用、利用、保守及び廃棄に関わる人又は組織が対象となっています。

そのため、このガイドラインの対象情報は、前文の情報システムや人又は組織の中で扱われる情報のうち、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）等が対象です。

したがって、他の医療機関から提供された電子化された情報についても、電子化された状態で利用・保存する限りはこのガイドラインの対象となります。

なお、個人情報の取扱いについては、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。）並びに「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」等を参照してください。

概２．２章

概Ｑ－４　電子保存が認められている文書とは具体的に何か。

Ａ　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 年厚生労働省令第 44 号。以下「e-文書法省令」という。）、施行通知で定められた文書です。

概２．３章

概Ｑ－５　「医療情報システム」とは具体的に何を示すのか。

Ａ　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・取得するようなコンピュータや携帯端末も範ちゅうとして想定しています。また、医療情報が通信される院内・院外ネットワークも含まれます。

概説３．２章

概Ｑ－６　オンライン資格確認や電子処方箋の導入において、どのような留意事項があるか。

Ａ　オンライン資格確認や電子処方箋の導入については、厚生労働省のホームページや医療機関等向けポータルサイトに資料が掲載されています。

［オンライン資格確認］
- 厚生労働省　オンライン資格確認の導入について（医療機関・薬局、システムベンダ向け）
  https://www.mhlw.go.jp/stf/newpage_08280.html
- オンライン資格確認・医療情報化支援基金関係医療機関等向けポータルサイト
  https://www.iryohokenjyoho-portalsite.jp/

［電子処方箋］
- 厚生労働省　電子処方箋
  https://www.mhlw.go.jp/stf/denshishohousen.html
- 電子処方箋ポータルサイト
  https://iryohokenjyoho.service-now.com/csm?id=csm_index

本ガイドラインを踏まえた留意事項としては、
- 「オンライン資格確認導入に向けた準備作業の手引き【医療機関・薬局の方々へ】」
- 「ネットワーク整備を含むオンライン資格確認導入に向けた準備作業の手引き【医療機関・薬局の方々へ】」
- 「電子処方箋導入に向けた準備作業の手引き【医療機関・薬局の方々へ】」

に掲載されている「システム事業者へ発注」「導入・運用準備」のステップにおいて、「オンライン資格確認の機器」「医療機関等が利用するシステム（レセプトコンピュータ、電子カルテシステム/薬局システム）」「オンライン請求ネットワーク」「ルーターなどのネットワーク機器」の購入・設置・設定・保守に関係するシステム事業者との間で、役割分担や責任分界を明確にし、契約や体制、ネットワーク構成図、機器設定を適切に管理することが求められます。

概４．３章

概Ｑ－７　医療情報を電子的に保存するに当たって定められた要件は何か。また、情報セキュリティの３要素（機密性・完全性・可用性）との違いはあるか。

Ａ　電子化する対象である全ての記録に対しての指針が、「６　医療情報システムの基本的な安全管理」に記載されています。さらに、保存義務のある記録の電子化には、e-文書法省令に従った内容が「７　電子保存の要求事項について」に記載されており、いわゆる電子保存の３要件（真正性、見読性、保存性）について規定されています。紙媒体の原本をスキャナで読み取り電子文書化する場合の記載は、「９　診療録等をスキャナ等により電子化して保存する場合について」に記載されています。保存義務のない書類であっても、これらの記載に準拠することが求められます。

電子保存の３要件は、「書面の保存等に関し、電子情報処理組織を使用する方法その他の情報通信の技術を利用する方法」[3]に必要とされる要件で、

- 真正性とは、「正当な権限で作成された記録に対し、虚偽入力、書換え、消去及び混同が防止されており、かつ、第三者から見て作成の責任の所在が明確であることである。なお、混同とは、患者を取り違えた記録がなされたり、記録された情報間での関連性を誤ったりすること」
- 見読性とは「電子媒体に保存された内容を、「診療」、「患者への説明」、「監査」、「訴訟」等の要求に応じて、それぞれの目的に対し支障のない応答時間やスループット、操作方法で、肉眼で見読可能な状態にできること」
- 保存性とは、「記録された情報が法令等で定められた期間にわたって真正性を保ち、見読可能にできる状態で保存されること」

と定義されています。

これは、e-文書法令第４条第４項の第１号から第３号までを具体化したものと言えます。

一方、情報セキュリティの３要素（機密性・完全性・可用性）は、情報資産の安全かつ信頼できる利用において求められる、情報セキュリティにおける要素です。これらについては、概説編「４．２　医療情報システムの安全管理に必要な要素」で詳述しています。

電子保存の３要件と、情報セキュリティの３要素が総じて満たすことは、多くの部分で重なります。例えば、文書を電子化したファイルが、完全性と可用性を満たすことにより、見読性の要件の大半を満たすと評価することができます。また、機密性を満たすことにより、真正性の要件の多くを満たしていると評価することもできます。さらには、機密性、完全性、可用性を満たすことで保存性の要件の多くを満たすことが可能であると考えられます。

[3] 「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）第 1 条

本ガイドライン第６．０版ではこのような関係を踏まえて、電子保存３要件のうち、情報セキュリティ３要素と重なる部分については、e-文書法令の対象だけではなく、医療情報を取り扱う情報システム全般に適用し、情報セキュリティの３要素から、遵守事項等を整理しました。

その上で、情報セキュリティ３要素だけでは満たせない内容については、別途遵守事項として定め、システム運用編の別添に示しています。

概Ｑ－８　SNS 等の Web サービスを利用して医療情報をやり取りする場合、考慮するべきことはあるか。

Ａ　SNS（Social Networking Service）等の Web サービスを利用して患者の医療情報を取り扱う場合、当該サービスは医療情報システムに該当し、ガイドラインの基準を満たす必要があります。

特に、SNS の場合、セキュリティが十分に確保されていないサービスもあることから、一般社団法人保健医療福祉情報安全管理適合性評価協会（HISPRO）が公表している「医療情報連携において、SNS を利用する際に気を付けるべき事項」[4]を参考に、適切な対策を講じてください。

概Ｑ－９　第５．２版では、付表で小規模病院、診療所などの対応について示されていたが、小規模の基準は病床数や職員数で決められているのか。また第６．０版では、小規模病院等の対応について、同様の対応などが示されているのか。

Ａ　「小規模」に、明確な数値基準はありません。

医療情報システムの安全対策におけるリスクを考える上で、医療機関等の規模は一つの視点となりますが、必ずしも規模だけでリスクやその対策が決まるわけではありません。例えば小規模医療機関等であっても、医療情報を取り扱うシステムを、医療機関等自らがアプリケーションを使って開発し、運用している場合には、システム開発や運用に関するリスクは必ずしも低くはなく、したがって適切な対策が求められます。

医療機関等においては、専任の情報システム運用担当がいない場合や、医療情報システムを外部のクラウドサービスにするなどで、医療機関等の直接的な負担を軽減し、安全な医療情報の取り扱いを図るため、外部の医療情報システム・サービス事業者に運用等を委ねる場合があり、小規模医療機関等において、特にみられる傾向と言えます。

第６．０版では、このように医療機関等の規模の大小ではなく、医療機関等における体制や、医療情報システムの構成に着目し、医療機関等に専任のシステム運用担当者が存在しない場合や、利用する医療情報システムがクラウドサービスだけの場合には、本ガイドラインの一部については、参照を簡略化できることとしています。

[4] http://www.hispro.or.jp/open/pdf/SNS_RiyouCheckJikou_20160126.pdf

このように小規模医療機関等における対策の負担軽減を直接示す内容は含まれていないものの、実質的には外部委託の活用等の対応が図れるようにしています。

また、診療所や薬局等の小規模医療機関等向けの特集も、補足資料として用意していますので、適宜、ご参照ください。

概Q－10　旧版のガイドラインの本編や別冊や別添等、全て読む必要があるか。

A　旧版は読む必要はありません。旧版の内容は、最新版で変更若しくは削除等されている場合があるため、最新版をお読みください。

概Q－11　このガイドラインの説明会や研修会等は実施されていないのか。

A　厚生労働省として実施しているものはありませんが、一般社団法人日本医療情報学会や一般社団法人保健医療福祉情報システム工業会等による講演会等で、解説が行われることがあります。

なお、厚生労働省では、医療機関等向けサイバーセキュリティ研修用動画、教材を提供しております[5]ので、こちらも参考にしてください。

[5] https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryou/iryou/johoka/cyber-security.html

経営管理編

経営管理編

１．安全管理に関する責任・責務

経１．１章

経Ｑ－１　電子的な医療情報を扱う責任を果たすうえで、どのようなことを理解すればいいか

Ａ　医療に関わる全ての行為は医療法等で医療機関等の管理者の責任で行うことが求められており、医療情報の取扱いも同様です。このことから、医療機関等の管理者には、収集、保管、破棄を通じて刑法（明治 40 年法律第 45 号）等に定められている守秘義務、個人情報保護に関する諸法及び指針のほか、医療情報の扱いに関わる法令、厚生労働省通知、他の指針等により定められている要求事項を満たすために適切な措置を講じることが求められます。平成29年５月に施行された平成27年度改正個人情報保護法では、個人情報の定義が明確化されるとともに、取扱いに特に配慮を要する「要配慮個人情報」や、特定の個人を識別することができないように加工した「匿名加工情報」等について、新たに規定が設けられた。このことを受けて、個人情報保護委員会が個人情報保護法についてのガイドラインを公表し、医療・介護分野においては「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」（平成 29 年 4 月 14 日、個人情報保護委員会・厚生労働省）等が定められているため、関連する規定を遵守し、適切な措置を講じてください。

故意に医療情報を漏えいさせた場合、刑法上の秘密漏示罪として犯罪行為となることがありますが、医療情報については過失による漏えいや目的外利用でも、故意の漏えいと同様に大きな問題となり得ます。そのため、医療機関等の管理者には、そのような事態が生じないよう、善良なる管理者の注意義務（善管注意義務）を果たすことが求められます。本来、医療情報の価値と重要性はその保存方法によって変化するものではないため、医療情報を電子化して保存する場合でも、医療機関等の管理者には、紙やフィルムにより院内に保存する場合と、少なくとも同等の善管注意義務を負うと考えられます。

ただし、電子化された医療情報には、次のような固有の特殊性もあります。

- 紙の媒体やフィルム等に比べて、その動きが一般の人にとって分かりにくい側面がある
- 漏えい等の事態が生じた場合に、一瞬にして大量に情報が漏えいする可能性がある
- 医療従事者が電子化された情報の取扱いの専門家とは限らないため、その安全の確保に慣れていないケースが多い

したがって、それぞれの医療機関等がその事情によりメリット・デメリットを勘案して電子化の実施範囲及びその方法を検討し、導入する医療情報システムの機能や運用方法を選択して、それに対して求められる安全基準等への対応を決める必要があります。

また、電子化された医療情報が医療機関等の施設内にとどまって存在するのではなく、ネットワークを用いた交換、共有、委託等が考えられる状況下では、その管理責任は、医療機関等だけでなく、医療情報システム・サービス事業者等にもまたがるようになります。

経１．１．２章

経Ｑ－２　医療情報の取扱いに際し、令和２年改正・令和３年改正個人情報保護法も含めて、医療機関等にはどのような責任が生じるか。

Ａ　医療情報の取扱いにおいては、まず医師法、医療法等において適正な管理が求められており、例えば医療法では診療記録を適切に備えることが求められています（第 21 条第１項第９号等）。

また医療情報は患者に関する個人情報であることから、個人情報保護法の適用対象になることは言うまでもありません。令和２年改正個人情報保護法では個人情報取扱事業者（医療機関等も含む）が医療情報のような要配慮個人情報を流出させた場合には、個人情報保護委員会に報告し、本人にも通知することが義務づけられました（法第 26 条、規則第６条の２、第６条の３）。

そのような報告義務・通知義務や、その前提である個人情報の安全管理のための措置を講じる義務（法第 23 条）等に違反しており、個人の権利利益を保護するため必要があると認められた場合には、個人情報保護委員会から当該医療機関等に対して是正勧告がなされることになります（法第 145 条第１項）。さらに是正勧告に正当な理由なく対応しない、違反行為がなされる等により、個人の重大な権利利益の侵害が切迫していると認められた場合には、個人情報保護委員会から違反行為の中止や是正措置実施の命令がなされます。（法第 145 条第２項、第３項）

令和２年改正個人情報保護法では、個人情報保護法に対する重大な違反行為に対する罰則も強化されています。例えば、上記の個人情報保護委員会から医療機関等に対する命令違反が生じた場合、命令違反をした場合の代表者や従業員が属する法人に対する罰金刑は従来の 30 万円以下から１億円以下に大きく強化されています。医療情報などの個人情報データベースを、不正に提供等を行った場合も同様の罰金刑となっています（法 179 条第１項）。

このように個人情報保護法では医療情報が漏洩した場合の報告義務等や、これに関連して必要な対応を行わずに命令違反を行った場合の医療機関等に対する罰則などが強化されていることを十分理解する必要があります。

なお、令和３年改正法では、医療機関等における責任に直接関係する内容の改正はありませんが、国公立の病院、大学等には原則として民間の病院、大学等と同等の規律を適用することとしています。

経１．２章

経Ｑ－３　このガイドラインに従いシステム構築等をしていたにも関わらず起こった情報セキュリティインシデントについて、責任のあり方をどのように考えるべきか。

Ａ　このガイドラインは、医療情報システムの安全管理及び e-文書法への適切な対応に関し、厚生労働大臣が法を執行する際の基準となるもののーつです。技術的なことだけではなく、運用を含めた安全対策を示したものであり、ガイドラインを遵守していたと認められる状況下で起こった情報セキュリティインシデントについては、一定程度の法的責任を果たしていたということが可能だと考えられます。

　しかしながら、その情報セキュリティインシデントによって患者等の第三者が不利益を被った場合に全て免責されない可能性もあります。医療情報システム運用時の責任についての考え方を「企画管理編　２．責任分界」に記していますので、適宜、ご参照ください。

経１．１．２章

経Ｑ－４　このガイドラインを遵守しなかった場合、課せられる罰則等や e-文書法以外に抵触する法令はあるのか。

Ａ　本ガイドラインは、e-文書法が医療分野において執行される際の指針となります。ガイドライン自体に罰則はありませんが、ガイドラインに違背した状態は、法令を遵守していないとみなされる可能性があります。

　本ガイドラインには、法令により要求されている事項等が列挙されています。したがって、これに違背することにより、e-文書法に求められる要件を満たすことができていないと認められる場合には、医療に関係する多くの法令等に違反したとみなされ、その罰則が適用されるおそれがあります。

経１．２．１章

経Ｑ－５　通常運用時において説明責任を果たす際、患者にどのような説明をすべきか。

Ａ　「診療情報を適正に保存するとともに、適正に利用すること」を医療情報システムの安全管理に関する方針の中に盛り込み公表する必要があります。また、詳細は、苦情・質問を受け付ける窓口を設け、「１．２．１　通常時における責任の【説明責任】」の項目の問い合わせに回答できるように、準備しておく必要があります。

経１．３章

経Ｑ－６　委託している事業者において、情報漏えい等の情報セキュリティインシデントが発生した場合、事業者に対応をさせればよいのか。

Ａ　情報漏えい等の情報セキュリティインシデントに際しては、当該情報を一次管理している医療機関等側に、説明責任及び善後策を講ずる責任が発生します。もちろん情報セキュリティインシデントを起こした事業者側も責任を免れるものではなく、両者が協力して説明及び善後策を講じる必要があります。

経１．２．１章

経Ｑ－７　委託先の事業者の対応にあたり、「個人情報保護の責任者」を選定する要件や考慮すべきこと（「個人情報の保護について一定の知識」など）はあるか。

Ａ　具体的な要件が定められているものではありませんが、医療に関わる全ての行為は、医療法等で医療機関等の管理者の責任で行うことが求められています。そのため、結果的には、個々の医療機関等の管理者が、権限を一部委譲するに適当と考える者を「個人情報保護の責任者」として選任することになると考えられます。

　電子化された「個人情報の保護についての一定の知識」についても、具体的な条件は示されていませんが、電子化された情報は、紙媒体の情報に比べ容易に大量の情報が漏洩する可能性がある特徴を持つことから、それらの特徴と扱い方について理解していることが重要です。

経１．３．２章、１．４章

経Ｑ－８　委託と第三者提供の情報管理責任上の違いは何か。

Ａ　委託とは、契約書等に基づき、業務の一部（例えば臨床検査）を外部に託すものであり、その情報の管理責任は一義的には委託元にあります。したがって、委託元は委託先の情報管理を監督しなければなりません。

　それに対し、第三者提供（例えば紹介状による治療情報の提供）とは、患者等の同意の下に情報を他の事業者等に提供することです。第三者提供では、情報提供が確実に行われた時点で提供された情報の管理責任は提供先に移動します。

　ただし、電子化された情報は提供が行われた場合でも提供元にも同じ情報が残ることが多く、残った情報の管理責任がなくなるわけではありません。

経３．３．２章

経Ｑ－９　外部監査はどのような機関に依頼すべきか。

Ａ　医療機関等が少人数の職員により運営されている等、内部監査の体制を構築できない場合には、第三者に外部監査を依頼することが考えられます。「第三者」の選定に際しては、依頼する監査の内容に応じて、医療情報システムに関する知見やシステムに求められる特性への理解を有していることが必要な場合もあれば、医療情報システムに関する知見や理解は持たず、一般的な情報セキュリティや情報システムに関する知見を有していることが重要な場合もあり、特定または専門の監査機関等に限られるものではありません。医療機関等として外部監査の目的や意義を踏まえて依頼する機関の選定を行ってください。

企画管理編

企画管理編

１．管理体系

企１章①第①条、１６章

企Ｑ－１　部門系で発生し、部門システムに保管する記録等は、ガイドラインでいう診療録、診療諸記録等としての適用を受けるのか。

例えば、エコー検査の紙画像や心電図の紙波形結果等、院内で発生した文書（ワープロやシステム出力）で、かつ手書き情報の付記のないものについては、スキャンして電子化した情報を原本として、元の紙を廃棄してよいか。

※　スキャンする際、どの患者の結果で、誰が、いつ記録したか、は登録することを前提とする。

※　紹介状や同意書等、外部からの文書や押印して初めて効力が発生する文書は、紙を原本として残すのが原則である。

上記の場合、診療録等として確定することになるのは、どの行為の時点になるのか。

スキャン時の作業責任者と情報作成管理者は、どのようになるのか。

また、情報作成管理者は、有資格者等である必要があるのか。

手書きの付記等がある場合は、どのように行えばよいのか。

Ａ　診断の根拠となる記録や診療方針に影響を与える記録等は、定められた期間保存する必要があります。紙等の物理媒体の保存義務がある記録をスキャナ等により電子化して保存する場合は、「１６．１　診療録等をスキャナ等により電子化して保存する場合の共通要件」を参照してください。

確定については、紙等の記録が作成された時点で記録は確定しており、確定された記録を電子化しているため、「１６．１　診療録等をスキャナ等により電子化して保存する場合の共通要件」に規定されるように、電子化された情報を保存義務の対象として扱うことができます。

作業責任者と情報作成管理者は運用管理規程等で定め、適正に運営されていることを監査すること等が求められますが、有資格者である必要はありません。

企１章第⑤条

企Q－２　「医療情報システムに対する情報セキュリティ方針（ポリシー）や患者の医療情報の保護に関する方針及び医療情報システムの安全管理に関する方針」とあるが、具体的にはどのようなものが想定されているのか。

A　関係する個人情報保護方針や医療情報システムの安全管理に関する方針について解説します。

【個人情報保護方針】

個人情報保護に関する方針に盛り込むべき具体的内容等について、「JIS Q 15001:2017（個人情報保護マネジメントシステム-要求事項）」では、下記のように定めています。

A.3.2.1　内部向け個人情報保護方針

トップマネジメントは，5.2.1 e）に規定する内部向け個人情報保護方針を文書化した情報には次の事項を含めなければならない。

a）事業の内容及び規模を考慮した適切な個人情報の取得，利用及び提供に関すること［特定された利用目的の達成に必要な範囲を超えた個人情報の取扱い（以下，“目的外利用”という。）を行わないこと及びそのための措置を講じることを含む。］。

b）個人情報の取扱いに関する法令，国が定める指針その他の規範を遵守すること。

c）個人情報の漏えい，滅失又は毀損の防止及び是正に関すること。

d）苦情及び相談への対応に関すること。

e）個人情報保護マネジメントシステムの継続的改善に関すること。

f）トップマネジメントの氏名

トップマネジメントは，内部向け個人情報保護方針を文書化した情報を，組織内に伝達し，必要に応じて，利害関係者が入手可能にするための措置を講じなければならない。

A.3.2.2　外部向け個人情報保護方針

トップマネジメントは，外部向け個人情報保護方針を文書化した情報には，A.3.2.1 に規定する内部向け個人情報保護方針の事項に加えて，次の事項も明記しなければならない。

a）制定年月日及び最終改正年月日

b）外部向け個人情報保護方針の内容についての問合せ先

トップマネジメントは，外部向け個人情報保護方針を文書化した情報について，一般の人が知り得るようにするための一般の人が入手可能な措置を講じなければならない。

【情報システムの安全管理に関する方針】

情報システムの安全管理に関する方針に盛り込むべき具体的内容等について、「JIS Q 27001:2014（情報セキュリティマネジメントシステム-要求事項）」では、下記のように定めています。

5.2 方針

トップマネジメントは、次の事項を満たす情報セキュリティ方針を確立しなければならない。

a) 組織の目的に対して適切である。

b) 情報セキュリティ目的（6.2 参照）を含むか、又は情報セキュリティ目的の設定のための枠組みを示す。

c) 情報セキュリティに関連する適用される要求事項を満たすことへのコミットメントを含む。

d) ISMS の継続的改善へのコミットメントを含む。

情報セキュリティ方針は、次に示す事項を満たさなければならない。

e) 文書化した情報として利用可能である。

f) 組織内に伝達する。

g) 必要に応じて利害関係者が入手可能である。

企１章第⑥条

企Q－３　医療情報システム導入に際して規程等を作成したいが、どのようなものが望ましいのか。

Ａ　個人情報保護方針については、「４．２　規程の整備（運用管理規程ほか）」において個人情報保護対策の制定について説明があります。また、「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」では、「Ⅰ　本ガイダンスの趣旨、目的、基本的考え方」「６．医療・介護関係事業者が行う措置の透明性の確保と対外的明確化」に要求事項が記載されているため、参照してください。

運用管理規程については、「４．２　規程の整備（運用管理規程ほか）」において、運用管理規程についての説明があります。

企１章第⑥条

企Ｑ－４　医療機関等がこのガイドラインに基づき、診療録等の電子保存に係る運用管理規程を作成し、その規定に沿って運用している場合、医療機関等の特性に応じた対象となる項目が本ガイドラインを満足していない項目があった場合、問題となるのか。

Ａ　たとえ手段が異なっていても、ガイドラインの趣旨を踏まえて、同様の効果を発揮するように実施することが求められます。「医療機関等の特性に応じた対象となる項目」が本ガイドラインを満足していない状態で何らかの問題が発生した場合は、医療機関等の特性に応じた対象となる項目本ガイドラインに沿った対応を行っていないことについて、理由や代替的にとっている措置に関する説明が求められます。

２．責任分界

企２章第①条

企Ｑ－５　委託したクラウド型の電子カルテサービス業者から自院の患者に関するデータが漏えいした場合、自院にはどのような責任が問われるのか。

Ａ　本ガイドラインの「２．２．２　委託における責任分界（複数事業者が関与する場合を含む）」の記述が適用されます。

管理責任は委託を行った医療機関等の責任者にあり、万一事故が起きた際には、受託する医療情報システム・サービス事業者と連携しながら本ガイドライン「経営管理編　１．２．２　非常時における責任」項の「説明責任」と「善後策を講ずる責任」を果たす必要があります。

企２章第⑥条

企Ｑ－６　第三者提供における責任分界をどのように考えればよいか。

Ａ　第三者提供とは、第三者が何らかの目的で医療情報を利用するために行われるもので、医療機関等の管理者にとっては、原則として、提供先との責任分界に基づく範囲で責任を有しています。適切な第三者提供がなされる限り、提供された後の情報保護責任は、提供した医療機関等の管理者ではなく、提供を受けた第三者が負うことになります。

ただし、例外的に、提供先で適切に扱われないことを知りながら情報提供をしたような場合は、提供元の医療機関等の責任が追及される可能性があります。

一方、電子化された情報の特性に着目すると、医療情報が第三者提供されても、医療機関等の側で当該情報を削除しない限り、当該医療情報を引き続き保存し続けることになります。したがって、その情報について情報保護責任がなお残ることはいうまでもありません。

医療情報が電子化され、ネットワーク等を通じて情報が提供される場合、第三者提供の際にも、医療機関等から提供を受ける第三者に直接情報が提供されるのではなく、医療情報システム・サービス事業者が介在することがあります。この場合、いつの時点で、第三者提供が成立するのか、すなわち医療情報システム・サービス事業者との責任分界というべき概念が発生します。

一旦、適切・適法に提供された医療情報については、提供元の医療機関等に送付先での情報保護責任がないことは先に述べたとおりですが、第三者提供の主体は提供元の医療機関等であることから、患者等に対する関係では、少なくとも情報が提供先の第三者に到達するまで、原則として、提供元の医療機関等に責任があると考えることができます。その上で、医療機関等と医療情報システム・サービス事業者との間の内部的な意味での「善後策を講ずる責任」をいかに分担するかは、医療情報システム・サービス事業者と医療機関等の間で、あらかじめ協議して明確にしておくことが望まれます。医療情報システム・サービス事業者の選任・監督義務を果たしており、特に責任が明記されていない場合に、医療情報システム・サービス事業者の過失で何らかの不都合な事態が生じた場合は、医療情報システム・サービス事業者が全ての責任を負うのが原則です。

企２章第⑥条

企Ｑ－７　第三者提供は、どの時点で成立するか。

Ａ　第三者提供では、原則本人の同意の下に情報が第三者に提供され、説明責任を含む管理責任が第三者に生じます。

第三者が明確に自己の管理範囲に情報が存在することを確認した時点が、第三者提供の成立した時点になります。したがって、何らかの方法で受領確認を行う必要があり、受領確認がなされた時点と考えることができます。

オンラインで情報を送付する場合も同様であり、例えば相手のデータベースに格納されたことを電子的に確認する手続きを明確にした上で、その確認をもって第三者提供が成立することを、契約等で合意することが必要です。送り手は送付したと考えているものの、受け手が受領したと認識していない等、責任の空白ができないようにする必要があります。

企２章第⑥条

企Ｑ－８　企画管理編２．２．３では第三者提供で責任分界を定める例が示されている。地域医療連携において、医療機関間での第三者提供の責任分界を定める際、どのような留意事項があるか。

Ａ　医療機関間での第三者提供の責任分界を定める場合として、以下の場面について解説します。

【「医療情報システム・サービス事業者の提供するネットワーク」を通じて医療情報の提供元医療機関等と提供先医療機関等で医療情報を交換する場合の責任分界】

ここでいう「医療情報システム・サービス事業者の提供するネットワーク」とは、医療情報システム・サービス事業者の責任でネットワーク経路上のセキュリティを担保する場合をいいます。

提供元医療機関等と提供先医療機関等は、ネットワーク経路における責任分界点を定め、不通時や事故発生時の対処を含め、契約等で合意してください。

その上で、自らの責任範囲において、医療情報システム・サービス事業者との管理責任の分担について責任分界点を定め、医療情報システム・サービス事業者の管理責任の範囲及びサービスに何らかの障害が起こった際の対処主体を明らかにしてください。

ただし、通常運用における責任及び事後責任は、委託の場合、原則として提供元医療機関等にあり、第三者提供の場合、適切に情報が提供される限り原則として提供先医療機関等にある。医療情報システム・サービス事業者に過失がない場合、医療情報システム・サービス事業者に生じるのは、あくまで管理責任の一部に留まることに留意する必要があります。

【提供元医療機関等と提供先医療機関等が独自に接続する場合の責任分界】

ここでいう「独自に接続」とは、接続しようとする医療機関等同士がルータ等の接続機器を自ら設定して１対１や１対Ｎで相互に接続する場合や電話回線等の公衆網を使う場合を言います。

そのうち、あらかじめ提供先又は提供先となる可能性がある医療機関等を特定できる場合は、委託又は第三者提供の要件に従って両医療機関等が責務を果たすこととなります。

このような場合、医療情報システム・サービス事業者には管理責任は発生せず、通信の品質確保の責任は発生するとしても、医療情報システム・サービス事業者が提示する約款に示されるような一般的な責任に限られます。

一方、提供先又は提供先となる可能性がある医療機関等が特定できない場合は、法令で定められている場合等の例外を除いて、原則として医療情報を提供できません。

【共同利用により他の医療機関等が収集した医療情報を利用する場合の責任分界】

地域医療連携で医療情報を交換する際、個人情報保護法上の共同利用により他の医療機関等が収集した情報を利用できます。この場合、医療機関等の間での責任分界などを規約や契約などで明確にすることが必要です。

企２章第⑥条

企Ｑ－９　地域連携のための医療情報システムとして、医療情報の所在だけを管理するレジストリと、各医療機関等が共有のために確保するリポジトリを設置する形態をとっている。利用者は、レジストリにアクセスして所在を知り、リポジトリにアクセスして実際の情報を利用する方式をとることができる（IHE XDS 統合プロファイル※）。この場合、各医療機関等は互いに保管された医療情報を共有する形となるので、共同利用という形と考えてよいか。

※　https://www.ihe.net/

また、レジストリは民間事業者等のデータセンターを利用することが適当と考えられるが、各医療機関等はデータセンターに所在情報の管理を委託してもよいか。

Ａ　診療情報を「共同利用」するためには、個人データを特定の者との間で共同して利用することを明らかにし、利用する個人データ項目、利用者の範囲、利用目的、個人データの管理責任の所在等を、あらかじめ本人に通知等している必要があります（詳細は「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」を参照してください。）。本ケースの場合は、これらの要件が不明確ですので、共同利用の要件を満たしていない可能性があります。共同利用の要件を満たしてない場合、他の施設での診療情報の利用は第三者提供に当たります。また、レジストリについて医療機関等以外の外部の事業者のデータセンターを利用する際には、医療情報を外部保存する場合と同等の要件を満足する必要があります。

企２章第⑥条

企Ｑ－１０　医療情報の共同利用において、どのような留意事項があるか。

Ａ　共同利用は、個人データの第三者提供の例外として個人情報保護法上認められている個人データの利用形態です（個人情報保護法第 27 条第 5 項第 3 号）。これは、形式的には個人データを直接の提供先とは別の組織が利用するものの、本人からみて、直接個人データを提供した相手先と一体的な利用であると合理的に考えられるため、共同利用する者は第三者には含まれないという趣旨に基づくものです。例えば地域医療連携や共同研究などの場合に、このような利用が認められる場合があります。共同利用は無限定になされると、本人（患者等）の利益を損なうことから、共同利用者の範囲や利用目的などが、「本人が通常予期し得ると客観的に認められる範囲内である必要」があります（「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）」3-6-3（個人情報保護委員会））。共同利用の考え方については、上記ガイドラインを参照ください）。

なお、共同利用については、令和２年改正個人情報保護法により、本人への通知等の義務が強化され、共同利用の事実、共同利用の対象となるデータ項目、利用者の範囲、利用目的、管理責任者の指名等の通知等のほか、管理責任者の住所、法人代表者の氏名も併せて本人への通知等の対象となりました。

企２章第⑥条

企Ｑ－１１　医療情報連携ネットワークにおける情報連携に際して、共同利用型の場合、どのような留意事項があるか。

Ａ　医療情報連携ネットワークにおける情報連携において、個人情報保護法が求める要件を具備した場合には、共同利用として利用することが可能です。ガイダンスでは、「病院と訪問看護ステーションが共同で医療サービスを提供している場合など、あらかじめ個人データを特定の者との間で共同して利用することが予定されている場合、㈠共同して利用される個人データの項目、㈡共同利用者の範囲（個別列挙されているか、本人から見てその範囲が明確となるように特定されている必要がある）、㈢利用する者の利用目的、㈣当該個人データの管理について責任を有する者の氏名又は名称及び住所並びに法人にあっては、その代表者の氏名をあらかじめ本人に通知し、又は本人が容易に知り得る状態においておくとともに、共同して利用することを明らかにしている場合には」、共同利用として利用できるものとしています。

なお、上記、㈠、㈡ については変更することができず、㈢、㈣については、本人が想定することが困難でない範囲内で変更することができ、変更する場合は、本人に通知又は本人の容易に知り得る状態におかなければならない、とされます。

企２章第⑥条

企Ｑ－１２　地域医療連携で暗号化を用いて第三者提供等を行う際、これに係る医療機関等と医療情報システム・サービス事業者における責任分界において、どのような留意事項があるか。

Ａ　【医療情報が提供元／提供先で暗号化／復号される場合の責任分界】

提供元医療機関等の医療情報システムにおいて、送信前に医療情報が暗号化され、提供先医療機関等の医療情報システムにおいて医療情報が復号される場合、医療情報システム・サービス事業者の責任は限定的になります。

しかし、この場合でも、医療情報システム・サービス事業者の管理責任は存在するため、ネットワーク上の情報の改ざんや侵入、妨害の脅威に対する医療情報システム・サービス事業者の管理責任の範囲について契約で明らかにしておく必要があります。

【医療情報が医療情報システム・サービス事業者の管理範囲で暗号化される場合の責任分界】

医療情報システム・サービス事業者の中には、例えば暗号化された安全なネットワーク回線の提供を主たるサービスとしている事業者も存在します。

そのようなネットワーク回線を使う場合、事業者が提供するネットワーク回線上における情報保護責任やサービスの可用性等の品質確保責任は事業者に発生します。したがって、それらの責任について契約で明らかにしておきます。

ただし、医療情報システム・サービス事業者が提供するネットワーク回線に到達するまでの情報保護責任は医療機関等に存在するため、医療機関間での責任分界に沿った考え方の整理が必要です。

企２章第⑥条

企Ｑ－１３　医療機関等の施設外から医療情報システムにアクセスする場合に、接続する者と医療機関等との間での責任分界において、どのような留意事項があるか。

Ａ　外部から医療情報システムにアクセスする場合に、接続者と医療機関等の責任分界を定める場合として、以下の場面について解説します。

【施設外から自らの機関の医療情報システムにアクセスし業務を行う、いわゆるテレワークする場合の責任分界】

昨今、医療機関等においても、医療機関等の施設外から自らの機関の医療情報システムにアクセスし業務を行う、いわゆるテレワークが一般的になってきました。

テレワークは、責任分界の観点では自組織に閉じていますが、医療情報システム・サービス事業者が管理するネットワークを利用することになります。また、通信回線として、公衆回線や施設内のＷｉ-Fi 等の多様なものが利用されることとなるため、個人情報保護について広範な対応が求められることになります。

特に、医療機関等の企画管理者やシステム運用担当者でない医療機関等の職員についても管理責任が問われることに注意を払う必要があります。

【第三者が保守を目的としてアクセスする、いわゆるリモートメンテナンス】

医療機関等の施設外から医療情報システムにアクセスする場合として、リモートログインを用いた医療情報システム・サービス事業者による遠隔保守（リモートメンテナンス）が考えられます。この場合、適切な情報管理やアクセス制御がなされていないと、医療情報の不正な読み取りや改ざんが行われるリスクがあります。他方、リモートメンテナンスを全面的に禁止してしまうと、遠隔保守が不可能となり、保守に要するコストが増大します。

したがって、保守の利便性と情報保護との兼ね合いを見極めつつ、リモートメンテナンスを認めるかどうか整理する必要があります。

また、リモートメンテナンスの場合でも、当然、医療機関等に「通常運用における責任」、「事後責任」が存在するため、医療情報システム・サービス事業者の報告を定期的に受け、必要な監督を行い、管理責任を果たす必要があります。

企２章第⑥条

企Ｑ－１４　地域医療連携における第三者提供等で、外部保存を受託する事業者が介在する場合、これに係る医療機関等と医療情報システム・サービス事業者との間の責任分界において、どのような留意事項があるか。

Ａ　地域医療連携で第三者提供等を行う際に、外部保存を受託する事業者が介在する場合、情報の保存を、外部保存を受託する事業者に委託することになるため、通常運用における責任、事後責任は医療機関等にあります。

これを他の医療機関等と共用しようとする場合は、双方の医療機関等において管理責任の分担を明確にし、共用に対する患者の同意も得ておく必要があります。併せて、地域医療連携における規約等において、提供側及び利用側の責任なども明らかにすることが求められます。

また、外部保存を受託する事業者とは、サービスに何らかの障害が起こった際の対処について契約で明らかにしておくことが求められます。

企２章第⑥条

企Q－15　レセプトのオンライン請求のように、第三者提供が法令に定められている場合、医療機関等と医療情報システム・サービス事業者との間の責任分界において、どのような留意事項があるか。

Ａ　法令で定められている場合等の特別な事情により、医療情報システム・サービス事業者に暗号化されていない医療情報が送信される場合は、医療情報システム・サービス事業者及びネットワーク事業者等において盗聴の脅威に対する対策を施す必要があります。

そのため、ネットワークの管理責任を負っている医療機関等は、医療情報システム・サービス事業者と医療情報の管理責任についての明確化を行わなくてはなりません。

また、医療情報システム・サービス事業者に対して管理責任の一部又は全部を委託する場合は、それぞれの事業者と個人情報に関する委託契約を適切に締結し、監督しなければなりません。

企２章第⑤条

企Q－16　外部保存を委託する際に、医療機関等と医療情報システム・サービス事業者との間の責任分界において、どのような留意事項があるか。

Ａ　本ガイドラインの「7．安全管理のための人的管理（職員管理、事業者管理、教育・訓練、事業者選定・契約）」を十分理解して委託先の選定と適切な契約を結ぶ必要があります。患者等に対する責任の主体は委託を行う医療機関等であるため、医療機関等が説明責任を果たすための資料や説明の提供を受託する事業者との契約で定め、受託する事業者における情報の取扱いを医療機関等としても理解する努力が必要です。さらに、例えば電子カルテを提供する医療情報システム・サービス事業者と、そのデータの外部保存のための資源を提供する事業者は異なることがあります。この場合、例えば障害が起こった際の対処の責任範囲について両事業者間で明確に定めた上で、医療機関等が理解しておく必要があります。

下図は、医療機関等が複数の事業者と外部保存に関する契約を行う例ですが、障害等が発生した非常時の場合に、最初に原因調査の範囲を決める責任を負う主体や、原因調査に必要な調査協力義務などについての役割、範囲等をそれぞれの事業者と取り決めておくことが求められます。複数事業者の提供サービス内容や契約内容を合わせて、本ガイドラインの要求に漏れなく適合していることの確認が必要です。

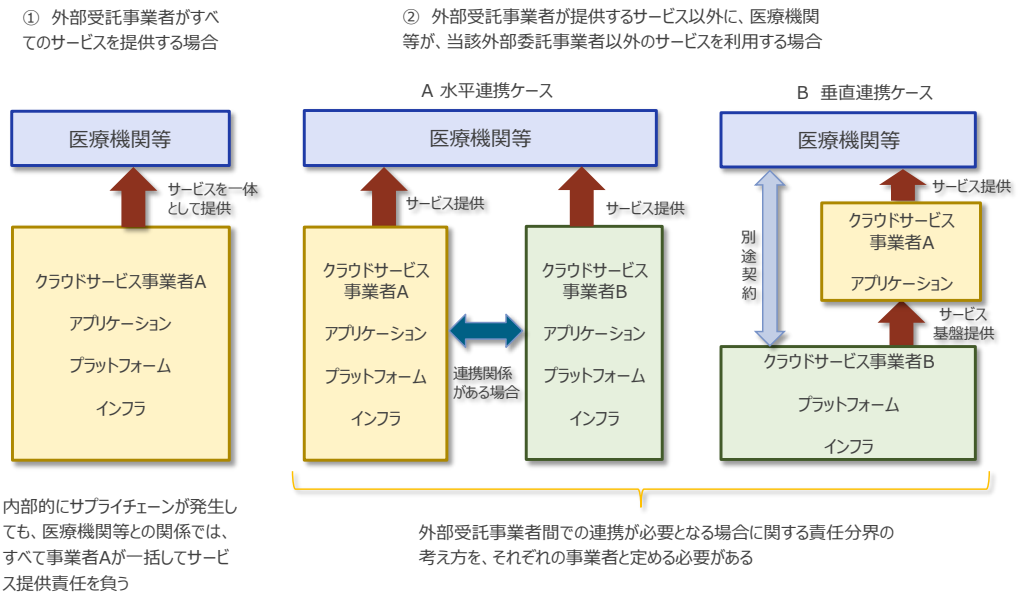

図　外部保存に関する委託例

企２章第①条

企Ｑ－17　医療機関等の業務の一部を委託することに伴い情報が外部に保存される際に、医療機関等と医療情報システム・サービス事業者との間の責任分界において、どのような留意事項があるか。

Ａ　遠隔画像診断、臨床検査等、診療等を目的とした業務の委託に伴い一時的にせよ情報を受託する事業者が保管する場合、医療機関等においては、受託する事業者の選定に関する責任やセキュリティ等の改善指示を含めた管理責任があるため、受託する事業者を適切に管理監督する必要があります。受託する事業者においても保存した情報の漏えい防止、改ざん防止等の対策を講じることは当然ですが、感染症情報や遺伝子情報等の機微な情報の取扱い方法や保存期間等については、双方協議して整理しておく必要があります。

　なお、治験のように、上記のようないわゆる業務委託ではなくとも、医療情報が外部の事業者に提供される場合は、これに準じてあらかじめ外部の事業者との間で双方の責任及び情報の取扱いについて取り決めることが必要です。

３．安全管理のための体制と責任・権限

企３章第⑨条、７章第⑦条

企Ｑ－18　安全管理のための人的管理（職員管理、事業者管理、教育・訓練、事業者選定・契約）として「原則、患者が受診している医療機関等と患者との間での同意に基づいて実施すること。」とあるが、どのように患者へ説明を行うべきか。

Ａ　外部保存実施に関する患者への説明 診療録等の外部保存を委託する医療機関等は、あらかじめ患者に対して、必要に応じて 患者の個人情報が特定の受託機関に送られ、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ります。

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してください。

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ません。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ります。

患者本人に説明し理解を得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、理解を得る必要があります。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ます。

６．リスクマネジメント（リスク管理）

企６章第⑤条

企Q－19　リスク分析で想定する脅威について、どのようなものがあるか。

Ａ　医療情報システムにおいては、システムに格納されている電子データの保護だけでなく、覗き見等の脅威にさらされるおそれのある、個人情報の入出力の際の保護方策についても考える必要があるなど、様々な脅威が想定されます。以下に様々な状況で想定される脅威を列挙します。なお「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」表 5-1 及びその別紙２（対策項目で対応できるリスクシナリオ例）も参考になります。

① 医療情報システムに格納されている電子データ
- （a）権限のない者による不正アクセス、改ざん、毀損、滅失、漏えい
- （b）権限のある者による不当な目的でのアクセス、改ざん、毀損、滅失、漏えい
- （c）コンピュータウイルス、マルウェア、ワーム等様々な形態・呼称を持つ不正ソフトウェア（以下「不正ソフトウェア」という。）や標的型メール等を用いたサイバー攻撃等による不正アクセス、改ざん、毀損、滅失、漏えい

② 入力の際に用いたメモ・原稿・検査データ等
- （a）メモ・原稿・検査データ等の覗き見
- （b）メモ・原稿・検査データ等の持ち出し
- （c）メモ・原稿・検査データ等のコピー
- （d）メモ・原稿・検査データの不適切な廃棄

③ 個人情報等のデータを格納したノートパソコン等の情報端末
- （a）情報端末の持ち出し
- （b）ネットワーク接続による不正ソフトウェアによるアクセス、改ざん、毀損、滅失、漏えい
- （c）情報端末に格納されたデータの漏えい
- （d）情報端末の盗難、紛失
- （e）情報端末の不適切な破棄

④ データを格納した可搬媒体等
- （a）可搬媒体の持ち出し
- （b）可搬媒体のコピー
- （c）可搬媒体の不適切な廃棄
- （d）可搬媒体の盗難、紛失
- （e）可搬媒体接続による不正ソフトウェア感染

⑤　参照表示した端末画面等
（a）端末画面の覗き見

⑥　データを印刷した紙やフィルム等
（a）紙やフィルム等の覗き見
（b）紙やフィルム等の持ち出し
（c）紙やフィルム等のコピー
（d）紙やフィルム等の不適切な廃棄

⑦　医療情報システム
（a）サイバー攻撃による IT 障害
- 不正侵入、不正操作
- 改ざん、毀損
- 不正ソフトウェアによる攻撃
- サービス不能（DoS：Denial of Service）攻撃 等

（b）非意図的要因による IT 障害等
- システムの仕様やソフトウェア上の欠陥（バグ）
- 操作ミス
- 故障外部サービスの利用に伴う、システムポリシー等の意図しない変更等

（c）災害による IT 障害
- 地震、水害、落雷、火災等の災害による電力供給の途絶
- 地震、水害、落雷、火災等の災害による通信の途絶
- 地震、水害、落雷、火災等の災害によるコンピュータ施設の損壊等
- 地震、水害、落雷、火災等の災害による重要インフラ事業者等における IT の機能不全

（d）許可されていない医療情報システムの利用
- 許可されていない機器、ソフトウェア、サービスの業務利用
- 管理されている機器、ソフトウェア、サービスの目的外利用

医療機関等には、受託する事業者の選定に関する責任やセキュリティ等の改善指示を含めた管理責任があるため、受託する事業者を適切に管理監督する必要があります。受託する事業者においても保存した情報の漏えい防止、改ざん防止等の対策を講じることは当然ですが、感染症情報や遺伝子情報等の機微な情報の取扱い方法や保存期間等については、双方協議して整理しておく必要があります。

企６章第⑨条

企Q－20	「 ISMS（Information Security Management System：情報セキュリティマネジメントシステム）を構築し、管理することが重要である」とあるが、医療情報の場合にはどのような考え方に基づいて行う必要があるか。

A　PDCA（Plan-Do-Check-Act）のステップをより身近にイメージできるようにするために、医療行為における安全管理のステップがどのように行われているかについて、一般財団法人日本情報経済社会推進協会（JIPDEC））の「医療機関向け ISMS ユーザーズガイド」では次のような例が記載されています。

【医療の安全管理の流れ】

事故やミスの発見と報告（Do）
「ヒヤリ、ハット事例」や「インシデントレポート」による事故やミスの発見と報告

↓

原因の分析（Check）
・「プロセスアプローチ」によって医療行為をプロセスと捉え、事故やミスの起きた業務全体を一つ一つの単体プロセス（動作）に分解し、フロー図として目に見える形にする。
（例えば注射を例にプロセスに分解すれば、①医師が処方箋を出し、②処方箋が薬剤部に送られ、③薬剤部から処方が病棟に届けられ、④病棟では看護師が正しく準備し、⑤注射を実施する、となる）
・作成したフロー図を分析し、どのプロセスに原因があったのかを調べる。

↓

予防／是正策（Act）
・再発防止のための手段を検討と実施（手順の変更、エラーチェックの仕組み導入、職員への教育の徹底等）

上記を見ると、主に D→C→A が中心になっています。これは医療等分野においては診察、診断、治療、看護等の手順が過去からの蓄積によって既に確立されているため、あとは事故やミスを発見したときにその手順を分析していくことで、どこを改善すればよいかがおのずと見え、それを実行することで安全が高まる仕組みができ上がっているためといえます。

反面、情報セキュリティでは IT 技術の目覚しい発展により、過去の経験の蓄積だけでは想定できない新たなセキュリティ上の問題点や弱点が常に存在する可能性があります。そのため情報セキュリティ独自の管理方法が必要であり、ISMS はそのために考え出されたものです。ISMS は医療の安全管理と同様 PDCA サイクルで構築し、維持していくことになります。

逆に言えば、医療関係者にとって ISMS 構築は P のステップを適切に実践し、ISMS の骨格となる文書体系や手順等を確立すれば、あとは自然に ISMS が構築されていく土壌があるといえます。

企６章第⑦条

企Q－21　医療情報システムで扱う情報の重要度の分類、確認方法、リスク分析結果はどのようにまとめるべきか。

A　最低限のガイドライン上記 1 から 7 の結果を系統的に文書化して管理してください。

７．安全管理のための人的管理（職員管理、事業者管理、教育・訓練、事業者選定・契約）

企７章第⑤条

企Ｑ－22　電子化された診療情報を外部保存できるか。できる場合、求められる要件は何か。

Ａ　電子媒体による外部保存を、ネットワークを通じて行う場合は「」に、可搬媒体を用いて行う場合は「８．２．２　記録媒体・機器情報機器等による持ち出し」に、それぞれ要件が記載されているため、そちらを参照してください。

企７章第⑤条

企Ｑ－23　クラウド型の電子カルテサービスを行う業者に認定制度のようなものはあるのか。もしなければ、業者を選定する際に３省のガイドライン※に準拠していることは、どうやって確認すればよいのか。

Ａ　認定制度は現在のところ存在しません。なお、厚生労働省のガイドラインは、サービス提供業者ではなく、サービスを委託する医療機関等が遵守すべきものです。

サービス業者の選定に当たっては、「「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」に準拠している旨」をサービス業者に確認させるとともに、契約を結ぶ際に、その旨を条項に盛り込んでおくとよいでしょう。

また、サービスを委託する医療機関は、当該サービスを利用した運用形態が、厚生労働省のガイドラインに準拠していることを、自ら確認してください。

※ ３省のガイドラインとは以下のガイドラインを指します。

- 厚生労働省「医療情報システムの安全管理に関するガイドライン」
- 総務省、経済産業省「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」

企７章第⑤条

企Ｑ－24　医療情報の外部保存を行う際、どのような留意事項があるか。

Ａ　現在の技術を十分活用し、かつ注意深く運用すれば、ネットワークを通じて、診療録等を医療機関等の外部に保存することが可能です。診療録等の外部保存を受託する事業者が、真正性を確保し、安全管理を適切に行うことにより、医療機関等の経費節減やセキュリティ上の運用が容易になる可能性があります。

ネットワークを通じて外部保存を行う方法は利点が多いが、情報の漏えいや診療に差し支えるような事故に繋がるおそれがあるため、セキュリティや通信技術及びその運用方法に十分な注意が必要です。仮にこのような事故が発生し、社会的な不信を招いた場合は、結果的に医療の情報化を後退させ、ひいては国民の利益に反することになりかねないため、慎重かつ着実に進めるべきです。

ネットワークを通じて医療機関等以外の場所に診療録等を保存することができれば、システム堅牢性の高い安全な情報の保存場所の確保によるセキュリティ対策の向上や災害時の危機管理の推進、保存コストの削減等により医療機関等において診療録等の電子保存が推進されることが期待できます。しかし、外部保存には保存機関の不適切な情報の取扱いにより患者等の情報が瞬時に大量に漏えいする危険性も存在し、その場合、漏えいした場所や責任者の特定が困難になる可能性があります。そのため、常にリスク分析を行いつつ万全の対策を講じなければならず、医療機関等の責任が相対的に大きくなります。

さらには、情報の保存を受託する事業者又は職員による、利益を目的とした不当利用の危惧があるのも事実です。その一方で金融情報、信用情報、通信情報は実態として保存・管理を当該事業者以外の外部事業者に委託しており、合理的に運用されています。金融・信用・通信に関わる情報と医療に関わる情報を一概に同様に扱うことはできないが、一般に実績あるデータセンター等の情報の保存・管理を受託する事業者は慎重で十分な安全対策を講じており、医療機関等が自ら管理することに比べても厳重に管理されていることが多いです。

本来、医療に関連した個人情報の漏えいや不当な利用等により、個人の権利利益が侵害された場合には、被害者の苦痛や権利回復が困難であることが多く、医療機関等や関係各者に対し、法律や各種ガイドライン等により格別の安全管理措置を講じることが求められています。したがって、診療録等のネットワークを通じた医療機関等以外の場所での外部保存については、通常求められる安全管理上の体制と同等以上の体制を確保した上で、患者に対する保健医療サービス等の提供に当該情報を利活用するための責任を果たせることが原則です。

企７章第⑤条

企Ｑ－25　医療機関等や委託事業者に外部保存を委託する場合、保存する情報の取り扱いに関して、どのような留意事項があるか。

Ａ　外部保存を委託する先を医療機関等と委託事業者それぞれに分けて、留意していただきたいことをまとめます。

【医療機関等に外部保存する場合】

情報を保存している機関に患者がアクセスし、自らの記録を閲覧するような仕組みを提供する場合は、情報の保存を受託した病院、診療所、医療法人等は適切なアクセス権限を規定し、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）が起こらないように配慮してください。

また、それら情報の提供は、原則、患者が受診している医療機関等と患者間の同意で実施されるものであり、情報の保存を受託した病院、診療所、医療法人等が患者から何らの同意も得ずに実施してはなりません。

病院、診療所等であっても、保存を受託した診療録等について分析等を行おうとする場合は、委託した病院、診療所及び患者の同意を得た上で、不当な利益を目的としない場合に限ります。

また、実施に当たっては院内に検証のための組織等を作り客観的な評価を行う必要があります。

匿名化された情報を取り扱う場合においても、地域や委託した医療機関等の規模によっては容易に個人が特定される可能性もあることから、匿名化の妥当性の検証を検証組織で検討したり、取扱いをしている事実を患者等に掲示等を使って知らせる等、個人情報の保護に配慮する必要があります。

【事業者に外部保存する場合】

いかなる形態であっても、保存された情報の外部保存を受託する事業者が独自に保存主体の医療機関等以外に提供してください。匿名化された情報であっても同様です。なお医療機関等が管理する端末等を用いて、医療機関等又は患者が患者情報に関するサービスを利用する場合に、受託する事業者において Cookie を取得することがあります。Cookie は直ちに個人を特定するものではないため、患者情報には当たらないとされうるものの、第三者提供することにより、患者等が特定されるリスクがあるため、受託する事業者において第三者に提供することは許されません。

外部保存を受託する事業者を通じて保存された情報を保存主体の医療機関等以外にも提供する場合は、あくまで医療機関等同士の合意で実施されなくてはならず、当然、個人情報保護法に則り、患者の同意も得た上で実施する必要があります。

このような場合において、外部保存を受託する事業者がアクセス権の設定を受託しているときは、医療機関等又は医療機関等に対して同意した患者の求めに応じて適切な権限を設定する等して、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）が起こらないようにしなくてはなりません。

したがって、このような形態で外部に診療録等を保存しようとする医療機関等は、外部保存を受託する事業者に対して、契約書等でこれらの情報提供についても規定しなくてはなりません。

外部保存を受託する事業者が医療機関等から委託を受けて情報を保存する場合、不当な利益追求を目的として情報を閲覧、分析等を行うことはあってはならず、許されません。したがって、外部保存を受託する事業者を選定する場合、医療機関等はそれらが実施されないことの確認、又は実施させないことを明記した契約書等を取り交わす必要があります。

外部保存の技術的な方法としては、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ことも考えられます。

さらに、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、あるいは医療情報システム・サービス事業者の管理者といえどもアクセスできない制御機構をもつことも考えられます。

具体的には、「暗号化を行う」、「情報を分散保管する」方法が考えられます。この場合、不測の事故等を想定し、情報の可用性に十分留意しなければならなりません。

医療機関等が自ら暗号化を行って暗号鍵を保管している場合、火災や事故等で暗号鍵が利用不可能になった場合、全ての保存委託を行っている医療情報が利用不可能になる可能性があります。

これを避けるためには暗号鍵を、外部保存を受託する事業者に預託する、複数の信頼できる他の医療機関等に預託する等が考えられます。分散保管においても同様の可用性の保証が必要です。

ただし、外部保存を受託する事業者に暗号鍵を預託する場合においては、暗号鍵の使用について厳重な管理が必要です。

外部保存を受託する事業者による暗号鍵の不正利用を防止するため、暗号鍵の使用について運用管理規程を策定し、使用を非常時に限定しなければなりません。また、実行時に暗号鍵を使用した証跡が残る暗号手法等を利用し、医療情報システムにおける証跡管理等を適切に実施することで、暗号鍵が不正利用されていないかを確認する必要がある。

企７章第⑥条

企Q－26　外部保存を委託する事業者の選定において、どのような留意事項があるか。

Ａ　法令上の保存義務を有する医療機関等は、システム堅牢性の高い安全な情報の保存場所を選定する必要があります。

また、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」の要求事項も満たす必要があります。

なお、選定にあたっては、外部委託事業者のセキュリティ対策状況を確認することが必要です。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」や「『製造業者/サービス事業者によるによる医療情報セキュリティ開示書』ガイド」によって、外部保存を受託する事業者におけるセキュリティ対応状況の概要を確認することができるため、サービスの性質等、必要に応じてその提供を求めることなどが有効です。

外部保存されている医療情報は、保存される情報やその目的に応じて厚生労働省等、所管する行政機関の調査等に供するため、提出等を行う必要が生じうることから、これを円滑に実現できることが求められます。そのため外部保存の受託事業者の選定にあたっては、国内法の適用があることや、逆にこれを阻害するような国外法の適用がないことなどを確認し、適切に判断した上で選定することが求められます。

企７章第⑥条

企Q－27　ISMS 認証を取得している事業者に対して、根拠資料を求めることはできるのか。

Ａ　例えば、ISMS 認証を取得している事業者の選定に際して、選定対象となる事業者が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てください。

企７章第⑥条

企Q－28　7. 安全管理のための人的管理⑥ｇの「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」とは、「政府情報システムのためのセキュリティ評価制度（ISMAP）」や「JASA クラウドセキュリティ推進協議 会 CS ゴールドマーク」等で公開されたサービスリストやマーク取得サービス一覧などに掲載されていることを確認することでよいか。

Ａ　サービスリストやマーク取得サービス一覧に掲載されたクラウドサービス であることだけをもって適切な外部保存に求められる技術及び運用管理能力 があるとはいえず、ISMAP や CS ゴールドマーク取得サービスでの評価、取得に際し、審査対象を定めた「言明書」が公開されているので、当該言明書を確認の上、事業者を決定してください。

企７章第⑦条

企Ｑ－29　外部保存を委託する場合のデータ閲覧権限はどうするといいか。

Ａ　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、原則として委託元の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てください。

企７章第⑦条

企Ｑ－30　個人識別に係る情報を適切に保管するために、外部保存を委託する事業者にどのような対策を求めればいいか。

Ａ　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ようにしてください。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ます。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てください。

企７章第⑨条

企Ｑ－31　外部保存の委託を終了する際、どのような留意事項があるか。

Ａ　診療録等が機微な個人情報であるという観点から、外部保存を終了する場合には、医療機関等及び受託する事業者双方で一定の配慮をしなくてはなりません。

　診療録等の外部保存を委託する医療機関等は、受託する事業者に保存されている診療録等を定期的に調べ、外部保存を終了しなければならない診療録等は速やかに処理した上で、当該処理が厳正に執り行われたかを監査しなくてはなりません。また、外部保存を受託する事業者も、医療機関等の求めに応じて、保存されている診療録等を厳正に取扱い、処理を行った旨を医療機関等に明確に示す必要があります。

　これらの廃棄・返却に関わる規定は、外部保存を開始する前に委託契約書等にも明記をしておく必要があります。また、実際の廃棄・返却に備えて、事前にソフトウェア等の廃棄・返却の手順を明確化した規定を作成しておくべきであります。

　これらの厳正な取扱い事項を双方に求めるのは、同意した期間を超えて個人情報を保持すること自体が、個人情報の保護上問題になり得るためであり、そのことに十分に留意しなければなりません。

　ネットワークを通じて外部保存する場合は、外部保存システム自体も一種のデータベースであり、インデックスファイル等も含めて慎重に廃棄しなければなりません。また電子媒体の場合は、バックアップファイルについても同様の配慮が必要です。

また、ネットワークを通じて外部保存している場合は、自ずと保存形式が電子媒体となるため、情報漏えい時の被害は、その情報量の点からも甚大な被害が予想されます。したがって、個人情報保護に十分な配慮を行い、確実に情報が廃棄されたことを、外部保存を委託する医療機関等と受託する事業者とが確実に確認できるようにしておかなくてはなりません。

企７章第⑩条

企Ｑ－32　医療情報の外部保存に関して、院内掲示以外の患者等への周知方法はどのようなものがあるか。

Ａ　院内掲示以外の周知方法としては、パンフレットの配布、問診表への記載、医師・看護師等による口頭説明等があります。さらに、インターネット上の医療機関等のホームページ上での公表を加えることもできます。

企７章第⑩条

企Ｑ－33　病態、病歴等を含めた個人情報の外部保存を行う場合、患者等にどのような説明を行うべきか。

Ａ　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してください。

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。

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。

８．情報管理（管理、持ち出し、破棄等）

企８章第③条

企 Q－34　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の方法として、どのようなものが挙げられるか。

Ａ　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してください。

例えば、次に掲げる対策を実施してください。

- 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。

企８章第⑥条

企 Q－35　情報及び情報機器の持ち出しを認める場合、どのような留意事項があるか。

Ａ　昨今、医療機関等において医療機関等の職員や医療情報システム・サービス事業者による情報及び情報機器の持ち出しにより、個人情報を含めた情報が漏えいする事案が発生しています。

一方で、在宅医療、訪問診療等の増加、モバイル端末の発展により医療情報を持ち出すニーズや機会が増加しています。

情報の持ち出しについては、ノートパソコン、スマートフォンやタブレットのような情報端末や CD-R、USB メモリのような可搬媒体が考えられます。また、情報をほとんど格納せず、ネットワークを通じてサーバにアクセスして情報を取り扱う端末（シンクライアント）のような情報機器も考えられます。さらにネットワークを通じてクラウドサービスを利用して持ち出すケースも想定されます。

まず重要なことは、「６．リスクマネジメント（リスク管理）」で述べていますように、取り扱う情報を適切に把握した上で、その情報についてリスク分析を実施することです。

その上で、医療機関等において把握している情報又は情報機器を持ち出してよいのか、持ち出してはならないのかの切り分けを行うことが必要であります。切り分けを行った後、持ち出してよいとした情報又は情報機器に対して対策を立てなくてはなりません。

適切に情報が把握され、リスク分析がなされていれば、それらの情報や情報機器をどのように管理すべきかが明確になります。例えば、情報の持ち出しについては許可制にする、情報機器は登録制にする等の対策も管理を明確にし、状況を把握するための方策となります。

一方、医療機関等の管理外のパソコン等の情報機器で、可搬媒体に格納して持ち出した情報を取り扱う時に、不正ソフトウェアの混入や不適切な設定のされたソフトウェアやサービスの利用、外部からの不正アクセスによって情報が漏えいすることも考えられます。この場合、情報機器が基本的には個人の所有物となりますが、そのような機器等の利用や情報の取扱いについては医療機関等の企画管理者の責任において把握する必要があります。

スマートフォンを利用する際の安全対策については、「スマートフォン・クラウドセキュリティ研究会最終報告～スマートフォンを安心して利用するために実施されるべき方策～」（総務省；平成 24 年６月）が参考になります。

企８章第⑤条

企Ｑ－36　「リスク評価に基づいて、医療情報の持ち出しに関する方針や、持ち出す情報、持ち出し方法に関する手順や管理方法を情報管理に関する規程で定める。」とあるが、具体的にどのような基準で判断をすればよいか。

Ａ　当該情報機器が医療情報を記録しているか否かで取扱いが異なります。

医療情報を記録している機器や媒体であれば、持ち出しには細心の注意が必要です。このような機器や媒体は、原則として持ち出すべきではないという基準にすべきです。その上で、やむを得ず持ち出す際には、情報機器を持ち出す必要性や漏えいのリスクを総合的に判断した上で、運用管理規程等に機器持ち出しの許諾ルールと判断基準を策定することが求められます。また、持ち出す機器については、システム運用編「７．情報管理（管理・持出し・破棄等）」に示す適切な防護措置を施すことが必要です。

リモートサービス等により医療機関等の情報にアクセスできる機器の場合、医療情報を機器に記録していなくても、機器そのものの盗難や置き忘れが情報漏えいのリスクになります。このような場合、機器に対する防護措置に加え、リモートサービスそのものでの防護措置が必要であり、システム運用編「７．情報管理（管理・持出し・破棄等）」に示された安全管理対策を実施していることが条件になります。

上記以外の情報機器については、機密情報の有無やその他の要件を考慮し、医療機関等における管理ルールを策定してください。

企８章第⑨条、シス７章⑧条、⑭条

企Ｑ－37　患者等に診療情報等を提供する場合、どのような留意事項があるか。

Ａ　まず原則として、医療機関等が患者等との同意の上で、自ら実施して患者等に診療情報等を提供する場合であることが想定されます。診療録及び診療諸記録の外部保存を受託する事業者が独自に診療情報等の提供を行うことはあってはなりません。

ネットワークを介して患者等に診療情報等を提供する場合、第一に意識しておかなければならないことは、診療情報等を閲覧する患者等のセキュリティ知識と環境に大きな差があるということです。また、一旦診療情報等を提供すれば、その情報保護の責任は医療機関等ではなく、患者等にも発生します。しかし、診療情報等を提供する医療機関等が患者等に十分に患者がセキュリティ対策の必要性や管理の責任を負うこと等の理解すべき事項を説明し、その提供の目的を明確にする責任があります。また、説明が不足している中で万一情報漏えい等の事故が起きた場合は、その責任を負う可能性があることを認識しなくてはなりません。

提供に用いるネットワークとしては、一般的にはオープンなネットワークを介することが現実的です。この場合、盗聴等の危険性は極めて高くなります。そのため利活用と安全確保の両面を考慮したセキュリティ対策が必須でとなります。特に、患者等に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しておく必要があります。そのため、ファイアウォール、アクセス監視、通信の TLS 暗号化、PKI 個人認証等の技術を用いるなどが求められます。

また、患者の委託先に診療情報等を送付する(クラウドサービスへのアップロード含む)際、外部の事業者に対して送付するよう、患者から依頼を受ける場合も想定されます。この場合、患者の委託先への送付であることから、第三者提供には当たらないものの、診療情報等の流出などに対する留意が求められる。送信先／アップロード先についての安全性等について疑義が生じた場合に患者からの依頼を断るなどのほか、送信等を行うに当たっては、患者との関係で責任分界についても取り決めておくことが求められます。

企８章⑫条

企Ｑ－38　「確実に情報の破棄されたことを確認すること」とは立ち会いを前提としているのか。

Ａ　立ち会いを前提とはしていません。破棄を行った証票を受け取る等、「７．安全管理のための人的管理（職員管理、委託先事業者管理、教育・訓練、委託先事業者選定・契約）」の内容を遵守し、確実に確認していただければ問題ありません。

９．医療情報システムに用いる情報機器等の資産管理

企９章②条関係

企 Q－39　情報及び情報機器の持ち出し並びに外部利用をする場合にどのような対応が必要か。

Ａ　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してください。

企９章④条関係、シス９章④条

企Q－40　事前の確認時と状況が変わり、請負事業者が倒産する等してソフトウェアの保証がなくなった場合、見読性は確保されていないことになるのか。

Ａ　倒産ではなく、請負事業者がソフトウェア事業を廃止する場合は、見読性を確保する条項等を契約書に明記することで、見読性を確保できます。

しかし、倒産の場合、使用継続は保証されるものの、長期の見読性は保証されないこととなり、使用者がこれを担保する必要があります。診療等に差し支えない期間内に見読性が保証される対策を講じなければならず、この対策を容易にするためにも標準化や相互運用性の確保は重要です。

11．システム運用管理（通常時・非常時等）

企１１章②条

企Q−41　医療情報システムに関するBCP（Business Continuity Plan：事業継続計画）の作成は、医療機関にとってどのような場面を想定するといいか。

A　我が国は大規模な自然災害が比較的多く見られ、事例の蓄積も多い。そのため医療情報システムが通常の状態で使用ができない事態に陥った場合における適切な BCP の作成と訓練は可能であり、必須の事項と考えられます。

「通常の状態で使用できない」とは、使用環境が非定常状態になる場合と、システム自体が異常動作又は停止になる場合とがあります。

前者は、自然災害発生時には多数の傷病者が医療サービスを求める状態になり、医療情報システムが正常であったとしても通常時のアクセス制御下での作業では著しい不都合の発生が考えられる場合です。この際の個人情報保護に関する対応は、「生命、身体の保護のためであって、本人の同意を得ることが困難であるとき」に相当すると解せられます。

後者は、医療情報システムが自然災害やサイバー攻撃等により、システム的に損傷を被ることにより、システムの縮退運用又は全面停止に至り、医療サービス提供に支障発生が想定される場合です。

企１１章②条

企Q−42　BCP（Business Continuity Plan：事業継続計画）の内容を検討する上で、参考になる内容はあるか。

A　以下に、BCP として策定すべき項目と運用に関する一般項目を参考に示します。

① BCP として事前に周知しておく必要がある事項

事前に関係者に対応策の周知を行い、信頼を得ておく必要がある。

- ポリシーと計画：何が「非常事態」なのかを理解し、定義すべきである。
- 非常事態検知手段：災害や故障の検知機能と発生情報の確認手段
- 非常時対応チームの連絡先リスト、連絡手段及び対策ツール
- 非常時に公にすべき文書及び情報

② BCP 実行フェーズ

災害、事故やサイバー攻撃等の発生（あるいは発生の可能性）を検知してから、BCP 実行か通常の障害対策かの判断を行い、BCP 実行と判断した場合は関係者の召集、対策本部等の設置、関係先への連絡・協力依頼を行い、システムの切り替え／縮退等の準備を行う。例えば、ネットワークから切り離したスタンドアロンでの使用や、紙での運用等が考えられる。

業務を受託する事業者との間の連絡体制や受託する事業者と一体となったトラブル対処方法等が明示されるべきである。また、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べきである。

具体的項目は、「基本方針の策定」、「発生事象の確認」、「安全確保・安否確認」、「関係先への連絡」及び「影響度の確認」である。

③ 業務再開フェーズ

BCP を発動してから、バックアップサイト・手作業等の代替手段により業務を再開し、軌道に乗せるまでのフェーズで、代替手段への確実な切り替え、復旧作業の推進、要員等の人的資源のシフト、BCP 遂行状況の確認、BCP 基本方針の見直しがポイントである。

最も緊急度の高い業務（基幹業務）から再開する。

具体的項目は「人的資源の確保」、「代替施設及び設備の確保」、「再開／復旧活動の両立」及び「リスク対策によって新たに生じるリスクへの対策」である。

④ 業務回復フェーズ

最も緊急度の高い業務や機能が再開された後、さらに業務の範囲を拡大するフェーズで、代替設備や代替手段を継続する中での業務範囲の拡大となるため、現場の混乱に配慮した慎重な判断がポイントとなる。

具体的項目は「拡大範囲の見極め」、「業務継続の影響確認」、「全面復旧計画の確認」及び「制限の確認」である。

⑤ 全面復旧フェーズ

代替設備・手段から平常運用へ切り替えるフェーズで、全面復旧の判断や手続きのミスが新たな業務中断を引き起こすリスクをはらんでおり、慎重な対応が要求される。

具体的項目は「平常運用への切り替えの判断」、「復旧手順の再確認」、「確認事項の整備」及び「総括」である。

⑥ BCP の見直し

正常な状態に復帰した後に、BCP に関する問題点や見直しを検討することが必要である。実際の非常事態においては、通常では予想し得ないような事象が起こることも少なくない。実際の対応における成功点、失敗点を率直に評価、反省し、BCP の見直しを行い、次の非常時に備えることが重要である。

企１１．３章、シス１１．２章

企Ｑ－43　災害等で電子システムが運用できない場合で、一時的に運用した紙データを後から電子システムに反映させることは、真正性の観点から問題にならないか（システムへの入力時のタイムスタンプが有効になるのではないか。）。

Ａ　適切な安全管理が実施されていれば、問題ありません。「１１．非常時（災害、インシデント、サイバー攻撃被害、システム障害）対応と BCP 策定」において要求事項が記載されているため、そちらを参照してください。

　また、紙データを電子システムに反映させる際に、紙データをオリジナルとして保存する必要が生じると考えられます。オリジナルの紙データをスキャナ等により電子化して保存する場合は、「１６．紙媒体等で作成した医療情報の電子化」を参照してください。

　電子カルテ等に転記した場合、転記した情報で診療等を実施することに問題はありません。ただし、オリジナルとしての紙若しくはスキャナ等で電子化したデータは、別途適切な安全管理を実施した上で、定められた期間保存する必要があります。

13. 医療情報システムの利用者に関する認証等及び権限

企１３章第②条

企Ｑ−44　「医療情報システムで利用する認証方法が安全なものとなるよう」にするために、どのようなリスクを想定すればよいか。

Ａ　利用者の識別・認証に用いられる情報が第三者に漏れがないように以下のようなリスクに対処することが想定されます。

- ID とパスワードが書かれた紙等が貼られていて、第三者が簡単に知ることができてしまう。
- パスワードが設定されておらず、誰でもシステムにログインできてしまう。
- 初期設定のパスワードが変更されておらず、利用者以外の者でもシステムにログインできてしまう。
- 代行作業等のために ID・パスワードを他人に教えており、システムで保存される作業履歴から作業者が特定できない。
- 一つの ID を複数の利用者が使用している。
- 容易に推測できる、あるいは、文字数の少ないパスワードが設定されており、容易にパスワードが推測できてしまう。
- 安全性が高くないパスワードを定期的に変更せずに使用しているために、パスワードが推測される可能性が高くなっている。
- 認証用の個人識別情報を格納するセキュリティ・デバイス（IC カード、USB キー等）を他人に貸与する、又は持ち主に無断で借用することにより、利用者が特定できない。
- 退職した職員の ID が有効になったままで、ログインができてしまう。
- 医療情報部等で、印刷放置されている帳票等から、パスワードが盗まれる。
- 不正ソフトウェアにより、ID やパスワードが盗まれ、悪用される。

企１３章第②条

企 Q－45　本人確認の方法として eKYC を採用する場合、どのような留意事項があるか。

A　eKYC （electronic Know Your Customer）は、従来、書面が使われていた利用者の身元確認のための資料を、電子的に対応するための仕組みになります。例えば金融機関における口座開設などで、本人の実在性を確認するために、従来は住民票等で身元確認を行ってきましたが、これに代わり、例えばマイナンバーカードを利用した公的個人認証サービスを利用するなど、オンラインで対応できるようになっています。

eKYC では、身元確認を行う際に、利用者が本人であることが前提となるため、これを利用者の認証方法とすることが考えられます。

ただし eKYC にも多様な方法などがあり、それに応じて本人認証に対する信頼性などが異なります。そこで、医療機関等が求める信頼性に応じたサービスを利用することが重要です。

また、eKYC はもともと身元確認を行うための手段なので、身元確認に必要な情報のやり取りが発生することもあります。そのため、単なるシステムの利用には不要な、利用者の個人情報の流通することもあり、その管理などを適切に行う必要なども生じます。

従って eKYC を採用する場合には、採用する eKYC の内容等を踏まえて、適切に行うことが求められます。

14. 法令で定められた記名・押印のための電子署名

企１４章第①条

企Q－46　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、どのような経緯があるか。

A　平成 11 年４月の「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通知」においては、法令で署名又は記名・押印が義務付けられた文書等は、「電子署名及び認証業務に関する法律」（以下「電子署名法」という。）が未整備の状態であったために対象外とされていました。

しかし、平成 12 年５月に電子署名法が成立し、また、e-文書法の対象範囲となる医療関係文書として e-文書法省令において指定された文書においては、「A. 制度上の要求事項」に示した電子署名によって、記名・押印に代わり電子署名を施すことで、作成・保存が可能となりました。

なお電子署名立会人型電子署名については、総務省・法務省・経済産業省から令和 ２年７月 17 日に示されている「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）」において、解説されていますが、これを解説するものとして「主務三省（電子署名法第３条関係）Q&A に関する解説」（電子認証局会議・トラスト・サービス推進フォーラム））があります（同解説は以下の URL から入手できます）。

https://www.dekyo.or.jp/tsf/wp-content/uploads/2021/02/%E9%9B%BB%E5%AD%90%E7%BD%B2%E5%90%8D%E6%B3%95Q%EF%BC%86A%E3%81%AB%E9%96%A2%E3%81%99%E3%82%8B%E8%A7%A3%E8%AA%AC.pdf

企１４章第①条の２

企Ｑ−47　通常閉域ネットワークを構築することが多い医療機関等において、一枚一枚の文書にリアルタイムにタイムスタンプを付与することは、実装が困難ではないか。

Ａ　「１４．法令で定められた記名・押印のための電子署名」は、診療情報提供書や診断書等の法令で記名・押印することが定められた文書等を対象としています。これら以外の文書等に一枚一枚タイムスタンプを付加することは必須ではありません。

しかしながら複数のスキャン画像ファイルなどにまとめてタイムスタンプを付す場合、方式によっては個々のファイルを個別に検証することができなくなるので留意が必要です。例えば、複数ファイルを ZIP ファイルに格納してタイムスタンプを付与した場合、タイムスタンプの検証時に ZIP ファイル全体を読み込む必要があり、ファイル個別に検証することができません。係争時等の外部提出を想定した場合に、関係のないファイルも提出する必要があるため適切な方法とはいえません。

そのため個別のファイルごとにタイムスタンプを検証することができる標準技術を使用すれば、適切にタイムスタンプを付すことができます。標準技術の例として、個々のファイルのハッシュ値を束ねて階層化した上で、頂点のハッシュにタイムスタンプを付す ERS（Evidence Record System）等があります。

なお、タイムスタンプを付与するにはセキュアなタイムスタンプ環境を構築する必要があります。

企１４章第①条

企Ｑ−48　クラウド型の電子カルテサービスを行う場合、利用者によるトランザクションごとに電子署名が必須となるのか。

Ａ　電子署名の付与に関する記述への対応として、個々のトランザクションを「ファイル」と考えれば、各々の情報単位で電子署名が必要になると解釈できないことはありません。しかし、ここではそれほど厳密な解釈を適用せず、トランザクション単位での電子署名の付与は不要だと考えられます。

本質問にある電子署名の付与には、２つの目的があると考えられます。１つは外部のネットワークを経由する際のメッセージの真正性の担保、もう１つはサービス側で情報を保存する際の真正性の担保（改ざん防止等の完全性の観点、否認防止の観点等）です。

これらを同時に満足するための技術的手法として、電子署名の付与は有効な方法です。しかし、これを個々のトランザクション・メッセージに適用することは必須ではありません。例えば、通信経路上の改ざん防止には、メッセージに電子署名を付与しないでも、TLS 等の適用で十分な場合があります。また、メッセージを保存する際に逐次電子署名を付与しなくても、それよりも大括りな情報単位（例えば一日単位）で電子署名を付与すること、あるいは本ガイドラインに例示された他の技術的手法・運用方法を適用することも可能です。

企１４章第①条の１⑵

企Ｑ−49　１４．法令で定められた記名・押印のための電子署名①⑵の「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⑻～⑹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」とあるが、要件を満たす具体的な手段は何か。

Ａ　２０２２（令和４）年 ３ 月 31 日時点で存在している、「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」に対し、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としては、１４．法令で定められた記名・押印のための電子署名①⑵)の⑻の「保健医療福祉分野 PKI 認証局の発行する電子証明書」

- 日本医師会 電子認証センターが発行する「医師資格証」
- 日本薬剤師会 認証局が発行する「薬剤師資格証」
- 医療情報システム開発センター(MEDIS) 電子認証局が発行する「HPKI 電子証明書」

があります。

なお、今後、⑻の「監査基準」を満たす新たな「保健医療福祉分野 PKI 認証局」や、(ｂ)の「適切な外部からの評価」を受けた事業者、電子的な資格確認に対応した(ｃ)の「公的個人認証サービス」による電子証明書が発行された場合、適宜、追加も考えられます。

企１４．２章の⑹

企Ｑ−50　１４．２　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の電子署名の要件 ⑹の２つ目の「・」の最初の「-」にある「医療機関等の管理者」とは、具体的には組織単位で考えればよいか。

Ａ　本ガイドラインにおける医療機関等とは「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」を指します。従ってここでも医療機関等ごとに管理者を設置することを想定しています。例えば、同一法人に複数の病院や診療所、薬局等が属している場合でも、それぞれの病院や診療所、薬局等の単位で管理者を設置することになります。

企１４．２章の(b)

企Q−51　１４．２　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の電子署名の要件(b)において、身分証明書や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）」とあるが、この「署名」と「押印」は同等と考えてよいか。

Ａ　郵送の場合、押印（実印が捺印され、印鑑登録証明書が添えてあること） に対して、署名が自署であることの確認を行うことが難しいため、署名をも って確認するには、医療分野の特性を踏まえ、十分に注意すること。

企１４章第①条の２

企Q−52　タイムスタンプはパソコンの時間と同じでよいか。

Ａ　タイムスタンプは電子署名を含む文書全体の真正性等を担保するために必要なものであることから、このガイドラインでは「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）が提供するものを利用することを求めています。※

※ 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、上記の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ありません。

企１４章第②条

企Q−53　暗号化を行うための適切な鍵管理を行うために、どのような対応が考えられるか。

Ａ　経路の暗号化や、電子署名・電子認証によるなりすましの防止や情報の改ざん防止を図る場合には、暗号／復号、デジタル署名に用いる鍵の管理を適切に行うことが重要である。特に共通鍵や、秘密鍵の管理を適切に行うことは、暗号化、デジタル署名の安全性を保証するために必要です。

鍵管理に求められる具体的な対応は、暗号鍵の利用目的に応じて異なる。すなわち、SSL/TLS、電子署名、その他外部との情報交換の際の暗号化、通信機器の認証などに応じて異なるため、それぞれにおいて必要な共通鍵、秘密鍵を保護する機能を具備することが求められます。本ガイドラインでは、電子署名や電子証明書を利用した本人認証などでは、電子証明書の認証を行う認証局が定める「証明書ポリシー」（Certificate Policy）に従って、管理することを求めています。

また、共通鍵や暗号鍵を格納する機器や媒体についても、一定の安全性が求められます。暗号モジュールに関するセキュリティ要件の仕様を規定するものとしては、米国連邦標準規格であるFIPS 140-2 (Federal Information Processing Standardization 140-2)※が定められています。機器等の安全性を担保するためには、この基準の最低限のレベルで求められる要件を具備することが望まれます。

※ FIPS140-2 では、製品に求めるセキュリティ要件として、Level1 から Level4 の 4 段階のレベルのものを定めている。このうち最も低い Level1 では、「製品レベルのコンポーネントの基本要件を満たす物理的セキュリティメカニズムが存在すればよい」とされる。(”SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES” P4 （NIST、2002.3.12）

15. 技術的な安全管理対策の管理

企１５章第②条

企Q−54　「8．情報管理（管理、持出し持ち出し、破棄等）③において医療情報が保存されている場所等については、記録・識別、入退室の制限等の管理を行うこと。また医療情報の保管場所には施錠等の対応を行うこと。」とあるが、例えば外来やナースステーション等では、それらの措置は困難ではないか。

A　外来やナースステーションでは患者や家族の入退がありますが、医療情報システムを導入していない場合にも行われているように、その事実をカルテ等に記録することにより、来訪を記録できます。

企１５章第⑧条

企Q−55　「2．1．1　医療機関等における責任と責任分界の運用管理においては、医療機関等と情報システム・サービス事業者事業者との間で決定された責任分界を、契約書や SLA（Service Level Agreement：サービス品質保証、サービスレベル合意書）などの形で双方の拘束力ある合意文書として明らかにしたうえで、具体的に責任分界を踏まえた運用を行うことが求められる。」とあるが、契約書の記載方法を教えてほしい。

A　「2．責任分界」に掲げている事項に関し、個別に責任範囲及び共同対応範囲を定めて、誰が何をどのタイミングで行うかを文書化してください。

　また、通信サービスを提供する事業者等に対しては、SLA（Service Level Agreement）を確認し、SLA に記載されていない若しくは不足する部分があれば、その部分について SLA の修正を要請する又は個別契約を結ぶことで対応してください。

企１５章第⑬条

企Q−56　外部の医療機関等から持ち込まれた X 線写真（コピー）や画像データを当院での診療に用いた場合、保存義務は生じるのか。

A　原本の保存義務は元の医療機関等にありますが、持ち込まれた診療情報を診療に利用した場合は、当該医療機関等においても保存義務が発生します。

企１５章第⑧条

企 Q－57　保守要員の専用アカウントの不正使用を防止するためにどのような方法があるか。また保守作業にあたってどのような作業を求めるといいか。

Ａ　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てください。

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、医療情報システム・サービス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してください。

医療情報システム・サービス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てください。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医療情報システム・サービス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ます。

16. 紙媒体等で作成した医療情報の電子化

企１６章第③条

企Ｑ−58　「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・タイムスタンプ等を遅滞なく行うこと。」とあるが、これは取り込み責任者を明確にすることか。

Ａ　取り込み責任者を明確にする目的だけでなく、改ざんやなりすましを防止するために、また、作業内容の正確性についての説明責任を果たすために実施するものです。

企１６章第③条

企Ｑ−59　「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。」とあるが、一定期間以内とはどれ位をいうか。外来診療の場合、１日の診療が終わった後にまとめて行う等の運用でもよいか。

Ａ　原則は１日以内です。ただし、深夜に来院し、次の日が休診である場合等は営業日として１日以内となります。

企１６章第⑤条

企Ｑ−60　どの程度の期間内でスキャナ等により電子化して保存すべきか。

Ａ　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ります。

企１６章第⑥条

企Ｑ−61　電子カルテを導入した場合、それまでの旧カルテ（紙カルテ）について保存義務があるか。あるとすれば何年か。

Ａ　紙の診療録の法定保存年限は医師法で一連の診療の終了後５年とされています。ただし、電子カルテの導入により、以前の紙の診療録がスキャナ等で適切に電子化されており、管理責任者によって保存義務の対象が電子化された診療録であると認められていれば、紙の診療録に法定上の保存義務はありません。このような処理を行わない場合は、法定の保存義務があります。

なお、情報の真正性、保存性の確保の観点から、スキャナ等で電子化して運用する場合でも、元の媒体である紙の診療録を併せて保存することは有効であり、法定期限に限らず保存することが望ましいです。ただし、この場合も電子化及び保存に関しては、「６.紙媒体等で作成した医療情報の電子化」等を参照の上、適切に実施する必要があります。

企１６章第⑥条

企Ｑ−62 ①　診療録等をスキャナで電子化した場合、原本の取扱いはどのようにすべきか。 ②　電子化された場合、法定保存年限を経過した文書も保存すべきと考えるべきか。

Ａ　「９.１　共通の要件」の記載に従って電子化し、電子化されたものを保存義務のある対象とする場合は、スキャンされた原本は個人情報保護の観点に注意して廃棄しても構いません。しかし、電子化した上で、元の媒体も保存することは真正性・保存性の確保の観点からきわめて有効であり、破棄を義務付けるものではありません。また、法定保存年限を経過した文書の保存期限は、各医療機関等で規定することとなります。

企１６章第⑦条

企Ｑ－63	「「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」とあるが、電子保存した内容を再度プリントアウトして、訂正後に再度電子化して保存するといった運用でもよいか。

Ａ　調剤済み処方箋をスキャナ等により電子化し、電子化した情報を原本とした後に修正を行う場合、真正性の確保の観点から、過去の電子署名の検証が可能な状態を維持する形で電子的に修正し、薬剤師の電子署名を付す必要があります。

そのため、プリントアウトしたものに訂正を行い、再度スキャナ等により電子化して保存することは、真正性の確保の観点から適切ではないと考えます。

スキャナ等による電子化は、１６．紙媒体等で作成した医療情報の電子化 に規定されているように、医療機関等において運用管理規程を適切に定めて実施されるものです。

例えば、事後修正が生じる可能性が十分低くなってから、スキャン等により電子保存する、又はスキャンした紙の調剤済み処方箋を一定期間バックアップとして保存すること等が考えられます。このような対応を講じることで、当該処方箋に修正の必要が生じた際に、スキャン等により電子化した情報を破棄した上で、その紙媒体を原本として修正を行い、改めてスキャン等により電子保存することができます。

企１６章第⑧条、シス１６章第①条

企Ｑ－64　紙媒体等をスキャナ等で電子化保存する場合は、どの程度の解像度がいいか。

Ａ　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してください。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す。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ます。

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）」を参考にしてください。

このほか心電図等の波形情報やポ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、その点に十分配慮してください。

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してください。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ります。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してください。

システム運用編

システム運用編

５．システム設計の見直し（標準化対応、新規技術導入のための評価等）

シス５章

シQ－１　「５．システム設計の見直し（標準化対応、新規技術導入のための評価等）」は具体的に何を遵守すればよいのか。

Ａ　「５．システム設計の見直し（標準化対応、新規技術導入のための評価等）」では、相互運用性の重要性と、それを実現するために医療機関等がシステムベンダに要求すべき内容が記述されています。具体的には、医療機関等はシステムベンダの標準化に対する基本スタンス、（標準に対応していないならば、その理由や対応案）についてシステムベンダから説明を受け、一定の理解を等しくしておくことが求められます。さらに、現在導入しているシステムの更新やシステムの新規導入の際に、システム間でのデータ互換性やシステム接続性が確保されるように、医療機関等においても相互運用性に係る中長期的なビジョンを持ち、計画的にベンダへ要求していくことが望まれます。

シス５．１章

シQ－２ ①　相互運用性と標準化を行うことのメリットは何か。 ②　基本データセットや標準的な用語集、コードセットを実装しなかった場合、どのような不利益が想像されるか。

Ａ　標準化のメリットには、システム間の相互運用性、データの長期的可用性等の確保があります。患者紹介や地域医療情報連携等で外部の医療機関等と医療情報をやり取りする場合、使用されているコードや用語が標準的でないと、適切な情報交換が難しくなります。また、システムをリプレイスする場合も、データ変換等が必要になってしまいます。これらの場合に、コードや用語が標準化されていれば、データ変換の手間や、変換機能の実装のための費用と時間の節約が期待できます。

　このような表受な対応を行わず、基本データセットや標準的な用語集、コードセットを実装しなかった場合、システム更新時のデータ移行に伴う作業によって、見読性、真正性の責任が果たせなくなることがあります。

シス５章第①条

シQ－３　「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、標準項目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」とあるが、標準形式は正式に定められたものがあるのか。

Ａ　標準化については、既に一定のレベルで確立された標準の情報項目等を利用することにより、以下の診療情報については高いデータ互換性を確保することが可能となりつつあります。これらは医療情報システムとして最も高いレベルの相互運用性が必要とされます。

- 医療機関情報
- 当該医療機関での受診歴
- 患者基本情報病名
- 保険情報
- 処方指示（含む用法）
- 検体検査（指示及び結果）
- 放射線画像情報
- 生理検査図形情報
- 内視鏡画像情報
- 注射
- 手術術式

これらの情報の相互運用性を確保するために必要とされ、これまでに確立された各種標準について、以下に示します。

【厚生労働省標準規格】

厚生労働省では通知「保健医療情報分野の標準規格として認めるべき規格について」で、厚生労働省における保健医療情報分野の標準規格（「厚生労働省標準規格」）を定め、その実装を推奨しています。

これは民間団体であるHELICS協議会によって制定された「医療情報標準化指針」で採択された規格等について、厚生労働省の保健医療情報標準化会議で審議され、その結果として出された提言に基づいて定められたものです。

令和５年３月現在、以下の規格等が厚生労働省標準規格に採択されています。

- HS001 医薬品HOTコードマスター
- HS005 ICD10対応標準病名マスター
- HS007 患者診療情報提供書及び電子診療データ提供書（患者への情報提供）
- HS008 診療情報提供書（電子紹介状）
- HS009 IHE統合プロファイル「可搬型医用画像」およびその運用指針
- HS011 医療におけるデジタル画像と通信（DICOM）

- HS012 JAHIS 臨床検査データ交換規約
- HS013 標準歯科病名マスター
- HS014 臨床検査マスター
- HS016 JAHIS 放射線データ交換規約
- HS017 HIS,RIS,PACS,モダリティ間予約,会計,照射録情報連携指針（JJ1017 指針）
- HS022 JAHIS 処方データ交換規約
- HS024 看護実践用語標準マスター
- HS026 SS-MIX2 ストレージ仕様書および構築ガイドライン
- HS027 処方・注射オーダ標準用法規格
- HS028 ISO 22077-1:2015 保健医療情報ー医用波形フォーマットーパート１：符号化規則
- HS030 データ入力用書式取得・提出に関する仕様（RFD）
- HS031 地域医療連携における情報連携基盤技術仕様
- HS032 HL7 CDA に基づく退院時サマリー規約
- HS033 標準歯式コード仕様
- HS034 口腔審査情報標準コード仕様
- HS035 医療放射線被ばく管理統合プロファイル
- HS036 処方情報 HL7 FHIR 記述仕様
- HS037 健康診断結果報告書 HL7 FHIR 記述仕様
- HS038 診療情報提供書 HL7 FHIR 記述仕様
- HS039 退院時サマリーHL7 FHIR 記述仕様

なお厚生労働省標準規格は、今後も保健医療情報標準化会議の提言等を踏まえ、適宜更新される方針ですので、必要に応じ、適宜最新版を参照する必要があります。最新版は、下記の URL から参照可能です。
https://www.mhlw.go.jp/seisakunitsuite/bunya/kenkou_iryou/iryou/johoka/index.html

【基本データセット】
経済産業省は、平成 20 年に「医療情報システムにおける相互運用性の実証事業（相互運用性実証事業）」において、一般社団法人保健医療福祉情報システム工業会（JAHIS）等に委託し、基本データセットとそれらを用いたシステム間でのデータのエクスポート・インポートのためのガイドラインを整備しました。
この基本データセットには以下が含まれます。
- 利用者情報
- 医療情報（基本情報）
- 医療情報（感染症、アレルギー情報、入退院歴、受診歴）
- オーダ情報（処方、検体検査、放射線）
- 検査結果情報（検体検査）
- 病名情報

- 注射に関わる指示、実施情報等
- 処置・手術

最新の基本データセットは JAHIS においてメンテナンスされています。データの互換性を確保するために、以下のガイドラインを参照する必要があります。

- JAHIS 基本データセット適用ガイドライン（第３版）
  https://www.jahis.jp/standard/contents_type=33

【用語集・コードセット】

前述の厚生労働省標準規格の制定に先立ち、厚生労働省は一般財団法人医療情報システム開発センター（MEDIS-DC）への委託事業により、以下の標準マスターを作成し、その後も維持管理を継続しています。これらの標準マスター類の一部は厚生労働省標準規格にも採択されています。

- 病　　名：病名マスター（ICD10 対応標準病名マスター）
- 手術・処置：手術・処置マスター
- 臨 床 検 査：臨床検査マスター（生理機能検査を含む）
- 医　薬　品：医薬品 HOT コードマスター
- 医 療 機 器：医療機器データベース
- 看 護 用 語：看護実践用語標準マスター
- 症 状 所 見：症状所見マスター＜身体所見編＞
- 歯 科 病 名：歯科病名マスター
- 歯科手術等：歯科手術・処置マスター
- 画 像 検 査：画像検査マスター

- J－MIX：電子保存された診療録情報の交換のためのデータ項目セット
- MEDIS 標準マスター類
  https://www.medis.or.jp/4_hyojyun/medis-master/index.html

MEDIS-DC では、前述の相互運用性実証事業において医薬品と臨床検査については、各医療機関が定める独自の用語・コードから標準的な用語、コードにマッピングするためのツールを開発しています。

シス５．１章

シQ－４　基本データセットを利用し、一般財団法人医療情報システム開発センター（MEDIS-DC）の標準マスタを組み合わせた場合、医療情報システムのリプレイス時の相互運用性は保証されるか。

A　基本データセット及び標準マスタを活用することは、相互運用性の確保を容易にしますが、保証はされません。なお、基本データセットに含まれない項目や標準が定められていない用語・コードも存在します。

　基本データセットや標準マスタは、概ね重要あるいは実装頻度の高いものを対象にしており、採用することによって、相互運用性を確保するためのコストを大幅に下げることができます。

シス５．１章

シQ－５　データ交換のための国際的な標準規格については、どのようなものがあるか。

A　医療情報に関する国際的な標準である HL7（Health Level Seven）や DICOM（Digital Imaging and Communications in Medicine）については、我が国において利用可能なように、JAHIS により標準規約化されています。

　主要なものとしては以下が挙げられます（一部は厚生労働省標準規格にも採択されています）。これらの規約は以下の URL で取得できます。

https://www.jahis.jp/standard/contents_type=33

- JAHIS 病理・臨床細胞 DICOM 画像データ規約
- JAHIS 病理診断レポート構造化記述規約
- JAHIS 処方データ交換規約
- JAHIS 生理検査データ交換規約
- JAHIS ヘルスケア PKI を利用した医療文書に対する電子署名規格
- JAHIS 内視鏡データ交換規約
- JAHIS 内視鏡 DICOM 画像データ規約
- JAHIS 病理・臨床細胞データ交換規約
- JAHIS 放射線データ交換規約
- JAHIS 放射線治療データ交換規約
- JAHIS 臨床検査データ交換規約
- JAHIS 生理機能検査レポート構造化記述規約
- JAHIS 病名情報データ交換規約
- JAHIS 注射データ交換規約
- JAHIS ヘルスケア分野における監査証跡のメッセージ標準規約
- JAHIS 介護標準メッセージ仕様
- 健康診断結果報告書規格

- リモートサービスセキュリティガイドライン
- JAHIS シングルサインオンにおけるセキュリティガイドラン
- JAHIS 心臓カテーテル検査レポート構造化記述規約
- JAHIS 診療文書構造化記述規約共通編
- JAHIS データ交換規約（共通編）
- JAHIS 保存が義務付けられた診療録等の電子保存ガイドライン
- JAHIS HPKI 電子認証ガイドライン
- HPKI 対応 IC カードガイドライン
- JAHIS 内視鏡検査レポート構造化記述規約

また医療情報システムの相互接続性を推進する国際的なプロジェクトの IHE（Integrating the Healthcare Enterprise）では、標準規格の使い方が定まっていないことに起因する問題を解決するために、標準規格の使い方の「ガイドライン」として Technical Framework を提案しています。これは、分野ごとに実際の医療現場での一般的なワークフロー調査を行い、その上でシステム連携を実現するために必要となる標準規格の使い方を示したガイドラインです。詳細は以下の URL から得られます。

https://www.ihe-j.org/

なお、日本 IHE 協会が IHE Technical Framework を参照した「地域医療連携における情報連携基盤技術仕様」を策定しており、厚生労働省標準規格として採択されています。

シス５．１章

シＱ－６　外字の使用について注意すべき点は何か。

Ａ　外字を使用したシステムでは、あらかじめ使用した外字のリストを管理しておき、システムを変更した場合又は他のシステムと情報を交換する場合に、表記に齟齬のないよう対策する必要があります。

シス５章第④条

シＱ－７　診療情報等が復元できなくなることなどが生じないように、どのような対応をすべきか。

Ａ　媒体・機器・ソフトウェアの不整合により、電子的に保存されている診療録等の情報が復元できなくなることがあります。具体的には、システム移行時にマスタデータベース、インデックスデータベースに不整合が生じること、機器・媒体の互換性がないことにより情報の復元が不完全となる又は読み取りができなくなること等です。このようなことが起こらないように、システム変更・移行時の業務計画を適切に作成する必要があります。

シス５章第④条

シQ－８　見読性を確保するために、どのような対応が必要か。

Ａ　電子媒体に保存された情報は、紙に記録された情報と違い、以下の理由によりそのままでは見読できない場合があります。

- 電子媒体に格納された情報を見読可能なように画面に呼び出すために、何らかのアプリケーションが必要である。
- 記録が、他のデータベースやマスター等を参照する形で作成されることが多く、データの作成時点で採用したマスター等に依存しなければ、正しい記録として見読できない。
- 複数に分かれて記録された情報の相互関係が、そのままでは一瞥して分かりにくい。

そのため、紙の記録と同等といえる見読性を確保するためには、電子媒体に保存された情報は、これらのことに適切に対応する必要があります。

また、ネットワークを通じて外部に保存する場合は、これらのことに適切に対応することに加えて、外部保存先の事業者におけるシステムやサービス等により見読性が損なわれることを考慮し、十分な配慮が求められます。その際には、あらかじめ事業者との間で責任を明確化しておき、速やかな復旧が図られるように配慮しておく必要もあります。

シス５章第④条

シQ－９　汎用性が高く、見読するソフトウェアに困らない形式にはどのようなものがあるのか。

Ａ　医療情報には様々な形態の情報があり、画像、図形、波形、テキスト、数値、グラフ等の形式のデータから構成されています。これらのデータを一様に見ようとするならば、画像化することが、おそらく最も汎用性の高い見読化手段になるでしょう。デジタル情報を画像化するには、PDF（Portable Document Format）が一般的な形式だと考えられます。紙やフィルムの形で存在する場合には、スキャナ等を用いて画像化することで見読可能にできますが、この場合には JPEG（Joint Photographic Experts Group）、PNG（Portable Network Graphics）等の形式を利用することができます。

これらのフォーマットは、PC やスマートフォンなどの情報機器で容易に取得できるソフトウェアによって見読可能な状態にすることができます。

シス５章第④条

シQ－10　X 線 CT の検査で、オリジナルの画像のほかに、オリジナル画像から生成した３D画像も使って診断している。 　電子保存を行う際に、オリジナル画像さえ保存しておけば、診断に使用した３D画像は消去してしまっても構わないか。 　3D 画像作成時のパラメータは保存されていないため、診断の際に生成した３D画像を完全に再現することが難しい状況である。

A　オリジナル画像から当該画像を生成することが原理的に可能であれば、直接診療に使用した処理画像データを保存しておく必要はありません。しかし、この例では、３D画像作成のパラメータがないと診断に用いた画像を完全に再現することが困難であるということなので、3D 画像を消去することはできません。

シス５章第④条

シQ－11　3D 画像処理を行った場合、処理を行う元となった画像は保存しなければならないか。

A　3D 画像処理を行う元となった画像を、3D を作成することのみに用い、診断に用いないならば保存する必要はありません。診断用に作成した 3D 画像は保存する必要があります。

シス５章第④条

シQ－12　確定保存された画像に関し、診断や患者説明のために一時的に医師が表示方法（濃度の変更、拡大など）のみを修正した場合、この画像を保存する必要があるか。

A　濃度の変更、拡大といった程度の処理ならば、改めて保存する必要はありません。

シス５章第④条

シＱ－１３　検像において、検像前の画像情報、検像後の画像情報のいずれを保存対象とすべきか。

Ａ　「検像」についての確かな定義はないため、ここでは医師の診断や読影のために、診療放射線技師等が画像の確定前に当該画像を確認し、必要に応じて画像の付帯情報の修正や不必要な画像の削除を行うことを指すものとします。保存義務の対象とすべき画像については、検像の後に診断に用いるのであり、検像後の画像を対象とすべきと考えられます。ただし、検像において情報の修正・削除といった行為により、照射記録と検像の後の画像情報が一致しない等のことが生じる場合には、修正履歴を保存しておく等、所定の措置が必要となります。また、これらの行為に対する責任の所在を組織として説明できるようにしておく必要があります。

7．情報管理（管理・持出し・破棄等）

シス７章第⑬条

シQ－14　「職員による外部からのアクセスを行う場合は、利用するPC等の端末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の導入を検討するなどの対応が求められる。」とあるが、どのような留意事項があるか。

Ａ　職員による外部からのアクセスで問題になることは、利用するＰＣや通信経路等の状態、及び周囲から盗み見されるおそれがある等、職員の作業環境が管理できないことなどが挙げられます。例えば、ＰＣにキーボードロガーのような不正ソフトウェアがインストールされているリスクや、空港や喫茶店等でアクセスすれば周囲の人に覗かれるリスクがあります。

　仮想デスクトップは、不正ソフトウェアの作用を避け、ＰＣ上に情報が残留することを防ぐ目的で使用されます。また、通信経路の安全性を確保するため、ＶＰＮの成立と連動して稼働することが望まれます。運用としては、周囲の環境に十分注意して盗み見を防止するとともに、過去のログイン時間の確認を確実に行うこと等を通じて、不正アクセスの検出に努める必要があります。

シス７章第②条

シQ－15　医療情報システム・サービス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はどのような対応をすべきか。

Ａ　例えば、保守に際して医療情報システム・サービス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、詳細な持出に関する記録や作業記録を残すよう求めてください。また、必要に応じて、医療機関等の監査に応じるよう求めてください。

シス７章第③条

シQ－16　情報機器の持ち出し並びに外部利用をする場合どのような対策をすべきか。

Ａ　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してください。

　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でください。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ってください。

８．利用機器・サービスに対する安全管理措置

シス８章第①項

シＱ－17　情報の破壊及び混同等を防ぐために、どのような対策が挙げられるか。

Ａ　不正ソフトウェア又は不具合等によるソフトウェアの不適切な動作により、電子的に保存された診療録等の情報が破壊されるおそれがあります。このため、不正ソフトウェアによる情報の破壊及び混同等を防ぐためには、不正ソフトウェアによるこれらの情報へのアクセス防止対策を講じることが求められます。

また、医療情報を取り扱うソフトウェアが改ざんされていないこと、及び仕様のとおりに動作していることを、適宜、確認しなければなりません。

さらに、保存されている情報が、改ざんされていない情報であることを確認できる仕組みを設けることが望ましいです。

シス８章第③項

シＱ－18　不正ソフトウェア対策等が大変なので、外部と遮断した環境を設定する方が望ましいのか。

Ａ　不正ソフトウェア混入等の脅威であり、しっかりとした対応が必要です。ただし、サイバー攻撃が巧妙化する中で、外部と遮断した環境とするだけで不正ソフトウェアの侵入を完全に防ぐことはできません。例えば、職員が不用意に USB ポートなどを利用する場合等でも、不正ソフトウェアが混入することがあります。よって、外部と遮断されている環境であっても、不正ソフトウェア対策ソフトの導入、ぜい弱性の対策を行ったソフトウェアの利用等の対策が必要です。

また、外部と遮断することによって、不正ソフトウェア混入のリスクを低減できることは事実ですが、一方で医療情報の有効な利用を図るために、外部との接続を行うことも広く行われるようになっています。この場合でも、効果的な対策を行うことで、リスクを許容範囲に収めることが可能です。

なお、不正ソフトウェア対策ソフトやぜい弱性の対策等については、外部との接続を断つことによって、最新のソフトウェア検知パターンファイルの取得、対策ソフトウェアの緊急アップデート等を、可搬記憶媒体を介して手作業により行うことになるため、作業が遅れたり、可搬記憶媒体が不正ソフトウェアの混入源となったりするリスクがあります。一方で、外部との接続を遮断しつつ、管理者が安全な形で外部から取得した最新の内部サーバから配信するという手段もありますので、利便性とリスクを踏まえて対応することになります。

また端末やサーバ装置の活動を監視し、不正プログラム等の検知や対処を行う EDR（Endpoint Detection And Response）ソフトウェア等の利用や、主体の操作に対する常時アクセス判断・許可アーキテクチャ（ゼロトラストアーキテクチャ、ゼロトラストセキュリティ等）を用いて内部ネットワーク、外部ネットワーク問わずに対策を講じることも有効な手段として挙げられています。

シス８章第⑥項

シQ－19　医療等分野における IoT 機器に対する安全対策を行う上で、どのような留意事項があるか。

A　近年、様々なモノがネットワークに繋がることで新たなサービス等を実現する「IoT（Internet of Things）」が普及しつつあり、医療等分野での活用も進んでいます。具体的には、医療機関等の内外で用いられる医療機器やバイタルを測定するウェアラブル端末等から患者のデータを収集し、医師の診療支援や経過観察等に活用することや、医療機関等内における職員の位置情報や動線を分析し、病床や人員の配置等を改善すること等が行われています。

このような仕組みやサービスにより、患者の状態をリアルタイムで捕捉できるようになる等、IoT の導入は医療機関等と患者の双方に利益をもたらす可能性があります。ただし、情報セキュリティの観点から、これまで想定されなかったリスクが顕在化するおそれもあります。

IoT 機器により医療情報を取り扱う場合は、医療機器か非医療機器かを問わず、製造販売業者からの情報提供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必要があります。

特に、ウェアラブル端末や在宅設置の IoT 機器を患者等へ貸し出す場合には、機器によって、セキュリティが十分に確保されないおそれがあります。そこで、ウェアラブル端末や在宅設置の機器を貸し出す際は、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事前に患者等へ説明し、同意を得ることが必要です。また、IoT 機器に異常や不都合が発生した場合の問合せ方法等について、患者等に説明する必要があります。

IoT 機器には、機器やサービスの導入後に脆弱性が発見されることがありますので、サービスへの提供に支障が生じないよう適切な時期・方法により対策を講じる必要があります。脆弱性に関しては、IoT 機器が用いる通信規格（例:Bluetooth、NFC 等）の脆弱性についても、併せて対応することが望まれます。

また、IoT の活用状況によって、大量の IoT 機器が同時に接続している環境が想定されますが、この場合、機器の接続状況や異常の発生を正確に把握することが難しいとされます。IoT 機器を含むシステムについて単独でそれぞれの状態を把握できることが望まれますが、機器・システムの中には、大量のログを管理したり、ログの暗号化を行う等の対策を講じることが難しい場合があります。この場合、IoT 機器に関連する他のシステムに監視装置を設置する等、システムやサービス全体での対策が検討することが求められます。

このほか、IoT 機器のリスクとして、使用を終えた又は停止した機器をネットワークに接続した状態のままにしておくと、利用者さえ気付かない間に当該機器が不正に接続される場合がある。さらに、機器の利用状況に関する情報を収集し、不正に利用者を特定される等のリスクも想定されます。

IoT の更なる普及によって、活用方法の多様化や安全性に対する脅威やその対策に係る技術的変化が進み、医療等分野のセキュリティに大きな影響を及ぼす可能性があります。医療機関等においても、今後の動向に注意を払う必要があります。

シス８章第⑧条、第⑨条、企９章第⑥条

シQ－20　「８．５　医療機関等が管理する以外の機器情報機器の利用に対する対策」について、適切な技術的対策や運用による対策はどのようなものがあるか。特に BYOD を行う場合に、どのような安全対策が必要か。

Ａ　下記の対策等が挙げられます。

療機関等が管理しているもの以外の機器情報機器の利用、特に BYOD を行う場合における技術的対策としては、職員のモバイル端末で、他のアプリケーション等からの影響を遮断しつつ、仮想デスクトップのような技術を活用して端末内で医療情報を取り扱うことを制限し、さらに個人でその設定を変更できないようにすること等が考えられます。この場合、OS レベルで業務利用領域（仮想デスクトップ）と個人利用領域を切り分け、管理領域を分離する必要があります。また、サービスや製品によっては十分な安全性が確保されない場合があるため、十分な知見を有する者が判断する必要があります。

さらに、上記の対策に加え、モバイルデバイスマネジメント（MDM）やモバイルアプリケーションマネジメント（MAM）等を施すことで、医療機関等が所有し、管理する端末と同等の安全性を確保するための、セキュリティ対策の徹底を図ることが期待されます。

また、運用による対策として、運用管理規程によって利用者による OS の設定変更（例えば、「設定」用のアプリケーションにより、医療情報システムへの接続に使用するアプリケーションに対して、他のアプリケーションが自動的にアクセスできるようにする等）を禁止し、かつ安全性の確認できないアプリケーションがモバイル端末にインストールされていないことを、管理者が定期的に確認すること等が想定されます。BYOD を行うに当たって、運用管理規程に記載すべき事項の例を下記に示します。

【BYOD に係る運用管理規程への記載事項（例）】

BYOD を認める場合、管理者は下記を遵守すること。

- 利用者に対し、端末や OS 等に応じて推奨されている適切な方法により、アプリケーションをインストールするよう指導すること。
- アプリケーション等の脆弱性に関する情報を収集し、利用者が脆弱性の明らかになったアプリケーションを使用していないか、定期的に確認すること。

シス８章第⑥条

シQ－21　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にはどのような方法あるか。

Ａ　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してください。

９．ソフトウェア・サービスに対する要求事項

シス９章第③条、企１６章第⑧条

シQ－22　紙媒体等をスキャナ等で電子化保存する場合は、どの程度の解像度であればいいか。

Ａ　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してください。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す。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ます。

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）」（※）を参考にしてください。

※　http://www.radiology.jp/content/files/20150417.pdf

このほか心電図等の波形情報やポ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、その点に十分配慮してください。

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ソフトウェアに困らない形式で保存してください。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ります。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してください。

10. システム・サービス事業者による保守対応等に対する安全管理措置

シス１０章第④条

シQ－23　医療情報システム・サービス事業者による保守対応が行われた場合に、診療録にアクセスした証跡を確認する方法はどのようなものがあるか。

A　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で表示し、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てください。

保守作業は、原則、医療機関等の関係者の立会いの下で行わせてください。また詳細なオペレーション記録を保守操作ログとして記録してください。

シス１０章第④条、企７章③条

シQ－24　医療情報システム・サービス事業者と保守契約を締結する際に、情報流出を防ぐためにどのような対応をすべきか。

A　保守を行う医療情報システム・サービス事業者と保守要員者との間で守秘義務契約があることを求めてください。

シス１０章第⑤

シQ－25　保守要員が外部機器を持ち込む場合、何を確認すべきか。

A　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混入していないことを確認してください。

11．システム運用管理（通常時・非常時等）

シス１１．１章

シQ－26　「１１．１　通常時における運用対策表１１－１　平常通常時に対応すべき技術的対応の例の広域災害対策（遠隔地バックアップ等）とあるが」とあるが、「遠隔地」の定義はあるのか。

Ａ　具体的な定義はありませんが、当該医療機関等が地震等の大災害に見舞われた場合でも、それらの被害を受けず、安全に保存できると考えられる地域と考えられます。

シス１１．１章、企１５章第④

シQ－27　システムが停止した場合の診療継続に備え、見読性を確保するために、医療情報システムにどのような対策を講じるべきか。

Ａ　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してください。

　また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ができるように、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してください。

シス１１．１章、企１５章第④条

シQ－28　大規模災害の発生により、サーバ等が使用できなくなった場合に備えてバックアップ体制はどのように構築すべきか。

Ａ　大規模火災等の災害対策として、遠隔地のデータバックアップを使用した見読機能を確保する必要があります。電子保存記録のバックアップを遠隔地に保存するとともに、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してください。

シス１１．１章、企１５章第④条

シQ－29　非常時における利用に備えて、診療録等をどのように保存すべきか。

Ａ　非常時に必要になることが予測される診療録等の見読性の確保するため、非常時に必要になる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してください。

　またその分量等ですが、各医療機関等の機能により判断すべきですが、診療録等の参照が迅速に行えないことで、患者の生命や身体に重大な影響を及ぼすおそれがあることが想定されるものが対象となります。例えば、これから手術を行う方や入院されている方の診療録等が想定されます。通常１週間程度のデータ、あるいは前回の診療データも目安になります。

シス１１．２章

シQ－30　障害等によるデータ保存時の不整合に備えて、どのような対応をすればいいか。

Ａ　ネットワークを通じて外部に保存する場合、診療録等を転送している途中でシステムが停止したり、ネットワークに障害が発生することなどにより、正しいデータが外部の委託先に保存されないことも起こり得ます。その際は、再度、外部保存を委託する医療機関等からデータを転送する必要が生じる場合があります。

　そのため、委託する医療機関等は、医療機関等内部のデータを消去する等の場合には、外部保存を受託する事業者において、当該データが保存されたことを確認してから行う必要があります。

12. 物理的安全管理措置

シス１２章第①条

シQ－31　不適切な保管・取扱いによる情報の滅失、破壊を防止するために、どのような対応が考えられるか。

A　電子的な情報を保存している媒体が不適切に保管されている、あるいは情報を保存している機器が不適切な取扱いを受けているために情報が滅失してしまうか、破壊されてしまうことがあります。このようなことが起こらないように、情報が保存されている媒体及び機器の適切な保管・取扱いが行われるように、技術面及び運用面での対策を施さなければなりません。

使用する記録媒体や記録機器の環境条件を把握し、電子的な情報を保存している媒体や機器が置かれているサーバ室等の温度、湿度等の環境を適切に保持する必要があります。また、サーバ室等への入室は、許可された者以外が行うことができないような対策を施す必要があります。

また、万一、滅失であるか改ざん又は破壊であるかを問わず、情報が失われるような場合に備えて、定期的に診療録等の情報のバックアップを作成し、そのバックアップを履歴とともに管理し、復元できる仕組みを備える必要があります。この際に、バックアップから情報を復元する際の手順と、復元した情報を診療に用い、保存義務を満たす情報とする際の手順を明確にしておくことが望ましいです。

シス１２章第②条

シQ－32　診療録等のデータを保存するサーバ等を保管する区画において、不正な行動による破壊の防止するために、どのような方法があるか。

A　診療録等のデータを保存するサーバや記録媒体、記録機器を保管する区画において、不正な行動による破壊等を防止するために、サーバ等は、許可された者しか入ることができない区画に保管するとともに、サーバ室等には、許可された者以外が入室できないよう、施錠等の物理的な対策を施してください。

また、その部屋の入退室の履歴を残し、保管及び取扱いに関する作業履歴と関連付けて保存してください。さらに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職員の行動を管理してください。

シス１２章第④条

シQ－33　診療録等のデータのバックアップの管理や方法に関して、どのような留意事項があるか。

A　診療録等のデータのバックアップについては、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てください。

　また、障害などに備えて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ってください。

シス１２章第⑤条

シQ－34　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を防止するために、どのような対応が考えられるか。

A　記録媒体、記録機器の劣化による読み取り不能又は不完全な読み取りにより、電子的に保存されている診療録等の情報が滅失してしまうか、破壊されてしまうことがあります。これを防止するために、記録媒体や記録機器の劣化特性を考慮して、劣化が起こる前に新たな記録媒体や記録機器に複写する必要があります。

シス１２章第⑥条

シQ－35　医療情報の入力や閲覧に際して、情報の漏えいを防ぐために具体的にどのような対策をすべきか。

A　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ってください。

　また　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）を実施してください。

13. ネットワークに関する安全管理措置

シス１３章第②条

シQ－36　専用線以外の回線サービスを利用する場合、どのような留意事項があるか。

A　過去には、重要な情報システムの利用に際しては、専用線などを用いることが多かったのですが、現在のブロードバンドの普及状況やセキュリティ技術の向上から、公衆回線等を活用した回線サービスを用いて医療情報システムで利用するネットワークを構築することで導入コストを削減したり、地域医療情報連携の仕組みを構築したりする等、その利用範囲が拡大していくことが考えられます。この場合、セキュアなネットワークを用いて、安全な通信を行うことが求められます。

その際、OSI 階層モデルを基本としたネットワーク経路上のセキュリティの詳細については「「医療情報システムの安全管理に関するガイドライン」の実装事例に関する報告書」（保健・医療・福祉情報セキュアネットワーク基盤普及促進コンソーシアム：HEASNET；平成 19 年３月）が参考になります。

※　OSI 階層モデル（Open Systems Interconnection）：開放型システム間相互接続のことで、異種間接続を実現する国際標準のプロトコル。

第7層	アプリケーション層	FTPやMail等のサービスをユーザに提供
第6層	プレゼンテーション層	データを人に分かる形式、通信に適した形式に変換
第5層	セッション層	データ経路の確立と開放に関係する層
第4層	トランスポート層	データを確実に届ける為に規定されている層
第3層	ネットワーク層	アドレス管理と経路の選択ための層
第2層	データリンク層	物理的通信経路の確立するために規定されている層
第1層	物理層	ビットデータを電気的、物理的に変換。機器の形状・特性を規定している層

表　OSI 階層モデル

接続先や経路先を管理することによりセキュアなネットワークの構築が期待されますが、OSI 階層に応じてこのリスクとそれを踏まえた対策が異なってきます。

例えば、SSL-VPN を用いる場合、５階層目の「セッション層」といわれる部分で経路の暗号化手続きがなされるため、正しく経路が暗号化されれば問題ありませんが、経路を暗号化する過程で盗聴され、適切でない経路を構築されるリスクが内在します。また、偽サーバへの対策が不十分なものが多いという指摘があります。一方、IPsec を用いる場合は、２階層目の「データリンク層」又は３階層目の「ネットワーク層」といわれる部分で経路の暗号化手続きがなされるため、SSL-VPN よりは危険度が低くなっています。そのため、SSL-VPN を使用する場合には、適切な手法の選択及び必要な対策を行う必要があります。ただし、この場合でも、経路を暗号化するための暗号鍵の取り交わしに IKE（Internet Key Exchange）といわれる標準的手順を組み合わせる等により、確実にその安全性を確保する必要があります。

また、IPsec を用いた VPN 接続等によるセキュリティの担保を行わず、インターネット等のオープンなネットワークを介し、他の医療機関や患者等が医療情報システムへ接続する場合（下図）は、少なくとも TLS による暗号化を用いた HTTPS の利用が求められます。

図　オープンネットワークで接続されている場合

しかし、昨今 TLS においてプロトコルやソフトウェアの脆弱性を突いた攻撃の報告が相次いでおり、TLS を適切に利用しなければ接続に HTTPS を用いても、必ずしも安全性を確保することができません。TLS を利用する上での適切な設定方法は、CRYPTREC が作成し独立行政法人情報処理推進機構によって発行された「TLS 暗号設定ガイドライン」にて指針が示されている。「TLS 暗号設定ガイドライン」にて示される設定をすることで、TLS への既知の攻撃から、一定の安全性を確保することができます。なお現時点で最新の「TLS 暗号設定ガイドライン 3.0.1 版」では 3 段階の設定基準が定められているところ、医療情報システムで利用する場合は、そのうち最も安全性水準の高い「高セキュリティ型」の設定を反映することで TLS への攻撃リスクを低減する必要があります。「高セキュリティ型」の設定の一つとして、利用可能なプロトコルバージョンを TLS1.3 に設定するものの、システムやサービス等の対応上、これによることが難しい場合には、TLS1.2 以上に限定して設定する必要があります。そのため、サーバ・クライアントともに TLS1.2 以上をサポートしていることが必須となることに注意することが必要です（TLS1.2、TLS1.3 のいずれかの利用に限定している場合には、それぞれのプロトコルをサポートしていることが求められる）。加えて、オープンなネットワークの場合、不特定の端末から接続されるリスクがあるため、対策の一つとして TLS クライアント認証を行う必要があります。

さらに、オープンネットワークで接続する場合には、IPsec や TLS によるセッションが安全でも、他セッションが同居できるため、ネットワークに接続している機器やシステムが標的型メール等の攻撃にさらされるリスクがある。仮に、このような攻撃によってネットワークに接続する端末等に不正ソフトウェアが混入し、遠隔操作が可能になると、IPsec や TLS1.2 以上によるセッションへの正規のアクセスが発生する可能性があります。

IPsec や TLS による接続は、適切な経路設定を行うことで、セッション間の回り込みを回避することが可能である。一般社団法人保健医療福祉情報安全管理適合性評価協会（HISPRO）が公開している「レセプト・オンライン請求用チェックシート項目集」（※）が参考になります。

※　「レセプト・オンライン請求用チェックシート項目集」
https://hispro.or.jp/open/pdf/2009090nRece%20koumoku.pdf

このように、オープンなネットワーク接続を利用する場合、様々なセキュリティ技術が存在し、内在するリスクも用いる技術によって異なることから、利用する医療機関等においては導入時において十分な検討を行い、リスクの受容範囲を見定める必要があります。なお、日頃からセキュリティインシデントの報道や事業者からの情報提供等を通じて、TLS 等の脆弱性リスクについて注意、認識しておくことが求められます。また、多くの場合、ネットワーク導入時に事業者等に委託をすることになるが、その際、リスクの説明を求め、理解しておくことも必要です。

なお、オープンネットワークを通じて外部から情報を取り込む際に、取り込む情報の安全性を確認する必要があり、そのため例えば取り込むデータ等についての無害化を図るなど、標的型攻撃等によるリスクを減少する対応を図ることが求められます。

また、外部との接続については、医療機関等がクラウドサービスを利用し、医療情報システム・サービス事業者等のサーバからデータを取得する場合も、同様のリスクを想定する必要があります。特にクラウドサービスの場合には、利用するサービスによって、取り扱う情報の機密性等が異なるため、事業者によってセキュリティの水準が異なることがあります。したがって、医療情報を取り扱う場合には、利用する各クラウドサービスにおけるリスク等を鑑みた対応をとることが求められます。必要に応じて、ネットワークの論理制御（例えばメールシステムと医療情報システムの情報が混在しないようにすること等）や、これを踏まえた情報交換のルールに基づく管理を行うことが望まれます。

シス１３章第②条

シQ－37　医療機関等におけるネットワークに対する不正アクセスへの対策を講じる際、どのような留意事項があるか。

A　クラッカーや不正ソフトウェアによる攻撃から情報を保護するための一つの手段として、ファイアウォールの導入がありますが、これに加えて、不正な攻撃を検知するシステムファイアウォールは、「パケットフィルタリング」、「アプリケーションゲートウェイ」、「ステートフルインスペクション」等の各種方式があります。また、その設定によっても動作機能が異なるので、単にファイアウォールを導入すれば安心というものではありません。単純な「パケットフィルタリング」で十分と考えるのではなく、それ以外の手法も組み合わせて、外部からの攻撃に対処することが望まれます。医療情報システム安全管理責任者は、その方式が何をどのように守っているかを認識する必要があります。このことは、医療機関等の外部から医療機関等の医療情報システムに接続する場合も同様です（「７．情報管理（管理・持出し・破棄等）」参照）。

部外者により物理的にネットワークに接続できる可能性がある場合、不正なコンピュータを接続し、不正ソフトウェアが混入したり、サーバやネットワーク機器に対して攻撃（サービス不能攻撃 DoS：Denial of Service 等）を行ったりすることや、不正にネットワーク上のデータを傍受したり改ざんしたりすることが可能となります。

不正なコンピュータの物理的な接続に対する対策を行う場合、一般的に MAC アドレスを用いてコンピュータを識別する場合が多いが、MAC アドレスは改ざん可能なため、そのことを念頭に置いた上で対策を行う必要です。不正アクセスの防止は、いかにアクセス先の識別を確実に実施するかが重要であり、特に、“なりすまし”の防止は確実に行う必要があります。無線 LAN のアクセスポイントを複数設置して運用する場合等、マネジメントの複雑さが増し、侵入の危険が高まるような設置をする場合には、一層留意が必要であります。

また、ネットワーク上を流れる情報の盗聴を防止するために、暗号化等による“情報漏えい”への対策も必要となります。

シス１３章第⑤条

シQ－38　「ルータ等のネットワーク機器について、安全性が確認できる機器を利用すること。」とあるが、どのようなものが安全性が確認できる機器として考えられるのか。

A　安全性が確認できる機器としては、ISO/IEC 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などが挙げられますが、この規格で認証された機器を導入することは必須ではありません。このガイドラインが求める安全対策のための要求事項を、導入を検討している機器ベンダに示して、回答を求めてください。満足する回答が得られれば、安全性が確認された機器と判断していただいて結構です。

また、「ルータ等のネットワーク機器の機能をソフトウェアで実現しているもの」については、その当該ソフトウェアに対して安全性が確認できる必要があります。「ルータ等のネットワーク機器」を「当該ソフトウェア」に読み替えてご対応ください。

シス１３章第⑥条

シQ－39　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）とは、具体的にどのような事象を指すものか。

A　例えば、下図のように、医療情報連携ネットワークの Web サーバへのアクセス等のために、医療機関等の専用端末がソフトウェア型の IPsec や TLS1.2 以上によりオープンネットワークに接続している場合、攻撃者は開放された当該端末のポートを標的として、何らかの攻撃（典型的には標的型メール攻撃等）を試みることが想定されます。

この攻撃により、当該専用端末が遠隔操作型のマルウェア等に感染すると、攻撃者は本人になりすまして医療情報連携ネットワークの Web サーバとのセッションの立上げを試みることが可能になります。セッションの立上げに成功すると、外観上は正規の権限によるアクセスが発生することになり、IPsec や TLS1.2 以上により適切に暗号化していても、攻撃者は医療情報連携ネットワークの Web サーバにアクセスできるようになります。

ガイドラインでは、この一連の攻撃を「セッション間の回り込み」と称しています。対策として、適切な経路設定を実施することに加え、医療情報連携ネットワークへのアクセスに当たって、二要素認証により利用者の識別・認証を行うことで、遠隔操作を防ぐこと等が考えられます。

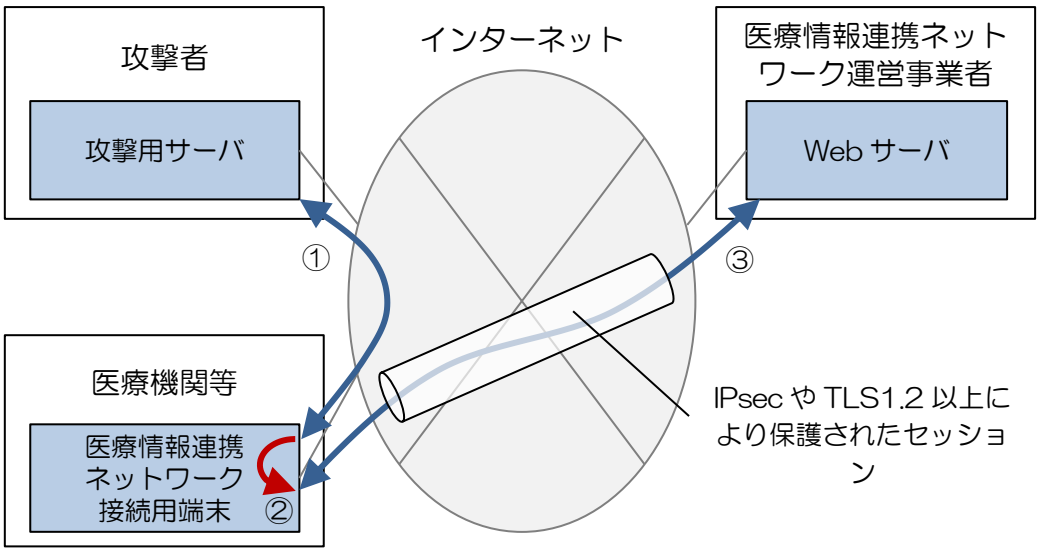

図　セッション間の回り込み（イメージ）

シス１３章第⑥条

シQ−40	「１３．ネットワークに関する安全管理措置 」⑥に「 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、使用する場合には適切な手法の選択及び必要な対策を行うこと」とあるが、具体的にはどのように利用するのか。

A　安全管理ガイドラインでは、偽サーバへの対策が不十分なものが多いため、医療情報システムでは原則として使用するべきではないとしています。しかし SSL-VPN についてもクライアント型と呼ばれるものについては、「専用のクライアントソフトがインストールされた端末との間でのみアクセスする。つまり、誤って偽サーバに接続することがなく、また内部サーバにアクセスできる端末も厳格に制限できるため、端末に IPsec-VPN ソフトをインストールして構成するモバイル型の IPsec-VPN に近い形での運用形態」が可能とされています（「TLS 暗号設定ガイドライン 3.01 版」IPA）。

従って、SSL-VPN を利用する場合には、１３．ネットワークに関する安全管理措置⑥に記載されているクライアント証明書を利用した TLS クライアント認証や「高セキュリティ型」に準じた適切な設定を行った上で例外的にクライアント型の SSL-VPN などの利用によることが考えられます。

シス１３章第⑬条

シQ－41　無線 LAN の利用において、どのような留意事項があるか。

A　無線 LAN は、看護師等が情報端末を利用し患者のベッドサイドで作業する場合等において利便性が高い反面、通信の遮断等も起こる危惧があります。そのため、情報の可用性が阻害されないように留意する必要があります。また、無線電波により重大な影響を被るおそれのある機器等の周辺での利用には注意が必要です。

無線 LAN の運用に関しては、総務省発行の「一般利用者が安心して無線 LAN を利用するために」や「企業等が安心して無線 LAN を導入・運用するために」を参考に対策を実施する必要があります。

シス１３章第⑪条

シQ－42　「なりすまし」に対しては、具体的にどのような対応をとればいいか。

A　ネットワークを通じて情報を伝送する場合、情報を送ろうとする医療機関等は、送信先の機関が確かに意図した相手であるかを確認しなければなりません。逆に、情報の受け手となる送信先の機関は、その情報の送信元の医療機関等が確かに通信しようとする相手なのか、また、送られてきた情報が確かに送信元の医療機関等の情報であるかを確認する必要があります。これは、ネットワークが非対面による情報伝達手段であることに起因するものです。

そのため、例えば通信の起点と終点の機関を適切に識別するために、公開鍵方式や共有鍵方式等の確立された認証の仕組みを用いてネットワークに入る前と出た後で相互に認証する等の対応を取ることが考えられます。また、改ざん防止と併せて、送信元が正当な送信元であることを確認するために、医療情報等に対して電子署名を組み合わせることも考えられます。

シス１３章第⑪条

シQ－43　「盗聴」に対しては、具体的にどのような対応をとればいいか。

A　ネットワークを通じて情報を伝送する場合には、盗聴に最も留意しなくてはなりません。盗聴は様々な局面で発生します。例えば、何者かがネットワークの伝送途中で仮想的な迂回路を形成して情報を盗み取ったり、ネットワーク機器に物理的な機材を取り付けて盗み取ったりする等、必ずしも医療機関等の責任といえない明らかな犯罪行為も想定されます。一方、ネットワーク機材の不適切な設定による意図しない情報漏えいや誤送信等、医療機関等が責任を負うべき事例も考えられます。

このように様々な事例が考えられる中で、医療機関等においては、万一、伝送途中で情報が盗み取られたり、意図しない情報漏えいや誤送信等が発生した場合でも、医療情報を保護するために適切な処置を取る必要があります。その一つの方法として医療情報の暗号化が考えられます。ここでいう暗号化とは、先に例示した情報そのものの暗号化（オブジェクト・セキュリティ）のことを指しています。

どのような暗号化を施すか、また、どのタイミングで暗号化を施すかについては伝送しようとする情報の機密性や医療機関等で構築している医療情報システムの運用方法によって異なるため、ガイドラインにおいて一概に規定することは困難ですが、少なくとも情報を伝送し、医療機関等の設備から情報が送出される段階においては暗号化されていることが望まれます。

この盗聴防止については、例えばリモートログインによる保守を実施する時も同様です。その場合、医療機関等は上記のような留意点について、保守作業を受託する事業者等に確認し、監督する責任を負うことになります。

シス１３章第⑪条

シQ－44　「改ざん」への対応として、どのような留意事項があるか。

A　ネットワークを通じて情報を伝送する場合には、正当な内容を送信先に伝えなければなりません。情報を暗号化して伝送する場合には改ざんの危険性は軽減するが、通信経路上の障害等により意図的・非意図的要因に係わらず、データが改変されてしまう可能性があることは認識しておく必要があります。また、ネットワークの構成によっては、ネットワーク自体に情報の秘匿化機能が不十分な場合もあるので、改ざんに対する対処は確実に実施しておく必要があります。

なお、改ざんを検知するための方法としては、例えば、電子署名を用いる等が想定されます。

シス１３章第⑪条

シQ－45　ネットワークを介して送信元と相手先の当事者間でやりとりする情報に対する暗号化等のセキュリティ対策を実施するためにはどのような技術があるか

A　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してください。

システム１３章第⑪条

システムＱ－46　許可された者以外の無線 LAN の利用を防止するためにはどのような対策が必要か。

Ａ　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してください。

システム１３章第⑬条

システムＱ－47　医療機関等におけるローカル５Ｇの利用について、具体的な事例等はあるか。

Ａ　医療分野でのローカル5G の利用については、現時点では実証段階のケースが多く、具体的な事例は多くはありません。今後具体的な導入実態を踏まえて導入の検討を図ることが望まれます。

14. 認証・認可に関する安全管理措置

シス１４章第①条

シQ－48　認証方法が安全な利用者の識別・認証方法を選定する際、どのような留意事項があるか。

A　利用者の識別・認証方法を選定する際には、認証の安全税を考慮する必要がありますが、その際に、認証強度が高い利用者の識別・認証を採用することが求められます。

これまで使われてきた ID・パスワードの組み合わせは、これまで広く用いられてきた方法ですが、ID・パスワードによる認証ではその運用によっては、リスクが大きくなります。認証強度を維持するためには、交付時の初期パスワードの利用者本人による変更や定期的なパスワード変更を義務付ける等、システムの実装や運用を工夫し、必ず本人しか知り得ない状態を保つよう対策を行う必要があります。

ただし、このような対策を徹底することは一般に困難であると考えられるため、その実現可能性の観点からは必ずしも推奨されません。

認証に用いる手段としては、ID・パスワードの組み合わせのような利用者の「記憶」によるもの、指紋や静脈、虹彩のような利用者の生体的特徴を利用した「生体情報」（バイオメトリクス）によるもの、IC カードのような「物理媒体」（セキュリティ・デバイス）によるものが一般的です。認証におけるセキュリティ強度を考えた場合、これらのいずれの手段であっても、単独で用いた場合に十分な認証強度を保つことは一般には困難です。そこで、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て認証を行う方式（二要素認証）を採用することが望ましいとされます。

なお、認証に際して、二段階で認証を行う二段階認証と呼ばれる方法がありますが、この場合には利用される認証要素が同一となることもあるため、実質的にリスク低下につながらないこともあります。そのため、二段階認証を選択するだけでは二要素認証の要求を満たさないと考えるべきでしょう。

また、シングルサインオン方式を用いて、一度の認証により複数のアプリケーションを操作する場合であっても、最初のログイン時に二要素認証を行っていれば、セキュリティは確保されていると考えられます。ただし、ログイン状態のまま長時間放置したり、特定の端末でログインしただけで院内の複数の端末にログイン可能となるような運用は認められません。また利用者が端末から長時間離席する場合には、正当な利用者以外の者による入力を防止するため、クリアスクリーン等の防止策を講じるべきでしょう。

シス１４章第③条

シQ－49　利用者の識別・認証に IC カード等のセキュリティ・デバイスを配布する場合、どのような留意事項があるか。

A　利用者の識別、認証、署名等を目的として、IC カード等のセキュリティ・デバイスに個人識別符号のうち指紋等の生体情報に関するデータや暗号化鍵、電子証明書等を格納して配布する場合は、これらのセキュリティ・デバイスが誤って本人以外の第三者の手に渡ることのないよう対策を講じる必要があります。また、万一そのセキュリティ・デバイスが第三者によって不正に入手された場合でも、簡単に利用されないようにすることが重要です。

したがって、利用者の識別、認証、署名等が、これらセキュリティ・デバイス単独で可能となるような運用はリスクが大きいため、必ず利用者本人しか知り得ない情報との組み合わせによってのみ有効になるようなメカニズム、運用方法を採用しなければなりません。

また、IC カードの破損等、本人の識別情報が利用できない時を想定し、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しておく必要があります。その際、安全管理のレベルを安易に下げることがないよう、本人確認を十分に行った上で代替手段の使用を許し、さらにログ等を残して、後日再発行された本人の正規の識別情報により、上記緊急時の操作のログ等の確認操作をすることが望まれます。

シス１４章第⑥条

シQ－50　「類推されやすいパスワードを使用させないよう、設定可能なパスワードに制限を設けること」とあるが、類推を防ぐために定期的な変更を求めることは有効か。 また、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、導入または更新する場合、原則として二要素認証を採用する趣旨は何か。

A　医療情報システムにおいては、医療情報を預かる医療従事者による職務上の安全確保という観点から、推定困難なパスワードを設定することが求められます。

パスワードの要件による安全性については、日々研究が進められています。近年では、定期的な変更を行うことで利用者が推定可能なパスワードを設定することで、むしろ脆弱になってしまうという報告もあります。

米国国立標準技術研究所（以下、「NIST」）から 2017 年６月に公表された「SP 800-63-3（Digital Identity Guidelines（デジタルアイデンティに関するガイドライン））第３版」においては、パスワードの定期的な変更を強制することにより、「類推されやすいパスワードを使用しない」という要件を満たさないことになるリスクが指摘されています。

他方、「政府機関等の対策基準策定のためのガイドライン（平成 30 年度版）（内閣官房 内閣サイバーセキュリティセンター（以下「NISC」））」においては、利用者にパスワードの定期的な変更を求めるか否かは、その効果と逆効果を勘案して判断する必要がある旨を指摘しています。例えば「オフライン攻撃を許す旧式の認証プロトコルが用いられている場合であって、13 文字といった十分に長いパスワードを設定できない旧式の情報システムを用いている場合には、パスワードの定期的な変更は必要である。この場合には、オフライン攻撃によってパスワードを復元されるまでにかかる時間を踏まえて、必要な周期での定期的な変更を求める必要がある」としています。

医療情報を取り扱う医療情報システムの性格や構成を鑑みると、原則として、容易に類推できないパスワードを使用しつつ、その定期的な変更を行うことが求められる。ただし、利用するパスワードが 13 文字以上のランダムな設定がなされており、パスワード管理の安全性などが担保されているシステムを用いている場合には、パスワードの定期的変更は必ずしも求められない（※１）。なお、これらのパスワード変更に関するルールは、ＩＤとパスワードのみによる認証を用いている場合に該当するものです。

なお二要素認証を採用している場合、必ずしもパスワードの定期的な変更は求められない。）。

また、医療情報システムのシステム上の制約等で 13 文字以上の文字列を設定できない又は適切な管理を行うことができない環境においては、推定困難なパスワードを、脆弱にならない形（※２）で定期的に変更させることにより、安全性を担保することができると考えられます。この場合、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のパスワードでもよいとしております。

しかしながら、ID とパスワードによる認証では、安全性の確保に限度があります。前述の報告においても、医療情報のような個人情報へのアクセスは二要素以上の認証を組み合わせる認証方式（二要素認証）とすることが示されています。そのため、できるだけ早く二要素認証を導入することが求められます。本ガイドラインでは、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、導入または更新する場合、原則として二要素認証を採用することを求めています。導入または更新に際して、対象となる製品・サービスがベンダ等から提供されていないなどの理由で二要素認証対応が困難な場合にも、対象となる医療情報システムの利用に供する部屋の入室管理を個人ごとに特定できるようにする等の措置を講じて、全体として二要素認証に相当する安全性の確保を行う必要があります。

（※１）例えば、漏えいしたことのある及び推定可能な脆弱なパスワードを設定できない技術的な制約を課すことや、設定しようとするパスワードの強度が確認できること等の管理が挙げられています。（実装に関係される方は“Digital Identity Guidelines から Authentication and Lifecycle Management”（NIST Special Publication 800-63B ）https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf を参照してください）。

（※２）例えば、以前のパスワードから推定可能なパスワードといった解析のヒントを与えないような形が想定されます。

シス１４章第③条

シQ－51　利用者の識別・認証で二要素認証を採用する際、指紋、虹彩等のバイオメトリクスを利用する場合、どのような留意事項があるか。

Ａ　利用者識別・認証に指紋や虹彩、声紋等のバイオメトリクスを用いる場合の留意点として、その測定精度にも注意を払うことが挙げられます。医療情報システムで一般的に利用可能と思われる各種のバイオメトリクス機器の測定精度は、現状では、１対Ｎ照合（入力された 1 つのサンプルが、登録されている複数のサンプルのどれに一致するか）には十分とはいえないため、１対１照合（入力されたサンプルが、特定の１つのサンプルと一致するか）での利用が妥当であると考えられます。

したがって、バイオメトリクスを用いる場合は、単独での識別・認証を行わず、必ずユーザ ID 等個人を識別できるものと組み合わせて利用するべきです。

また、生体情報を基に認証するに当たって、以下のような生体情報特有の問題があります。

- 事故や疾病等による認証に用いる部位の損失等
- 成長等による認証に用いる部位の変化
- 一卵性の双子の場合における特徴値の近似
- 赤外線写真等による“なりすまし”（IC カード等の偽造に相当）

上記のことを考慮の上、生体情報の特徴を吟味し適切な手法を用いる必要があります。欠損への対処としては異なる手法や異なる部位の生体情報を用いること、なりすましへの対処としては二要素認証（IC カードやパスワードとバイオメトリクスの組み合わせ等）を用いることが求められます。これらのことを踏まえ、実際の採用が想定される二要素認証の方式として、下記の例が挙げられます。

二要素認証の採用例

- ユーザ ID＋パスワード＋指紋認証
- IC カード＋パスワード
- IC カード＋静脈認証等

シス１４章第③項

シQ－52　FIDO 認証（※１）に関して、どのような留意事項があるか。

A　FIDO 認証を使用し、医療情報システムの利用者の識別・認証を行う場合には、求められる当人認証の頑強性として、「Digital Identity Guidelines」（NIST　SP800-63）で定められている AAL（Authentication Assurance Level）の強度：Level２以上の技術を採用することが望ましいです（※２）。

例えば、FIDO―U2F（Universal 2nd Factor）は、２要素認証による技術であるため、安全性が高く、AAL３に位置付けられますが、２要素認証によらない場合には、AAL３を満たさないこともあります。

FIDO 認証のメリットとしては、既存のスマートフォンの機能などを活用することが可能であるため、導入しやすいなどが挙げられます。他方で、デメリットとしてはパスワード認証との併用、利用者の使用デバイスの登録などによる認証フローが複雑になりやすいなどがあります。

（※１）FIDO（Fast IDentity Online）認証とは、オンラインの認証サーバを通じてパスワード不要で利用者を認証する仕組みです。具体的な利用方法は、FIDO 認証対応のスマートフォンで利用者に対する使用デバイスの登録を行い、本人認証を行うなどが挙げられます。なお、FIDO 認証では生体認証機能を利用することでパスワードに代わる認証が行われることが多いとされますが、生体認証に限らず他の方式の技術によることも可能とされています。

（※２）「企画管理編　１３．医療情報システムの利用者に関する認証等及び権限」参照

シス１４章第①条

シQ－53　ネットワーク上からの不正アクセスを防止するためにどのような対策が必要か。

A　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）等を適切に設定してください。

シス１４章第⑥条

シQ－54　パスワードを用いた利用者認証に関して、不正な攻撃への対応としてどのようなことが挙げられるか。

A　不正な攻撃に対応するために、類推されにくいパスワードや辞書攻撃を受けにくいパスワード等が求められます。

例えば以下のような例が挙げられます。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ります。

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。

このうち c.の場合、二要素認証となり、ＩＤ／パスワードのみの認証よりも安全性が高いことから、二要素認証におけるパスワードについては、同項 a.、b.の要件とは異なり、8 文字以上の推定困難な文字列であっても定期的な変更は求めないこととしています。

パスワード長については、原則として英数字、記号を混在させた８文字以上としていますが、例外として二要素認証のもう片方の認証要素を使う際に、ＰＩＮなどが設定されているなどの安全管理が施されている場合には、上記のパスワード長のルールは求めないこととしています。この理由は、IC カードに格納されている電子証明書等の認証要素（知識以外の要素）を使うために設定されている場合のＰＩＮは、ＩＤ／パスワード（知識）におけるＩＤに紐づくものではなく、厳密に言えばパスワードとは異なるためです。このようなケースでは利用者認証全体を勘案すると、ＩＤ／パスワードのほかに、ＩＣカード（所有）や指紋認証（生体）などの知識ではない認証要素、さらに追加の認証要素（知識）を利用するＰＩＮなどが設定されていることになるため、十分な安全性が確保されるものと評価されると考えられます。そのため、このような場合には、英数字、記号を混在させた８文字以上というパスワードの要件は求めないこととしています。具体的には下図の通りなります。

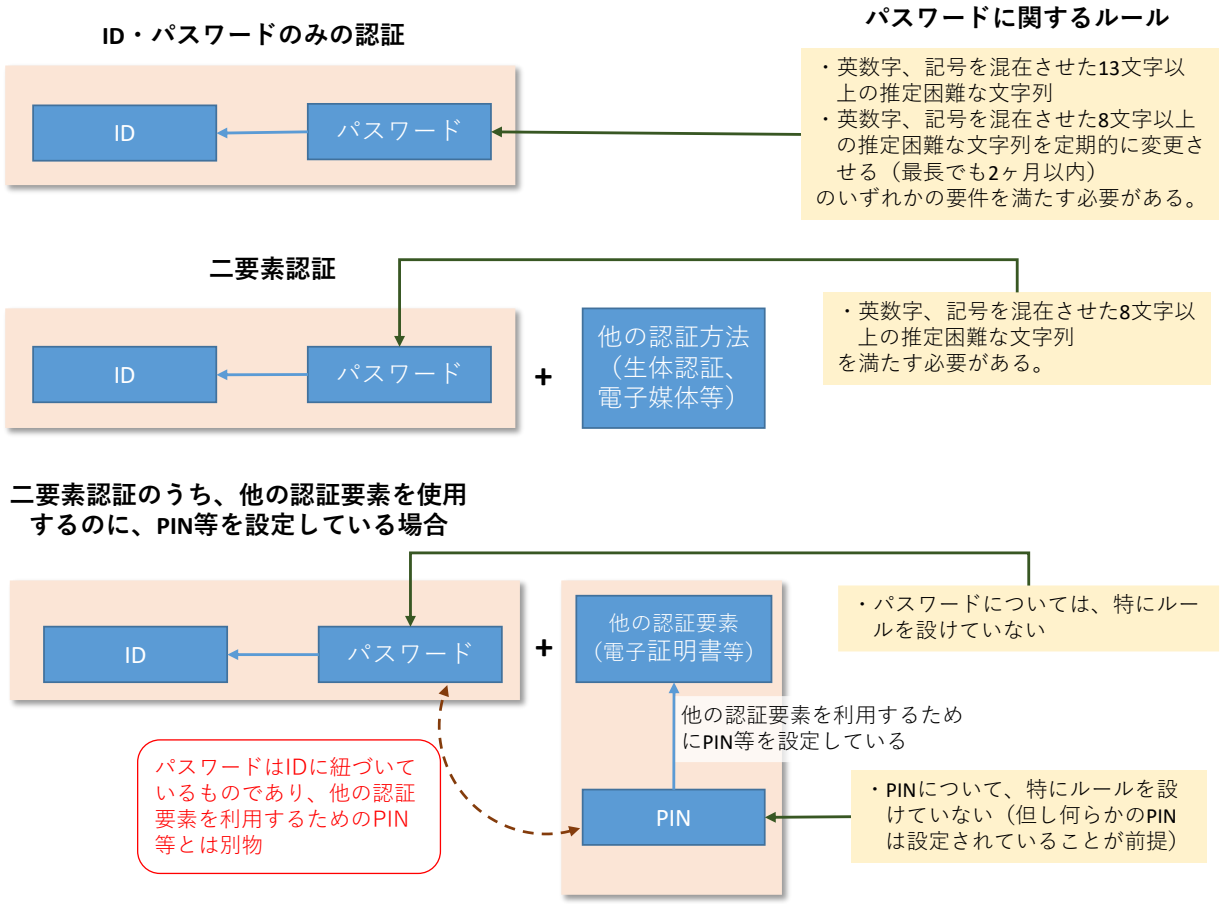

図　パスワードを用いた利用者認証

また不正な攻撃に対して、連続する攻撃を避けるため、次に掲げる対策を実施してください。

- 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
- 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

シス１４章第⑤条、企１５章第⑥条

シＱ－55　認証を伴う情報機器を通じた不正アクセスを防止するためにどのような対策が必要か。

Ａ　まず、情報機器やソフトウェアに関しては、出荷時の初期パスワード、可能であればＩＤも含めて変更することが求められます。そのうえで、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てください。

シス１４章第⑧条

シＱ－56　「虚偽入力、書換え、消去及び混同を防止する」ために、はどのように、どのような対応が求められるのか。

Ａ　保存義務のある文書等の電子保存に際して、電子保存を実施する医療情報システム安全管理責任者は、正当な手続を経ずに、あるいは過失により、電子化した診療情報等が誤入力、書換え・消去及び混同されたりすることを防止する対策を講じる必要があります。また、システムで診療録等の情報の作成、書換え、消去等の作業をする入力者（以下「入力者」という。）、記録の確定（※）を実施する権限を有する確定者（以下「確定者」という。）は、情報の保存を行う前に情報が正しく入力されており、過失による書換え、消去及び混同がないことを確認する義務があります。

※　記録の確定とは、入力者により入力された情報に対して、確定を実施する権限を有する確定者によって入力の完了が確認されることや、検査、測定機器による出力結果の取込みが完了することです。

虚偽入力、書換え、消去及び混同に関しては、入力者等の故意又は過失に起因するものと、使用する機器、ソフトウェアに起因するものの２つに分けることができます。

前者は、例えば、入力者が故意に診療録等の情報を改ざんする場合や、入力ミス等の過失により誤った情報が入力されてしまう場合等が考えられます。

後者は、例えば、入力者は正しく情報を操作しているが、使用している機器やソフトウェアの誤動作やバグ等により、入力者の入力した情報が正しくシステムに保存されない場合等が考えられます。

これらの虚偽入力、書換え、消去及び混同の防止は、機器やソフトウェアにおける技術的な対策だけで防止することが困難なため、運用的な対策も含めて防止策を検討する必要があります。

①　故意又は過失による虚偽入力、書換え、消去及び混同の防止

故意による虚偽入力、書換え、消去及び混同はそもそも違法行為であるが、それを防止するためには、以下が守られなければなりません。

- 情報の入力や記録の確定に係る作業の手順等を運用管理規程に記載すること。
- 情報の入力者、及び入力者と確定者が異なる場合はその両者（以下「入力者及び確定者」という。）が明確で、いつでも確認できること。

- 入力者及び確定者の識別・認証を確実に行うこと。すなわち、なりすまし等が行えないような運用操作環境を整備すること。
- 入力者やシステムを操作できる者の権限に応じてアクセスできる情報を制限すること。
- 入力者及び確定者が行った操作に関して、いつ、誰が、どこで、どの情報に対して、どんな操作を行ったのかが記録され、必要に応じて、操作記録に対して医療機関等が定めた運用管理規程に準拠した適正な利用であることが監査されること。
- 確定された情報は、確定者によって確定操作が実施されたことが医療機関等で定めた運用管理規程に準拠して監査できること。
- 確定され保存された情報は、運用管理規程で定めた保存期間内は履歴を残さないで改変、消去ができないようにすること。
- システムの改造や保守等で診療録等にアクセスされる可能性がある場合には、真正性確保に留意し、6.8 章に記載された手続きに従うこと。

過失による虚偽入力、書換え、消去及び混同は、単純な入力ミス、誤った思い込み、情報の取り違えによって生じます。誤入力等を問題ないレベルにまで低減する技術的方法は存在しないため、入力ミス等は必ず発生するとの認識の下、運用上の対策と技術的対策の両面から誤入力等を防止する対策を講じることが求められます。例えば、情報の確定を行う前に十分に内容の確認を行うことを運用管理規程に定めるとともに十分な教育訓練を行う、あるいは、ヒヤリ・ハット事例に基づき誤操作の発生しやすい箇所を色分け表示する等、操作者に注意喚起を行う技術的対策を施すことが望ましいです。

② 使用する機器、ソフトウェアに起因する虚偽入力、書換え、消去及び混同の防止

使用する機器、ソフトウェアに起因する虚偽入力、書換え、消去及び混同とは、入力者が正当に入力したにも関わらず、利用しているシステム自体に起因する問題により、結果が入力者の意図したものと異なる状況となるリスクを指す。このような状況が発生する原因として下記のケース等が考えられます。

- システムを構成する機器、ソフトウェア自体に問題がある場合（故障、熱暴走、ソフトウェアのバグ、バージョン不整合等）
- 機器、ソフトウェアに問題はないが、正しく設定されていないために所定の機能動作をしない状態になっている場合
- 正当な機器、ソフトウェアが悪意ある第三者により別のものに置き換えられている場合
- 不正ソフトウェアが混入し、データの不正な書換え、消去や、ソフトウェアの誤動作が発生している場合

これらの脅威は、システムの導入時に入念な検証を行うとともに、システムの維持と管理を適切に行うことで防止できると考えられるため、医療機関等においてシステムの品質管理を十分に行う姿勢が重要である。具体的な方策については、「C. 最低限のガイドライン」の記述を参照してください。

シス１４．３章

シQ－57　「作成の責任の所在を明確する」ために、はどのように、どのような対応が求められるのか。

Ａ　電子保存の対象となる情報は、記録を作成するごとに入力者及び確定者が明確になり、作成の責任の所在が明らかになっている必要があります。また、一旦記録された情報を追記・訂正・消去することも日常的に行われるものと考えられるため、追記・訂正・消去するごとに入力者及び確定者が明確になっている必要があります。

医療機関等の規模や管理運営形態により、作成・追記・訂正等の確定者が自明となる場合も考えられます。その場合、確定者が明確になるよう運用方法を定め、運用管理規程等に明記した上で、入力者が作成や追記・訂正・消去した内容について確定者が確定した旨の何らかの記録を残した形で運用を実施する必要があります。電子保存の対象となる情報の入力は、診療行為等の実施者が行うことが原則です。しかし、例えば外科手術時の経過をカルテに記録する際のように、本来の診療行為の実施者である執刀医による入力が物理的に不可能であるため、代行者が入力する場合も想定される。また、医師事務作業補助者が、医師の指示の下で電子カルテに入力をすることも考えられます。このように、診療行為等の実施者でない者が、その者に代わって入力を行う場合は、代行入力に関する規定の策定と、その実施に関して記録を残さなければなりません。

ここでは次の４つを要件として取り上げ、それぞれについての考え方を示します。

- 入力者及び確定者の識別と認証
- 記録の確定
- 識別情報の記録
- 更新履歴の保存

① 入力者及び確定者の識別・認証

真正性を確保する上で、何らアクセス権限を持たない者がシステムを利用することを排除し、自身の ID を持つ適正な入力者に利用を限定しなければなりません。よって、入力者の識別・認証は必須となります。また、入力者と確定者が異なる場合は、確定者の識別・認証も必要となります。

具体的な対策については、１４．認証・認可に関する安全管理措置の利用者の識別・認証に係る記述を参照してください。

代行入力を行う場合の留意点

医療機関等の運用上、代行入力を実施する場合には、必ず入力を実施する個人ごとに ID を発行し、その ID でシステムにアクセスしてください。また、日々の運用においても ID、パスワード等を他人に教えたり、他人の ID でシステムにアクセスしたりすることは、システムで保存される作業履歴から作業者が特定できなくなるため、禁止しなければなりません。

② 記録の確定

記録の確定は、当然、その記録の確定を実施できる権限を持つ確定者によって実施されなければなりません。多くの場合は、入力者にその権限があることが想定されるが、入力者にその権限がない場合は、権限を持つ確定者が記録の確定を実施する必要があります。

記録の確定は、確定された時点から真正性を確保して保存することを明確にするもので、いつ・誰によって入力され、また確定されたかを明確にして、その保存情報自体にはいかなる追記、変更及び消去も行われてないことを保証することを目的とします。なお、確定以降に追記、変更、消去の必要性が生じた場合は、その内容を確定済みの情報に関連付けた新たな記録として作成し、別途、確定保存しなければなりません。

手入力（スキャナやデジタルカメラ等の周辺機器からの情報取込操作を含む。）により記録が作成される場合は、入力者は過失による誤入力や混同のないことを確認する必要があります。また、それ以降の情報の追記、書換え及び消去等との区別を明確にするために、確定者により確定操作が行われなければなりません。

なお、明示的な確定操作が行われなくとも、最終入力から一定時間経過又は特定時刻通過により記録が確定されるとみなして運用される場合においては、入力者及び確定者を特定する方法とともに運用方法を定め、運用管理規程に明記する必要があります。

手入力以外に外部機器システムからの情報登録が行われる場合は、取込みや登録の時点で目的とする情報の精度や正確さが達成されていることを確認して、確定者による確定操作が行われる必要があります。

臨床検査システム、医用画像の撮影装置（モダリティ）やファイリングシステム（PACS）等の特定の装置又はシステムにより作成される記録では、当該装置からの出力結果を当該装置の管理者の責任において確定情報として扱い、運用される場合もあります。この場合、確定情報は、どの記録が・いつ・誰によって作成されたかが、システム機能と運用の組み合わせにより、明確になっている必要があります。

③ 識別情報の記録

確定された記録は、第三者から見て、いつ・誰が入力し、また確定したものであるかが明確になっている必要があります。入力者及び確定者の識別情報には、氏名及び作成された時刻を含むことが必要である。また、入力者及び確定者の識別情報が記録情報に関連付けられ、通常の手段では誤った関連付けができないこと、及びその関連付けの分離・変更又は改ざんができないことが保証されている必要があります。

識別情報は、入力者及び確定者が責任を持つ個別の行為ごとに、個々の患者の診療録等に対して記録又は記載されることを原則とします。初回の診療録等の作成時に入力者及び確定者の識別情報が必要であるが、確定の上で保存された後の追記、修正、削除等を行う場合も、該当する診療録等に対してその情報に係る入力者及び確定者の識別情報が必要です。

また、グループ診療のように、入力者が複数存在する場合でも、情報を入力する者は個々人であり、その複数の個人をそれぞれ入力者として記録する。かつ、その記録の確定は「（2）記録の確定」に従って実施しなければなりません。

④　更新履歴の保存

例えば、診療情報は診療の遂行に伴い増加し、その際、新たな知見を得たことにより、確定済みで保存してある記録に対して追記や修正を行うことが少なくないです。このような診療行為等に基づく記録の更新と、不正な記録の改ざんは容易に判別されなければなりません。そのためには記録の更新内容、更新日時を記録するとともに、権限に基づき更新内容の確定を行った確定者の識別情報を関連付けて保存し、それらの改ざんを防止でき、万一改ざんが起こった場合にもそれが検証可能な環境で保存しなければなりません。

シス１４章第⑧条

シQ－58　医療情報システムの認証において、真正性の確保を求める場合について、記載されている情報と確定者には具体的にどのような組み合わせがあるか。

Ａ　情報と確定者の組み合わせとしては下記のような例があります。

例 1）　医師が患者の診察時にカルテに所見を記述する。

情報　：所見

確定者　：実際に診察を行った医師

例 2）　看護師が医師の指示に基づく処置を行った際に、実施状況を看護記録に記述する。

情報　：処置実施記録

確定者　：実際に処置を行った看護師

例 3）　読影担当医が放射線画像の読影レポートを作成する。

情報　：読影レポート

確定者　：読影を行った放射線科医師

例 4）　検査技師が検査ラインから出力された検査結果のバリデーションを実施し、システムに取り込む。

情報　：検査結果

確定者　：バリデーションと取り込み操作を行った検査技師

例 5）　夜間等で当直医が主担当医の電話での指示により、指定された薬剤のオーダ入力を行った。

情報　：投薬指示

確定者　：実際にオーダを実施した当直医

シス１４章第⑧条ｆ

シQ－59　「１４．認証・認可に関する安全管理措置」 ⑧ｆにおいて、「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」とあるが、具体的にどのような場合を指すか。

Ａ　例えば、在宅で治療を行っている患者の様態が急変した等、緊急で対応すべき事由が発生したため、確定操作を行う時間的余裕もなく、担当医が外出せざるを得なくなった等の事例が考えられます。

シス１４章第⑧条

シQ－60　代行入力を行う場合、代行を許可した証拠はどのように残しておけばいいのか。

Ａ　代行入力を実施する場合には、必ず入力を実施する個人ごとに ID を発行し、代行入力を行う者はその ID でシステムにアクセスしなければなりません。その際、入力者のログ、あるいは作業報告等の台帳を作成し、記録を残す必要があります。

　また、誰の意思決定に基づいて代行入力を実施したかが説明できるように、上記の内容を含めた代行入力に関する運用管理規程等の策定が必要です。

シス１４章第⑧条

シQ－61　記録を確定する方法として、①入力者が情報を入力画面を見ながら入力して記録する場合、②外部機器等から確定されていない情報を取り込み記録する場合、③外部システムで確定された情報を取り込み記録する場合が考えられるが、それぞれどのように対応すべきか。

Ａ　確定操作は、文書の責任者が誰かを明らかにし、操作の時点で対象とする文書の記述に誤入力や改ざん等がないことを保証し、記載に対して責任を持つという意味合いがあります。そのため、上記①～③の対応について下記のように考えられます。

①　「入力者が情報を入力画面を見ながら入力し記録する場合」

　この場合には、確定するという操作を行うことで、内容を確定者が保証することになります。「確定者が」としたのは、文書の入力を確定者が自ら行う場合や代行入力による場合があるからです。いずれの場合も、運用管理規程等によって決められた確定者が確定したということになります。また、処理としては署名を施す等になります。

　代行入力の場合には、確定者が必ず確認を行った上で、確定を実施しなければなりません。

② 「外部機器等から確定されていない情報を取り込み記録する場合」
この場合には入力者が、記述の改ざんや誤入力等がないことを確認した上で、スキャナ等による読み込みを行い、誰の記録であるかを関連付けして、①の確定操作を行うことになります。

③ 「外部システムで確定された情報を取り込み記録する場合」
改めて受け取り側で確定操作を行う必要はありませんが、外部システムで確定されていることを確認することが必要です。ただし、確定された情報しか取り込まれないようにシステムが構築されている場合、その限りではありません。

シス１４章第⑧条

シQ－62　画像の確定に当たっては明示的な確定操作が必要か。

A　必ずしも必要ではありません。例えば、①PACS が受信した時点、②PACS で受信してから一定時間経過した時点、③PACS で受信してから一定時刻を過ぎた時点をもって確定とすること等が考えられます。これらについては、各医療機関等において、運用管理規程に明記することが必要です。

シス１４章、シス１２章

シQ－63　情報の重要度に応じでセキュリティ対策を講じたい場合どのように整理すべきか。

A　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してください。

15. 電子署名、タイムスタンプ

シス１５章第①条

シQ－64　法令で定められた記名・押印のための電子署名における要件として暗号に関するものがあるが、具体的にはどのようなものを採用する必要があるか。

A　ガイドラインにおいては、電子署名法における特定認証業務に係る電子署名等が要件を満たすものとして挙げられています。電子署名法における特定認証業務に係る電子署名の基準として、電子署名法施行規則第２条及び電子署名及び認証業務に関する法律に基づく特定認証業務の認定に係る指針（平成十三年四月二十七日総務省・法務省・経済産業省告示第二号）第３条では、RSA 方式であって、ハッシュ関数として SHA-256 を使用するもの、SHA-384 を使用するもの又は SHA-512 を使用するもののうち、モジュラスとなる合成数が2048bit以上のもの、RSA-PSS方式であって、SHA-256、SHA-384 又は SHA-512 を使用するもののうち、モジュラスとなる合成数が 2048bit 以上のもの、ECDSA 方式であって、ハッシュ関数として SHA-256 を使用するもの、SHA-384 を使用するもの又は SHA-512 を使用するもののうち、楕円曲線の定義体及び位数が 224bit 以上のもの、DSA 方式であって、ハッシュ関数として SHA-256 を使用するものであり、かつ、モジュラスとなる素数が 2048bit 以上のものが定められています。

シス１５章第①条

シQ－65　共通鍵、秘密鍵を使用して情報を管理する場合どの程度のレベルのものが必要か。

A　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ってください。

16. 紙媒体等で作成した医療情報の電子化

シス１６章第①条、同章第②条

シＱ－66　「１６．１　保存義務がある書面等に関する紙媒体等の電子化」における技術的な対応にある「また、スキャンにより、保存できない有用な情報」とは、どのようなものがあるか。

Ａ　現在のスキャナの機能は向上しており、高い解像度での読み取りや筆圧などを記録できるものもあります。一方、紙媒体においては、例えば、患者が疾患・症状から書面作成時に用紙をペン先で突き破ってしまったり、用紙の固定がうまくできず、不規則な折れ目（しわ）が付くこともあります。

　このような変化はスキャナで必ずしも正確に記録できないことがあるため、このような場合の記録を電子的に行う際は、スキャナで電子化するのではなく、適切に動画撮影をする方が正確な記録となる可能性があります。

　このようにスキャナで直接記録される文字情報等以外に、紙媒体の物理的な状態などの有用な情報があることについて、示したものです。

シス１６章第②条、企１６．２章

シＱ－67　診療録等をスキャナ等により電子化して保存する場合に、診療の用途に差し支えない精度の基準はあるか。

Ａ　画一的な基準はありません。手書き文書、ワープロ印刷文書、インスタント写真等、対象ごとに診断等の診療目的の利用に十分な精度を満たしていることをあらかじめ確認した上で、運用管理規程等で定めてください。

　なお、第３版までは 300dpi、RGB 各８ビット以上としていましたが、一般に販売されている汎用のスキャナでもこれ以上の性能を持つものが大多数を占めるために、記載を改めたものです。不用意に精度を下げることを推奨しているものではありません。

シス１６章第②条

シＱ－68　「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。」とあるが、どのようなケースで、どれくらいの対応時間内で行う必要があるのか。

Ａ　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、電子化した情報はあくまでも参照情報です。

　緊急時とは、例えばシステムダウン等が想定できます。また、一般に「診療のために直ちに特定の診療情報が必要な場合」とは継続して診療を行っている場合であり、患者の診療情報が緊急に必要になることが予測されるときは、診療に差し支えない範囲で原本である紙媒体を閲覧可能な状態にしておくことが必要です。

18. 外部からの攻撃に対する安全管理措置

シス１８省第①条

シQ－69	「１８．外部からの攻撃に対する安全管理措置」⑴の３つ目の「－」において、「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、」とあるが、外部からの攻撃を受けた場合の復旧のための対応としては、どのような点を考慮して、バックアップを取得する必要があるか。

A　バックアップ取得のポリシーは、医療の社会的な影響度を鑑みて、医療機関等における診療業務の継続性を確保するため、できる限り診療に影響に及ぼさないよう、計画を立てることが求められます。この部分は一般企業におけるバックアップに対する考え方との大きな違いになります。

但し具体的なバックアップ取得の計画については、取扱うデータの利用頻度やシステムが停止した場合に復元すべき時点、システムの特性などを考慮して、総合的に決定されるため、一意に決まるわけではありません。

例えばバックアップの取得範囲として、通常、フルバックアップ、差分バックアップ、増分バックアップなどがあり、適切に組み合わせて、対応することになります。

そのうえでさらに具体的な例として、日次で差分バックアップ、週次でフルバックアップを行う場合、前々週以前のフルバックアップ及びその週以前の日時の差分バックアップは、ネットワークから切り離した記録媒体で保管すること（磁気テープ、DVD、Blu-Ray 等）あるいは論理的に書き込み禁止（磁気ディスク等）の状態にする等の対策が必要となります。

最近ではクラウドサービスを利用したバックアップを行うことも考えられます。例えば、原本データ以外にクラウド上でバックアップを取得する場合、バックアップデータを追記できない設定としたり、複数のバックアップデータを取得したりするなどの方式で、複数方式によるバックアップを行うことが想定されます。

また電子カルテ、医事システム、LIS、RIS（PACS 含む）等のサブシステムがそれぞれデータベースを持つ場合、それぞれについてシステム特性やデータの影響度を鑑みて、バックアップ取得の計画を策定することになります。

具体的な例としては、電子カルテ、LIS 等保存データがあまり大きくないサブシステムについては、日次でバックアップを確保し、電子カルテは５世代、その他のシステムは３世代保存するなどにより、前週までのデータを回復することが想定されます。この場合、ランサムウェア等の攻撃への対策という観点から、電子カルテで３世代以降のバックアップデータについては、ネットワーク的あるいは論理的に書き込み禁止属性とし、その他のシステムは３世代目をネットワーク的あるいは論理的に書き込み禁止とするなどが求められます。

一方、PACS を含む RIS のような大量のデータを扱う場合はバックアップそのものが困難な場合もありえます。この場合には、サイバーセキュリティを考慮すると、確定されたデータについては書き込み禁止に設定するべきです。そのうえで、運用上可能であれば、例えばキー画像の指定がされた画像データ等は電子カルテと同様の対策するなどにより、医療の継続性の確保において極めて有用な対応になると考えられます。

バックアップ計画の策定に際しては、利用する医療情報システムやサービスを提供する事業者からの情報提供等を踏まえて検討することが重要です。例えば「「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」[6]では、「医療機関等には、情報を保存する場所や、その場所ごとの保存可能容量、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運用管理規程にまとめ、関係者に周知することが求められます。」（P24）とし、事業者によるバックアップに関する情報提供の有無が確認できることとなっています。事業者から情報提供されている場合には、その内容などを参考に、計画の策定を行うことが考えられます。また医療機関等が自らシステム構築を行う場合には、「非機能要求グレード 2018」（独立行政法人情報処理推進機構）などを参考に、バックアップ計画を策定するなども一案です。

なお別冊「[特集] 医療機関等におけるサイバーセキュリティ」も併せてご活用ください。

[6] 一般社団法人保健医療福祉情報システム工業会、一般社団法人日本画像医療システム工業会医用画像システム部会セキュリティ委員会