医療情報システムの安全管理に関するガイドライン

第 5.2 版

本編

令和 4 年 3 月

厚生労働省

改定履歴

版数	日付
第 1 版	平成 17 年 3 月
第 2 版	平成 19 年 3 月
第 3 版	平成 20 年 3 月
第 4 版	平成 21 年 3 月
第 4.1 版	平成 22 年 2 月
第 4.2 版	平成 25 年 10 月
第 4.3 版	平成 28 年 3 月
第 5 版	平成 29 年 5 月
第 5.1 版	令和 3 年 1 月
第 5.2 版	令和 4 年 3 月

【目次】

1. はじめに

本ガイドラインは、医療情報システムの安全管理や「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。）への適切な対応を行うため、技術的及び運用管理上の観点から所要の対策を示したものである。ただし、医療情報の適切な取扱いの観点からは、医療情報システムに関わる対策のみを実施するだけで十分な措置が講じられているとは言い難い。したがって、本ガイドラインを使用する場合、医療情報システムの担当者であっても、「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」を十分理解し、医療情報システムに関わらない部分でも医療情報の適切な取扱いのための措置が講じられていることを確認することが必要である。

本ガイドラインは、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（以下「医療機関等」という。）における電子的な医療情報の取扱いに係る責任者を対象とし、理解のしやすさを考慮して、現状で選択可能な技術にも具体的に言及した。したがって、本ガイドラインは技術的な記載の陳腐化を避けるために定期的に内容を見直す予定である。本ガイドラインを利用する場合は最新の版であることに十分留意すること。

第 2 版から第 5.1 版までの改定概要については別冊に掲載。

改定概要

【第 5.2 版】

本ガイドライン第 5.1 版の公表以降、医療等分野及び医療情報システムに対するサイバー攻撃が一層、多様化・巧妙化が進み、医療機関等における診療業務等に大きな影響が生じる被害も見られる。特にランサムウェアに代表される攻撃への対策は、喫緊の課題となっている。そのほか本ガイドラインを踏まえた対策を医療機関等が行う重要性が高まっている。

そのため、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例示などの部分を分けて記述した。具体的には、利用用途に応じて閲覧しやすいように本編と別冊とに分冊化を行った。

ランサムウェア対策との関係では、6.10 章において、ランサムウェアによる攻撃への対応としてのバックアップのあり方等の対策を示した。また適切なリスク分析を行い、被害に遭った際の対策を速やかに講じられるよう、6.2 章において、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）を整備する旨について示した。

医療機関等が利用する医療情報システムにおいて外部サービスとの連携が進む中で、アプリケーション間の安全性を確保する観点から、6.5 章において外部アプリケーションとの連携における利用者の認証・認可に関する記述を示した。

本ガイドラインにおいて、従来から利用が認められているシステムやサービスの利用形態に関して、これらの利用が安全に管理されている状況下で利用が可能であることを、改めて示すよう、一部記述の追記等を行った。具体的には、BYOD については安全に管理されている環境下での利用について、6.9 章において具体的な記述を行った。また外部ネットワークを利用する上で医療機関等が負うべき管理内容を明示した。

電子署名については、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 章の記載を整理した。具体的には、文書の作成者に資格が必要な場合に求められる署名についての要件等について示した。

その他関係制度の変更等に伴う修正を行った。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を 6.12 章において行った。併せて、電子署名に用いる暗号アルゴリズムの参照規格について、実務の状況を勘案して、JIS から ISO に参照規格を変更する旨を 6.12 章に示した。また外部保存を行う際の事業者の選定に関して、「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」（総務省・経済産業省　令和 2 年 8 月 21 日）における基準に揃えて 8.3 章の変更を行った。

その他、分かりやすさや表現の平仄を合わせる観点から、一部構成を修正した。

2. 本ガイドラインの読み方

本ガイドラインは本編において、医療機関等において実施すべき内容を示し、別冊でその考え方や、具体的な対応例などを示す形としている。医療機関等において、医療情報システムの安全対策上、求められる内容は本編において確認し、具体的な対策を検討するに際して、本編で述べた内容の考え方や具体例などを別冊において確認すること。本編においては次のような構成になっている。医療機関等の管理者、医療情報システム安全管理責任者及び医療機関等から業務を受託する事業者が、それぞれ関連する箇所を理解した上で、必要な対策を実施することを期待する。

なお、本ガイドラインでは、医療情報、医療情報システムという用語を用いているが、これは医療に関する患者情報（個人識別情報）を含む情報及びその情報を扱うシステムという意味で用いている。

【1 章～6 章及び 10 章】

医療情報を扱う全ての医療機関等が参照すべき内容を含んでいる。

【7 章】

保存義務のある診療録等を電子的に保存する場合に参照すべき内容を含んでいる。

【8 章】

保存義務のある診療録等を電子媒体により外部保存する場合に参照すべき内容を含んでいる。

【9 章】

e-文書法に基づいてスキャナ等により電子化して保存する場合の指針を含んでいる。

なお、本ガイドラインの大部分は法律、厚生労働省通知、他の指針等の要求事項に対応する対策を示すことを目的としており、そのような部分では概ね、以下の項に分けて説明している。

A. 制度上の要求事項

法律、厚生労働省通知、他の指針等の要求事項を記載している。

B. 考え方

要求事項の解説及び原則的な対策方針について記載している。

C. 最低限のガイドライン

A 項の要求事項を満たすために必ず実施しなければならない対策を記載している。ただし、医療機関等の規模により実際に必要な対策が異なる場合や、幾つかの対策の中の一つを選択する場合もあるため、付表の運用管理表を活用し、適切な対策を採用して、実施しなければならない。

D. 推奨されるガイドライン

実施しなくても A 項の要求事項を満たすことが可能であるが、説明責任の観点から実施した方が理解を得やすい対策を記載している。

また、最低限のシステムには使用されていない技術を使用する上で一定の留意が必要な事項の記載も含んでいる。

なお、別紙の 3 つの付表は、安全管理上要求事項を満たすための技術的対策と運用的対策の関係を要約したもので、運用管理規程の作成に活用されることを期待して作成した。安全管理対策は技術的対策と運用的対策の両面でなされて初めて有効なものとなるが、技術的対策には複数の選択肢があることが多いため、付表を活用して、採用した技術的対策に相応した運用的な対策を実施すること。なお、付表は以下の項目で構成している。

1. 運用管理項目：安全管理上の要求事項で多少とも運用的対策が必要な項目
2. 実施項目：上記管理項目を実施レベルに細分化したもの
3. 対象：医療機関等の規模の目安
4. 技術的対策：技術的に可能な対策（一つの実施項目に対して選択可能な対策を列挙した）
5. 運用的対策：上記 4. の技術的対策を行った場合に必要な運用的対策の要約
6. 運用管理規程文例：運用的対策を規程に記載する場合の文例

各医療機関等は、実施項目に対して採用した技術的対策に応じ、必要な運用的対策を運用管理規程に含め、実際に規程が遵守されていることを確認することで、実施項目を達成することが可能となる。また、技術的対策を選択する前に、それぞれの運用的対策を検討することで、各医療機関等で運用可能な範囲の技術的対策を選択することも可能となる。一般に運用的対策の比重を大きくすれば医療情報システムの導入コストは下がるが、技術的対策の比重を大きくすれば利用者の運用的な負担は軽くなる。運用的対策と技術的対策について適切なバランスを求めることは非常に重要なので、運用的対策及び技術的対策の選択に、これらの付表が活用されることを期待する。

3. 本ガイドラインの対象システム及び対象情報

本ガイドラインは医療情報を保存するシステムだけではなく、医療情報を扱う全ての情報システムと、それらのシステムの導入、運用、利用、保守及び廃棄に関わる人及び組織を対象としている。ただし、「7　電子保存の要求事項について」、「8　診療録及び診療諸記録を外部に保存する際の基準」、及び「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」は対象となる医療情報が、一部の文書等に限定されている。

3.1. 7章及び9章の対象となる文書について

医療情報を含む文書は、法令等によって保存、作成、交付等が定められている文書と、そうでない文書に大別できる。7章及び9章は、法令等によって保存、作成、交付等が定められている文書の一部であり、具体的には、e-文書法の対象範囲となる医療関係文書等として、「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日厚生労働省令第44号。以下「e-文書法省令」という。）、「「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日付け医政発0331第30号・薬生発0331第10号・保発0331第26号・政社発0331第1号厚生労働省医政局長、医薬・生活衛生局長、保険局長、政策統括官（社会保障担当）連名通知。以下「施行通知」という。）で定められた文書等（別冊参照）を取り扱う場合を対象としている。

また、介護事業者が取り扱う文書等のうち、一部の文書等（別冊参照）は、e-文書法の対象範囲でかつ当該文書の内容に医療情報が含まれることがある。この場合、この文書等に限らず、介護事業者は、7章及び9章の規定を遵守する必要がある。

3.2. 8章の対象となる文書等について

8章は、「「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日付け医政発0325第15号・薬食発0325第9号・保発0325第5号厚生労働省医政局長・医薬食品局長・保険局長連名通知。以下「外部保存改正通知」という。）で定められた文書等（別冊参照）を取り扱う場合を対象としている。

なお、調剤録の保存については、薬局開設者の責任とされており、外部保存を行う場合についても従前と同様に薬局開設者の責任で行う必要がある。また、調剤録は当該薬局に備えることとされているため、当該薬局の調剤録を外部保存する場合には、他の薬局の調剤録と明確に区分し、薬局ごとに個別に管理する必要がある。

3.3. 紙の調剤済み処方箋と調剤録の電子化・外部保存について

紙の調剤済み処方箋の電子化は、紙の処方箋に法令で定められた事項を記入した後、記名押印又は署名を行い調剤済みとしたものを 9 章に示す方法により実施することとなる。

薬局で紙の処方箋を受け取った場合、調剤済みとなるまでは電子化したものを原本としてはならない（誤った運用例：薬局で紙の処方箋を受け付けた時点で電子化し、それを原本として調剤を行い、薬剤師の電子署名をもって調剤済みとする等）。

なお、調剤終了時までは特段の問題なく経過した処方箋であっても、その後に内容の修正が発生することを完全には否定できない（例：記載事項を確認したものの修正を忘れた場合等）。そのため、一旦電子化した紙の調剤済み処方箋であっても、その修正が発生する可能性がある。

この場合、既に電子化された紙の調剤済み処方箋に対して、過去の電子署名の検証が可能な状態を維持する形で、電子的に修正を実施し、薬剤師の電子署名を付すことが必要となる。

なお、電子処方箋を（電子的な）調剤済み処方箋とした場合には 7 章を、さらにそれを外部保存する場合には、8 章を参照すること。

3.4. 取扱いに注意を要する文書等

3.1 章に示した文書等のほか、医療関係文書等のうち個人情報の保護について留意しなければならないものには、①施行通知には含まれていないものの、e-文書法の対象範囲で、かつ患者の個人情報が含まれている文書等（麻薬帳簿等）、②法定保存年限を経過した文書等、③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、④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）等がある。

これら①～④に示した文書等については、個人情報保護関連各法の趣旨を十分理解した上で、各種指針及び本ガイドライン 6 章の対策事項を実施するとともに、情報管理体制確保の観点から、バックアップ情報等を含め、それらを破棄せず保存している限り、3.1 章に示す文書等に準じて取り扱う必要がある。

なお、「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」も、適宜参照すること。

また、3.2 章に示す文書等がその法定保存年限を経過する等の事由によって、施行通知や外部保存改正通知の対象外となった後においても、外部保存を実施（継続）する場合には、3.2 章に示す文書等に準じて取り扱わなければならない。

4. 電子的な医療情報を扱う際の責任のあり方

本章では、医療機関等、情報処理事業者、電気通信事業者等の関係者間での電子的な医療情報の取扱いにおける責任の在り方について、「医療機関等の管理者の情報保護責任の内容と範囲」及び「他の医療機関等や事業者に情報処理の委託や他の業務の委託に付随して医療情報を委託する場合と第三者提供した場合」に分けて、責任分界という概念を用いて整理した（具体的な内容は別冊「4.電子的な医療情報を扱う際の責任のあり方」参照)。

4.1. 医療機関等の管理者の情報保護責任について

医療機関等の管理者が医療情報を適切に管理するための善管注意義務を果たすためには、通常の運用時における医療情報保護の体制を構築し管理する責任と、医療情報について何らかの不都合な事態（典型的には情報漏えい）が生じた場合に対処をすべき責任とがある。便宜上、本ガイドラインでは前者を「通常運用における責任」、後者を「事後責任」と呼ぶこととする。

(1) 通常運用における責任について

ここでいう通常運用における責任とは、医療情報の保護のための適切な情報管理ということになるが、適切な情報管理を行うことが全てではなく、以下に示す 3 つの責任を含む必要がある。

① 説明責任

医療情報システムの機能や運用方法の取扱いに関する基準を満たしていることを患者等に説明できるようにする責任である。この責任を果たすためには、以下のことが必要である。

- 医療情報システムの仕様や運用方法を明確に文書化すること
- 仕様や運用方法が文書化した方針のとおりに機能しているかどうかを定期的に監査すること
- 監査結果をあいまいさのない形で文書化すること
- 監査の結果問題があった場合は、真摯に対応すること
- 対応の記録を文書化し、第三者が検証可能な状況にすること

② 管理責任

医療情報システムの運用管理を行う責任である。医療情報システムの管理を受託する事業者に任せきりにしているだけでは、これを果たしたことにはならないため、医療機関等においては、以下のことが必要である。

- 管理状況の報告を定期的に受けること

・　管理に関する最終的な責任の所在を明確にすること
・　受託する事業者を監督すること

さらに、「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。）上は、受託する事業者との対応に当たり、以下のことが必要である。

・　個人情報保護の責任者を定めること
・　電子化された個人情報の保護について一定の知識を有する責任者を決めること

③ 定期的に見直し必要に応じて改善を行う責任

情報保護に関する技術は日進月歩であり、情報保護体制が陳腐化するおそれがあるため、医療情報保護の仕組みの改善を常にこころがけ、現行の運用管理全般の再評価・再検討を定期的に行う責任がある。この責任を果たすためには、以下のことが必要である。

・　医療情報システムの運用管理の状況を定期的に監査すること
・　問題点を洗い出し、改善すべき点があれば改善すること

⑵ 事後責任について

医療情報について何らかの不都合な事態（典型的には漏えい）が生じた場合、医療機関等の管理者には、以下の責任がある。

なお、「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 Ⅳ 8.」では、漏えい等の報告等について規定していることから、参照すること。

① 説明責任

特に医療機関等は一定の公共性を有するため、個々の患者に対する説明責任があることは当然ながら、併せて監督機関である行政機関や社会への説明・公表も求められる。そのため、医療情報について何らかの不都合な事態が生じた場合、以下のことが必要である。

・　その事態の発生を公表すること
・　原因及びそれに対する対処方法について説明すること

②　善後策を講ずる責任

また、医療情報について何らかの不都合な事態が生じた場合、善後策を講ずる責任として、以下のことが必要である。

・　原因を追及し明らかにすること
・　損害を生じさせた場合にはその損害を填補すること
・　再発防止策を講ずること

4.2. 委託と第三者提供における責任分界

医療情報を外部の医療機関等や事業者に伝送する場合、個人情報保護法上、その形態には委託（第三者委託）と第三者提供の 2 種類がある。本節では、それぞれの形態における医療機関等の管理者の情報保護責任のあり方を、前節で挙げた責任の分類に従って整理して示す。

4.2.1. 委託における責任分界

委託の場合、管理責任の主体はあくまでも医療機関等の管理者である。医療機関等の管理者は、患者に対する関係では、受託する事業者の助けを借りながら、前節に掲げた「説明責任」、「管理責任」及び「定期的に見直し必要に応じて改善を行う責任」を果たす義務を負う。

万一、何らかの不都合な事態が生じた場合にも同様に、受託する事業者と連携しながら「説明責任」及び「善後策を講ずる責任」を果たす必要があるため、受託する事業者との契約において、受託する事業者の義務を明記すべきである。

また受託する事業者の責任によって不都合な事態が生じた場合に、受託する事業者との間で「善後策を講ずる責任」をどのように分担するかについても、受託する事業者との契約で明記すべきである。

そのため、「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」に示す「サービス仕様適合開示書」、「サービスレベルアグリーメント」において、その内容を明記させる必要がある。

4.2.2. 第三者提供における責任分界

医療機関等が医療情報の第三者提供を行う場合、個人情報保護法、関連するガイドライン、「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」等を遵守する必要がある。

4.3. 例示による責任分界点の考え方の整理

責任分界点について検討する際に、いくつか例が想定される。各例において、医療情報システムや外部接続時のネットワークの安全管理の考え方、保存義務のある書類の保存、外部保存を受託することが可能な機関の選定基準等を検討する際には、それぞれ 6 章、7 章、8 章を参照する必要がある。具体的な例としては、

- 地域医療連携で「患者情報を交換」する場合（第三者提供による場合、共同利用による場合等）
- 業務の必要に応じて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
- 医療機関等の業務の一部を委託することに伴い、情報が「一時的に外部に保存」される場合
- オンライン外部保存を委託する場合

などが挙げられる。特にオンライン外部保存を委託する場合については、医療情報システムにおいて、オンプレミスばかりではなく、クラウドサービスを利用するケースも増えていることから留意点を示す。

クラウドサービスを利用する際の医療情報システムの新規導入・更新や運用は、受託事業者経由で行うことになるほか、サービスの性格上、サービスに用いている機器等を共同利用することとなる。そのため、医療情報システムの管理監督や責任分界においても、このような特性を踏まえた管理方法による取決めを行う必要がある。

各例における具体的な考え方は、別冊において示す。

4.4. 技術的対策と運用による対策における責任分界点

医療情報システムの安全を担保するためには、「技術的な対応（対策）」と「組織的な対応（運用による対策）」を総合的に組み合わせる必要がある。

特に、技術的な対応（対策）は、医療機関等の総合的な判断の下、主にシステム提供側（システムベンダ及びサービス事業者）を中心に医療機関等と協働で対策を行うことが求められ、組織的な対応（運用による対策）は利用者側（医療機関等）の責任で実施される。

5. 情報の相互運用性と標準化について

医療機関等では、業務上様々な情報のやりとりが行われ、それらによる指示、報告、連絡等の意思の共有によって一連の業務が成立する。

これらのやりとりを単に電子化するだけであれば、これまでの業務に情報入力という業務を付加してしまうだけである。しかし、その電子化された情報の再利用が可能であれば、幾度もの同一情報の入力作業を軽減し、業務の総量を減ずることが可能となる。また、紙等の情報を読解して再入力する際のミスの防止、指示の誤記・誤読の防止という観点から、医療安全に資することにもなる。

事実、医療機関等において電子化された情報を扱うシステムの導入は、当初、事務処理の合理化を目的としたものであったが、現在では情報共有の推進や、医療安全、ひいては医療の質の向上に資することを目的としたものになっている。

このような電子化された情報のやりとりを、段階的に導入されたシステム間や、異なるシステムベンダ及びサービス事業者から提供されたシステム間で行う際に必要となるのが、相互運用性の確保である。

一方、医療情報システムの安全な管理・運用における重要な観点として、情報セキュリティの重要な要素の一つである「可用性」が挙げられる。ここでいう可用性とは、必要なときに情報が利用可能であることを指し、情報を利用する任意の時点で可用性が確保されなければならない。このことは、7.2 章及び 7.3 章で述べるように、例えば、医療機関等で医療情報を長期間保存する際に、システム更新を経ても旧システムで保存された医療情報を確実に利用できるようにしておくこと、すなわち相互運用性を確保することも意味する。

さらに、地域連携等における医療機関等間の情報の共有、蓄積、解析、再構築、返信、再伝達等といった場面においても、相互運用性の考え方は重要である。

このような医療情報の相互運用性を確保するためには、誰もが参照可能かつ利用可能で将来にわたりメンテナンスの継続が期待される標準規格（用語集やコードセット、保存形式、メッセージ交換手続等）を利用するか、それらに容易に変換できる状態で保存することが望ましい。よって、本章ではそれらについて記した。

医療情報における標準規格に関する民間主導の取組みとして、各種の標準化団体・規格制定団体等が会員となっている一般社団法人医療情報標準化推進協議会（Health Information and Communication Standards Organization ： HELICS 協議会）がある。HELICS 協議会が利用目的ごとに採択すべき標準規格を推奨し、その利用のための医療情報標準化指針を示している。

経済産業省・厚生労働省においても、種々の国際規格との整合を図り、これを推奨する等の取組みを進めてきた。

特に、HELICS 協議会が指針として掲げた標準規格のうち、我が国で必要不可欠と考えられるものについては、厚生労働省の保健医療情報標準化会議での審議を経て「厚生労働省標

準規格」とし、その実装を強く推奨しており、標準化の一層の推進が期待されるところである（具体的な内容は別冊「5.情報の相互運用性と標準化について」参照)。

医療機関等において、自らこれらの用語・コードのメンテナンスや標準規格の実装作業をすることは稀であろうが、標準規格に基づく相互運用性の確保の推進に向けて、システムベンダ及びサービス事業者にこういったことを要件として求めていくことが重要である。

したがって、医療情報システムを導入しようとするときや、現に保有する医療情報システムの運用に当たっても、下記のことについてシステムベンダ及びサービス事業者から説明を受ける等して、一定の理解を共有しておく必要がある。

- 標準化に対する基本スタンス
- 標準規格に対応していないならばその理由
- 将来のシステム更新、他社システムとの接続における相互運用性に対する対応案

さらに、現在導入している医療情報システムの更新や医療情報システムの新規導入の際に、医療機関等においても相互運用性について中長期的なビジョンを持ち、計画を策定していくことが望ましい。

6. 医療情報システムの基本的な安全管理

医療情報システムの安全管理は、個人情報保護関連各法（個人情報保護法、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）及び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））に規定された安全管理・確保に関する条文によって法的な責務として求められている。安全管理を疎かにすることは上記法律に違反することになるが、医療において最も重要なことは患者等との信頼関係であり、単に違反事象が起こっていないことを示すだけでなく、安全管理が十分であることを説明できるようにすること、つまり説明責任を果たせるようにすることが求められる。この章での制度上の要求事項として、個人情報保護法の条文を例示する。

A. 制度上の要求事項

（安全管理措置）

個人情報取扱事業者は、その取り扱う個人データの漏えい、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。

（従業者の監督）

個人情報取扱事業者は、その従業者に個人データを取り扱わせるに当たっては、当該個人データの安全管理が図られるよう、当該従業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。

（委託先の監督）

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。

（個人情報保護法　第 23 条　第 24 条　第 25 条）

6.1. 方針の制定と公表

B. 考え方

「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」において、個人情報保護に関する方針を定め公表することが求められている。本ガイドラインが対象とする医療情報システムの安全管理も、個人情報保護対策の一部として考えることができるため、この方針の中で、医療情報システムの安全管理についても言及する必要がある。

個人情報を取り扱う医療情報システムを運用する組織は、これらの要求事項を勘案して組織の実情に合った基本的な方針を策定し、適切な方法で公開することが重要である。

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。
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

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

安全管理を適切に行うための標準的なマネジメントシステムが ISO（ISO/IEC 27001:2013）及び JIS（JIS Q 27001:2014）によって規格化されている。適切なマネジメントシステムを採用することは、安全管理の実践において有用である。

なお、医療情報システムで扱われている情報のリストアップやリスク分析及び対策に当たっては、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が重要である。その際には、「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」（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」や、保健医療福祉情報システム工業会の JAHIS 標準及び日本画像医療システム工業会規格（JESRA）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が参考になる。

「『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」は以下の URL から取得できる。

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

https://www.jira-net.or.jp/publishing/jesra_public.html

6.2.1. ISMS 構築の手順

ISMS の構築は PDCA モデルによって行われる。JIS Q27001:2006（※）では PDCA の各ステップを次の様に規定している。

※ JIS Q27001:2014 では PDCA との記述は使われていないが、「情報セキュリティマネジメントシステム」として「組織は、この規格の要求事項に従って ISMS を確立し、実施し、維持し、かつ、継続的に改善しなければならない。」と記述されている。そのモデルとして PDCA サイクルが理解しやすいので旧版を引用している。

ISMS プロセスに適用される PDCA モデルの概要

Plan－計画 （ISMS の確立）	組織の全般的方針及び目的に従った結果を出すための、リスクマネジメント及び情報セキュリティの改善に関連した、ISMS 基本方針、目的、プロセス及び手順の確立
Do－実施 （ISMS の導入及び運用）	ISMS 基本方針、管理策、プロセス及び手順の導入及び運用
Check－点検 （ISMS の監視及び見直し）	ISMS 基本方針、目的及び実際の経験に照らした、プロセスのパフォーマンスのアセスメント（適用可能ならば測定）、及びその結果のレビューのための経営陣への報告
Action－処置 （ISMS の維持及び改善）	ISMS の継続的な改善を達成するための、ISMS の内部監査及びマネジメントレビューの結果又はその他の関連情報に基づい

	た是正処置及び予防処置の実施

P（Plan）では ISMS 構築の骨格となる文書（基本方針、運用管理規程等）により、ISMS 構築手順を確立する。

D（Do）では P で準備した文書や手順を使って実際に ISMS を構築する。

C（Check）では構築した ISMS が適切に運用されているか、監視と見直しを行う。

A（Action）では改善すべき点が出た場合に是正処置や予防処置を検討し、ISMS を維持する（具体的な内容は別冊「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」参照)。

6.2.2. 取扱い情報の把握

医療情報システムで扱う情報を全てリストアップし、安全管理上の重要度に応じて分類を行い、常に最新の状態を維持する必要がある。このリスト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されなければならない。

安全管理上の重要度は、安全性が損なわれた場合の影響の大きさに応じて決める。少なくとも患者等の視点からみた影響の大きさと、業務継続の視点からみた影響の大きさを考慮する必要がある。このほかにも、医療機関等の経営上の視点、人事管理上の視点等の必要な視点を加えて重要度を分類する。

個人を識別可能な医療に係る情報の安全性に問題が生じた場合、患者等に極めて深刻な影響を与える可能性があるため、医療情報は最も重要度の高い情報として分類される。

6.2.3. リスク分析

分類された情報ごとに、管理上の過誤、機器の故障、外部からの侵入、利用者の悪意、利用者の過誤等の脅威を列挙する。医療機関等では一般に他の職員等への信頼に基づいて業務を進めているため、利用者の悪意や過誤を想定することに抵抗があると思われる。しかし、情報の安全管理を達成して説明責任を果たすためには、例え起こり得る可能性は低くても、万一に備えて対策する必要がある。また、説明責任を果たすため、これらのリスク分析の結果は文書化して管理する必要がある。この分析により得られた脅威に対して、6.3 章から 6.12 章の対策を行うことになる。

また、情報の安全管理や、個人情報保護法で原則禁止されている目的外利用の防止は、システム機能だけでは決して達成できないことに留意しなければならない。システムとして可能なことは、人が正しく操作すれば誰が操作したかを明確に記録しつつ安全に稼動することを保証することであり、これが限界である。したがって、人の行為も含めた脅威を想定し、運用を含めた対策を講じることが重要である。加えて、この観点から、組織が管理しない機器やソフトウェア、サービスの利用を禁止することが求められる。

リスク分析で明らかとなった脅威について対策を行うことにより、発生可能性を低減し、リスクを実際上問題のないレベルにまで小さくすることが必要である。

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。
2. リストアップした情報を、安全管理上の重要度に応じて分類し、常に最新の状態を維持すること。
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。
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
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。
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。
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。

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。

6.3. 組織的安全管理対策（体制、運用管理規程）

B. 考え方

安全管理について、従業者の責任と権限を明確に定め、規程や手順書を整備運用し、その実施状況を日常の自己点検等によって確認しなければならない。これは組織内で医療情報システムを利用するかどうかに関わらず遵守すべき事項である。組織的安全管理対策には以下の事項が含まれる。

① 安全管理対策を講じるための組織体制の整備
② 安全管理対策を定める規程等の整備と規程等に従った運用
③ 医療情報の取扱い台帳の整備
④ 医療情報の安全管理対策の評価、見直し及び改善
⑤ 情報や端末の外部持ち出しに関する規則等の整備
⑥ 端末等を用いて外部から医療機関等のシステムにリモートアクセスする場合は、その端末等の管理規程
⑦ 事故又は違反への対処

管理責任や説明責任を果たすために運用管理規程は極めて重要であり、必ず定めなければならない。

なお、情報及び情報機器を医療機関等以外に持ち出して取り扱う場合についての詳細については、別途、6.9 章に記載しているので参照すること。

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。
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。
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。
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。
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

6.4. 物理的安全対策

B. 考え方

物理的安全対策とは、医療情報システムにおいて個人情報が入力、参照又は格納される端末や情報媒体等を物理的な方法によって保護することである。具体的には情報の種別、重要性と利用形態に応じていくつかのセキュリティ区画を定義した上で、以下の事項を考慮して、適切に管理する必要がある。

- 入退館（室）の管理（業務時間帯、深夜時間帯等の時間帯別に、入室権限を管理）
- 盗難、覗き見等の防止
- 機器、装置、情報媒体等の盗難や紛失防止も含めた物理的な保護及び措置

また、医療情報システムを格納するデータセンター等の場所については、6.2.3 章のリスク分析を踏まえて、適切に選定することが重要である。

なお、情報及び情報機器を医療機関等以外に持ち出して取り扱う場合についての詳細については、別途、6.9 章に記載しているので参照すること。

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。
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。
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。
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。
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。

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。

6.5. 技術的安全対策

B. 考え方

技術的な対策のみで全ての脅威に対抗できる保証はないため、運用管理による対策との併用は必須である。

しかし、その有効範囲を認識し適切な適用を行えば、技術的な対策は強力な安全管理の手段となり得る。ここでは 6.2.3 章のリスク分析で列挙した脅威[1]に対抗するために利用できる技術的な対策として下記の項目について解説する。

(1) 利用者の識別・認証
(2) 情報の区分管理とアクセス権限の管理
(3) 外部のアプリケーションとの連携における認証・認可
(4) アクセスの記録（以降、アクセスログという。）
(5) 不正ソフトウェア対策
(6) ネットワーク上からの不正アクセス
(7) 医療等分野における IoT 機器の利用

なお、情報及び情報機器を医療機関等以外に持ち出して取り扱う場合についての詳細については、別途、6.9 章に記載しているので参照すること。

(1) 利用者の識別・認証

医療情報システムへのアクセスを正当な利用者のみに限定するために、医療情報システムは利用者の識別・認証を行う機能を持たなければならない。

小規模な医療機関等で医療情報システムの利用者が限定される場合には、日常の業務の際に必ずしも識別・認証が必須とは考えられないケースが想定されることもあるが、一般的にこの機能は必須である。

認証を実施するためには、医療情報システムへのアクセスを行う全ての職員及び関係者に対し ID・パスワードや IC カード、電子証明書、生体認証等、本人の識別・認証に用いる手段を用意し、統一的に管理する必要がある。また更新が発生する都度速やかに更新作業が行われなければならない。

このような利用者の識別・認証に用いられる情報は、本人しか知り得ない、又は持ち得ない状態を保つ必要がある。

認証強度の考え方として、現状において、医療情報システムにアクセスする端末ごとに二要素認証を追加実装することは、医療機関等の負担が増加すると考えられる。このような技術は、本来システムにあらかじめ実装されているべきであり、今後、認証に係

[1] 具体的な脅威については、別冊 6.2 を参照。

る技術の端末への実装状況等を考慮し、できるだけ早期に対応することが求められる（※）。

※ 二要素認証技術の端末等への実装を促してきたが、さらに強く推し進めるため、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、導入又は更新する場合、原則として二要素認証を採用することが求められる。

また医療情報システムに二要素認証が実装されていないとしても、例えば放射線管理区域や薬局の調剤室など、指定された者以外の者の入室が法令等により制限されるような区画の中に端末が設置されている医療情報システムであって、当該区画への入場に当たって利用者の識別・認証が適切に実施されており、入場時と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る場合には、二要素認証に相当すると考えてよい。

(2) 情報の区分管理とアクセス権限の管理

医療情報システムの利用に際しては、情報の種別、重要性と利用形態に応じて情報の区分管理を行い、その情報区分ごと、組織における利用者や利用者グループ（業務単位等）ごとに利用権限を規定する必要がある。ここで重要なことは、付与する利用権限を必要最小限にすることである。

知る必要のない情報は知らせず、必要のない権限は付与しないことでリスクを低減できる。医療情報システムに、参照、更新、実行、追加等のようにきめ細かな権限の設定を行う機能があれば、さらにリスクを低減できる。

アクセス権限の見直しは、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適宜行う必要があるため、その運用方法について組織の規程で定めなければならない。

また、クラウドサービスを利用する場合、利用するサービスによっては、医療機関等の規程に基づいて定めたシステム上の設定（ポリシー）が、デフォルトの設定となる等、自動的に意図しない内容に変更されてしまう危険性がある。これにより、アクセス権限等が変更され、医療情報が意図しない相手先に送付されるなどのリスクが想定される。このような状況を防ぐため、意図せぬ設定の変更に関して検知できる措置を講じることが求められる。特に自動的に検知し、運用に反映できることが必要となる。

(3) 外部のアプリケーションとの連携における認証・認可

クラウドサービスなどの普及から、外部のアプリケーションを連携して用いる場面等が多くなってきている。院内のシステムと外部アプリケーションを連携して用いる場合や、複数のクラウドサービスを連携して用いる場合には、アプリケーション間でデータの引き渡しなどを行う必要が生じる。昨今、システム間連携のインタフェースとして、Web 技術のうち、連携のしやすさから、REST API（Representational State Transfer Application Programming Interface）が活用されている。REST API は Web の技術を用

いてサーバにアクセスして情報をやりとりする手順であるが、インターネット上で公開されることにより、IoT 機器や ASP サーバ等も含め、広くシステム間での情報連携の促進が期待できる。一方で、このような API がサイバー攻撃の起点となる可能性を踏まえ、セキュリティ上の対応策が求められる。このことは、HL7 FHIR の規格を用いた API ごとの連携促進の観点からも重要な問題となる。

API 連携のセキュリティ確保のためには、外部からの攻撃や意図せぬアクセスを防止できるように、必要に応じてネットワークセキュリティを確保し、API 連携により利用するユーザー・アプリケーションやデバイスの範囲を限定し、その責任分界とアクセスポリシーやログ管理を明確にした上で、それに沿った認証・認可に関する仕組みを設ける必要がある

(4) アクセスログ

個人情報を含む資源については、全てのアクセスログを収集し、定期的にその内容をチェックして不正利用がないことを確認しなければならない。

アクセスログは、それ自体に個人情報が含まれている可能性があること、さらにはセキュリティ事故が発生した際の調査に非常に有効な情報であることから、その保護は必須である。したがって、アクセスログへのアクセス制限を行い、アクセスログへの不当な削除／改ざん／追加等を防止する対策を講じなければならない。このためにログサーバで統合して管理し、ログサーバのアクセス制限を講じることも有効である。

また、アクセスログの証拠性確保のため、記録する時刻の精度も重要である。精度の高いものを使用し、管理対象の全てのシステムで同期を取らなければならない。

加えて、ログを分析し、緊急時にアラートを発する仕組みを講じることも求められる。

医療情報システムの管理を事業者に委託している場合には、ログの管理方法や提供等に関して、明確にする必要がある。

なお、医療機関等において取り扱っている医療情報システムにアクセスログを収集する機能がない場合には、システム操作に係る業務日誌等を作成し、操作の記録（操作者及び操作内容等）を管理する必要がある。

(5) 不正ソフトウェア対策

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。）は、電子メール、ネットワーク、可搬媒体等を通して医療情報システム内に入る可能性がある。不正ソフトウェアの侵入に際して適切な保護対策が行われていなければ、セキュリティ機構の破壊、システムダウン、情報の漏えいや改ざん、情報の破壊、資源の不正使用等の重大な問題が引き起こされる。そして、何らかの問題が発生して初めて、不正ソフトウェアの侵入に気付くことになる。

対策としては不正ソフトウェアのスキャン用ソフトウェアの導入が最も効果的であ

ると考えられ、このソフトウェアを医療情報システム内の端末、サーバ、ネットワーク機器等に常駐させることにより、不正ソフトウェアの検出と除去が期待できる。また、このことは医療機関等の外部で利用する端末や PC 等についても同様であるが、その考え方と対策については、6.9 章を参照すること。

ただし、これらの不正ソフトウェアは常に変化しているため、検出するためのパターンファイルや検索エンジンを常に最新のものに更新しておく必要がある。

また、たとえ優れたスキャン用ソフトウェアを導入し、適切に運用したとしても、全ての不正ソフトウェアが検出できるわけではない。不正ソフトウェアの対策としては、スキャン用ソフトウェアを導入するだけでなく、医療情報システム側の脆弱性を可能な限り小さくしておくことが重要である。そのために実施すべき対策として、セキュリティ・ホール（脆弱性）が報告されているソフトウェアへのパッチ適用、利用していないサービスや通信ポートの非活性化、マクロ等の利用停止、メールやファイルの無害化がある。また、EDR（Endpoint Detection and Response）や「振る舞い検知」などの方策も有効である。なお、いずれの対策を行う場合も、対策を実施した際の業務への影響や、対策処理の速度や可用性、網羅性について、十分な検討が必要である。

(6) ネットワーク上からの不正アクセス

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る。

また、不正な攻撃を検知するシステム（IDS：Intrusion Detection System)、不正な攻撃を遮断するシステム（IPS：Intrusion Prevention System）もあるため、医療情報システムと外部ネットワークとの関係に応じて、IDS、IPS の採用も検討すべきである。また、システムのネットワーク環境におけるセキュリティホール（脆弱性等）に対する診断（セキュリティ診断）を定期的に実施し、パッチ適用等の対策を講じておくことも重要である。

さらに、近時のサイバー攻撃の高度化・多様化に鑑みると、上記対策等に加えて、不正ソフトウェアが侵入した場合を想定した内部脅威監視などのモニタリングを講じることも、有効な対策として挙げられる。モニタリングについては、費用対効果を鑑みて、リスクの高いところについて重点的に行うなども考えられる。

(7) 医療等分野における IoT 機器の利用

本節では、IoT 機器（センサ等で自動的に情報を取得し、又は他の機器が自動的に取得した情報を中継し、ネットワークを通じて他の医療情報システムに送信する機器）によって医療に関する個人の情報を取得し、ネットワークを介して収集する仕組みを利用する場合に遵守すべき事項を規定する。

なお、本ガイドラインにおいては、医療情報の適切な保全を目的として IoT 機器の適

切な取扱いに関する要件を定めているものであり、「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 8 月 10 日法律第 145 号）において定める医療機器のサイバーセキュリティの保全については、厚生労働省医薬・生活衛生局から発出されている「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 日付け薬食機参発 0428 第 1 号、薬食安発 0428 第 1 号）等を踏まえて、医療機器の製造販売業者と必要な連携を図ること。

施設外からネットワークに接続する場合の基準については、6.11 章の規定を参照すること。

IoT セキュリティに関しては「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）が取りまとめられており、参考になる。

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。
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。
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。
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。
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。
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。
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。
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。

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。
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、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。
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。
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。
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。
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、パスワード漏えい流出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。

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。

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やアップデートが困難な場合に代替措置を講じる方法を検討し、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。

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。

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。

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。
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。
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。
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。
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。

6.6. 人的安全対策

B. 考え方

医療機関等は、情報の盗難や不正行為、情報設備の不正利用等のリスク軽減を図るため、人による誤りの防止を目的とした人的安全対策を策定する必要がある。これには守秘義務と違反時の罰則に関する規定や教育、訓練に関する事項が含まれる。

医療情報システムに関連する者として、次の 5 種類を想定する。

(a) 医師、看護師等の業務で診療に関わる情報を取り扱い、法令上の守秘義務のある者
(b) 医事課職員、事務委託者等の医療機関等の事務の業務に携わり、雇用契約の下に医療情報を取り扱い、守秘義務を負う者
(c) システムの保守事業者等、医療機関等とは雇用契約を結ばずに医療機関等の業務に携わる者
(d) 見舞い客等の医療情報にアクセスする権限を有しない第三者
(e) 診療録等の外部保存の委託においてデータ管理業務に携わる者

このうち、(a)、(b)に対する人的安全対策は、医療機関等の従業者に対する人的安全管理措置、(c)に対する人的安全対策は、事務取扱受託業者の監督及び守秘義務契約として説明する。

(d)については、そもそも医療機関等の医療情報システムに触れてはならない者であるため、物理的安全管理対策や技術的安全管理対策によって、システムへのアクセスを禁止する必要がある。また、万一、第三者によるサイバー攻撃等によってシステム内の情報漏えい等が発生した場合については、不正アクセス行為の禁止等に関する法律等の他の法令の定めるところにより適切な対処等をする必要がある。

(e)については、「外部保存」を受託する事業者等に該当するが、これに関しては詳細を 8 章に記述する。

また、近年、医療機関等を標的としたサイバー攻撃のリスクが高まっていることから、日本医療情報学会が公表している「標的型攻撃メールへの対処について」や情報処理推進機構の「対策のしおりシリーズ」等を参考に、標的型メール等のサイバー攻撃の対応について、従業者への教育を実施する必要がある。

C. 最低限のガイドライン

医療機関等の管理者は、個人情報の安全管理に関する施策が適切に実施されるよう措置するとともにその実施状況を監督するため、以下の措置をとること。

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。

(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。

(3) 従業者の退職後の個人情報保護規程を定めること。

2. 事務取扱受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。

(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。

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。

6.7. 情報の破棄

B. 考え方

医療に係る電子情報は、破棄を確実に行うことにより、破棄に際しても安全性を確保する必要がある。しかし、例えばデータベースのように情報が互いに関連して存在する場合は、一部の情報を不適切に破棄したために、その他の情報が利用不可能になる場合もあるため、注意しなくてはならない。

実際に破棄する場合に備えて、事前に破棄の手順を明確化しておくべきである。

C. 最低限のガイドライン

1. 6.2 章 C.1 で把握した情報種別ごとに破棄の手順を定めること。手順には破棄を行う条件、破棄を行うことができる従業者、具体的な破棄方法を含めること。
2. 情報処理機器自体を破棄する場合、必ず専門的な知識を有するものが行うこと。また、破棄終了後に、残存し、読み出し可能な情報がないことを確認すること。
3. 外部保存を受託する事業者等に破棄を委託した場合は、6.6 章 C.2 に従うとともに、確実に情報が破棄されたことを確認すること。
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棄に関する規定を定めること。

6.8. 医療情報システムの改造と保守

B. 考え方

医療情報システムの可用性を維持するためには、定期的なメンテナンスが必要である。メンテナンス作業には主に障害対応や予防保守、ソフトウェア改訂等があるが、特に障害対応においては、原因特定や解析等のために障害発生時のデータを利用することがある。この場合、システムのメンテナンス要員が管理者モードで直接医療情報に触れる可能性があるため、想定される脅威に対する十分な対策が必要になる。

リスク分析で明らかとなった改造と保守において想定される脅威からデータを守るためには、医療機関等の適切な管理の下に保守作業が実施される必要がある。そのためには、①保守事業者との守秘義務契約の締結、②保守要員の登録と管理、③作業計画報告の管理、④作業時の医療機関等の関係者による監督等の運用面を中心とする対策が必要である。

保守作業によっては保守事業者からさらに外部の事業者に再委託されることが考えられる。そのため、保守事業者との契約の締結に当たっては、再委託する事業者への個人情報保護の徹底等について医療機関等と保守事業者の契約と同等の契約を求めることも重要である。

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。
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。
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。
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。
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。
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。

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。
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。
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。

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。
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。
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。
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。
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。
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ること。

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

情報又は情報機器の持ち出しについては組織的な対策が必要となり、組織として情報又は情報機器の持ち出しをどのように取り扱うかという方針が必要である。また、小規模な医療機関等であって、組織的な情報管理体制を行っていない場合でも、可搬媒体や情報機器を用いた情報の持ち出しは想定されることから、リスク分析を実施し、対策を検討しておくことが必要である。

この際留意すべきは、可搬媒体や情報機器による情報の持ち出し特有のリスクである。情報を持ち出す場合は、可搬媒体や情報機器の盗難、紛失、置き忘れ等の人による不注意、過誤のリスクの方が、医療機関等に設置されている医療情報システム自体の脆弱性等のリスクよりも相対的に大きくなる。

したがって、情報又は情報機器の持ち出しについては、組織的な方針を定めた上で、人的安全対策を施す必要がある。

ノートパソコンや、タブレット、スマートフォン等を用いて医療情報システムにログインする場合においても、二要素認証を用いることが望ましい。利用者の識別・認証に係る説明や留意点については、6.5 章の記載を参照すること。

また、以降のガイドラインと内容は重複するが、タブレット PC 及びスマートフォンを用いる場合の守るべき事項をまとめると以下のようになる。

- 機器自体の管理を、運用管理規程を定めて実施すること。盗難・紛失を早期に発見することはもちろんのこと、不要なアプリの存在や、パスワードの設定が適切であること等を定期的に確認しなければならない。
- 端末自体の起動パスワード等の設定は必須であり、パスワードを用いる場合、パスワードは容易に推定されることがないものとし、かつ定期的な変更を行わなければならない。
- 端末内に患者等の情報が保存されている場合、あるいはアクセス先に存在する患者等の情報を表示や編集できる場合は、その機能を持つアプリ自体にもパスワードを設定し、端末内に情報が存在する場合は暗号化しなければならない。
- 業務に用いる機能に影響を与えないために、必要最小限のアプリ以外はインストールしないこと。OS のメモリ管理機能で、メモリを隔離して他のアプリの影響を受けないアプリが構築可能な場合は、確実にメモリ隔離ができることを確認することが必要である。
- ネットワークは 6.11 章の基準を満たしたもの以外は利用しないこと。特に公衆無線 LAN はリスクが大きいため、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、6.11 章の基準に則った利用を認める。また、自動的に公衆無線 LAN に接続してしまう端末も存在するので、業務アプリ起

動時に VPN 接続を確立しない場合は、公衆無線 LAN への自動接続機能を切る必要がある。

- 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（以下「BYOD」(Bring Your Own Device) という。）は、上記の要件を実現するために、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こと、あるいは、技術的対策として、他のアプリケーション等からの影響を遮断しつつ、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し、OS レベルで管理領域を分離すること、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、適切な対策を選択・採用し、十分な安全性が確保された上で行う必要がある。コンピュータウイルスや不適切な設定のされたソフトウェアにより、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るため、管理されていない端末での BYOD は行わない。管理者が BYOD によるコスト・利便性とリスクを評価して検討することが求められる。
- 覗き見防止対策の実施が望ましい。

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。
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。
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。
4. 運用管理規程で定めた盗難、紛失時の対応を従業者等に周知徹底するとともに、教育を実施すること。
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。
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。
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。
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、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。

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。
10. 個人保有の情報機器（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。

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。
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。
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。
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。

6.10. 災害、サイバー攻撃等の非常時の対応

B. 考え方

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。また、サイバー攻撃の場合は、自医療機関の診療等への影響だけでなく、他医療機関へ影響が波及することもあり、適切な対応が求められる。このような事態に可能な限り対応するためには、普段から想定されるあらゆるレベルの異常時について、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（BCP：Business Continuity Plan）と呼ぶ。

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る。

医療機関等全体の BCP は本ガイドラインの範疇を超えるため、ここでは自然災害やサイバー攻撃による IT 障害等の非常時に、医療情報システムが通常の状態で使用ができない事態に陥った場合における医療情報システムの BCP や留意事項について述べる。ただし、医療機関等全体の BCP の一部として医療サービスの提供が最優先されるように、整合性のある対策にならなければならないことはいうまでもない。

(1) 非常時における事業継続計画

非常事態が発生している最中では適切な意思決定は望み難いので、事前にできるだけ多くの意思決定を準備しておくことが望ましい。非常事態を事前に適切に分類することは難しく、可能な限り下記の事項・フェーズごとに計画内容を事前演習等で検証することが望ましい。

① BCP として事前に周知しておく必要がある事項
② BCP 実行フェーズ
③ 業務再開フェーズ
④ 業務回復フェーズ
⑤ 全面復旧フェーズ
⑥ BCP の見直し

(2) 医療情報システムの非常時使用への対応

① 非常時用ユーザアカウントの用意

停電、火災、洪水への対策と同様に、正常なユーザ認証が不可能な場合の対応が必要である。医療情報システムは使用可能であっても、使用者側の状況が定常時とは著しく違い、正規のアクセス権限者による操作が望めない場合に備えなくてはならない。例えば、ブレークグラスとして知られた方法では、非常時の使用に備えたユーザアカウントを用意し、患者データへのアクセス制限が医療サービス低下を招かないように配慮して

いる。ブレークグラスでは、非常時用ユーザアカウントの通常時の明示的な封印、使用状態に入ったことの周知、使用の痕跡を残すこと、定常状態に戻った後は新しい非常時ユーザアカウントへ変更することを基本としている。

② 非常時の運用に対応する機能の実装

災害時は、通常時とは異なる人の動きが想定される。例えば、災害時は、受付での患者登録を経ないような運用を考慮する等、必要に応じて非常時の運用に対応した機能を実装する必要がある。

上記のような非常時使用への対応機能の用意は、関係者に周知され非常時に適切に用いる必要があるが、逆にリスクが増えることに繋がる可能性がある。不用意な使用を行わないために管理・運用は慎重でなくてはならない。

(3) サイバー攻撃を受けた際の対応

医療情報システムに不正ソフトウェアが混入するなどによるサイバー攻撃を受けた場合、以下の対応等を行う必要が生じる場合がある。これらに備え、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必要がある。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。また、非常時に備えたバックアップの実施と管理については、7.2 章及び 7.3 章も参照すること。

- 攻撃を受けたサーバ等の遮断や他の医療機関等への影響の波及の防止のための外部ネットワークの一時切断
- 他の機器への混入拡大の防止や情報漏えいの抑止のための当該混入機器の隔離
- 他の機器への波及の調査等被害の確認のための業務システムの停止
- バックアップからの重要なファイルの復元（重要なファイルは数世代バックアップを複数の方式（追記可能な設定がなされた媒体と追記不能設定がなされた媒体の組み合わせ、端末及びサーバ装置やネットワークから切り離したバックアップデータの保管等）で取得することが重要である）

医療情報システムは一般に複雑で、医療機関の規模等によって運用やバックアップの方法も様々である。一様に指針を示すことは困難であるが、医療機関においては、重大な障害により医療提供体制に支障が生じた場合であっても、診療の継続や早期に業務を再開することが求められる。バックアップに関しては、全ての情報をバックアップから復元するのではなく、ある程度のリスクを許容することで運用が容易になり、確実に対

応することが可能になることも多い。診療のために直ちに必要な情報をあらかじめ十分に検討し、確実に運用できるバックアップを確保しておくことが必要である。

特に、一定規模以上の病院や、地域で重要な機能を果たしている医療機関等においては、ランサムウェア等のようにデータ自体を利用不能にするようなものについてバックアップデータまで被害が拡大することのないよう、バックアップを保存する電磁的記録媒体等の種類、バックアップの周期、世代管理の方法、バックアップデータを保存した媒体を端末及びサーバ装置やネットワークから切り離して保管すること等を考慮して対策を講じることが強く求められる。例えば、日次でバックアップを行う場合、数世代（少なくとも 3 世代）確保し、遅くとも 3 世代目以降はネットワーク的あるいは論理的に書き込み不可の状態にする等の対策が必要となる。

また、サイバー攻撃によるセキュリティインシデントが発生した際、数世代前までのバックアップデータは既に不正ソフトウェアが混入による影響が及んでいる可能性が高く、不用意にバックアップデータから復旧することで被害を繰り返し、場合によっては被害を拡大することになりかねない。不正ソフトウェア対策を講じつつ復旧するための手順をあらかじめ検討し、BCP として定めておくとともに、サイバー攻撃を想定した対処手順が適切に機能することを訓練等により確認することなども重要である。

なお、復旧するにあたっては、侵入継続と被害拡大を防ぐ観点から、

・バックドアを残さない
・無効にされたセキュリティ機能を復旧する
・同じ脆弱性を突かれて侵入されない
・他の脆弱性を突かれない
・不正に作成されたり、盗まれたりした ID・パスワード等を使われないようにする

などの方策をとり、同様の被害を繰り返したり、盗まれた情報による被害を拡大させたりしないようにする必要がある。なお専門的な知見に関して、情報処理推進機構が、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。

(4) 非常時に備えたセキュリティ体制の整備

非常時やサイバー攻撃などに対して、的確に対応できるためにセキュリティ体制を医療機関等においても構築することが求められる。非常時等において必要な原因関係の調査、必要なセキュリティ対応等に関する指揮、所管官庁等への報告などの体制については、医療の継続を確保する観点からも平常時から明確にする必要がある。

また、一定規模以上の病院や、地域で重要な機能を果たしている医療機関等においては、そのために情報セキュリティ責任者(CISO)等の設置や、緊急対応体制（CSIRT 等）を整備するなどが強く求められる。

また、日頃から脆弱性情報を収集し、速やかに対策を行える体制を整えておくことが

必要である。

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。
2. 非常時における対応に関する教育及び訓練を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。
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。
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。
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、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）

6.11. 外部のネットワーク等を通じた個人情報を含む医療情報の交換に当たっての安全管理

B. 考え方

本章では、組織の外部と情報交換を行う場合に、個人情報保護及びネットワークのセキュリティに関して特に留意すべき項目について述べる。医療機関等において外部と個人情報を含む医療情報を交換する場合、医療情報システムを医療機関等が管理する内部ネットワークを通じて外部のネットワークに接続して利用することが考えられる。

ネットワークを利用して医療情報を外部と交換する場合、送信元から送信先に確実に情報を送り届ける必要があり、「送付すべき相手に」、「正しい内容を」、「内容を盗み見されない方法で」送付しなければならない。すなわち、送信元の送信機器から送信先の受信機器までの間の通信経路において上記内容を担保する必要があり、送信元や送信先を偽装する「なりすまし」や送受信データに対する「盗聴」及び「改ざん」、通信経路への「侵入」及び「妨害」等の脅威から守らなければならない。

医療機関はこれらの脅威に留意したうえで、医療情報システムに接続するネットワーク、機器、サービス等を適切に選定し、6.2.3 章のリスク分析を行い、6.2 章の情報セキュリティマネジメントシステム（ISMS）を実践することが必要である。

なお、可搬媒体や紙を用いて情報を搬送する場合は、付則 1 及び 2 を参照すること。

(1) 医療機関等における留意事項

医療機関等において、ネットワークを利用して医療情報を外部と交換する際の留意事項としては、

・「盗聴」の危険性に対する対応
・「改ざん」の危険性への対応
・「なりすまし」の危険性への対応
・適切な暗号鍵の管理

などが挙げられる。

(2) 選択すべきネットワークのセキュリティの考え方

医療情報を内部ネットワークと外部ネットワークを接続して交換する際、ネットワークの接続形態により選択すべきセキュリティの考え方が異なる。

・クローズドなネットワークで接続する場合
・オープンなネットワークで接続する場合
・モバイル端末等を使って医療機関等の外部から接続する場合

の 3 つの場合について、それぞれ接続先の医療機関等のネットワーク構成や経路設計によって、意図しない情報漏えいが起こる可能性について留意し、確認する責務がある。

①クローズドなネットワークで接続する場合

ここで述べるクローズドなネットワークとは、業務に特化された専用のネットワーク網のことを指す。この接続の場合、インターネットには接続されていないネットワーク網として利用されているものと定義する。このようなネットワークを提供する接続形式としては、「①専用線」、「②公衆網」、「③閉域 IP 通信網」がある。

これらのネットワークは基本的にインターネットに接続されないため、通信上における「盗聴」、「侵入」、「改ざん」、「妨害」等の危険性は比較的低い。ただし、「(1)医療機関等における留意事項」で述べた物理的手法による情報の盗聴の危険性は必ずしも否定できないため、伝送しようとする情報自体の暗号化については考慮が必要である。また、複数拠点の接続により内部ネットワークが拡張する場合、内部トラフィックにおける脅威の拡散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・パッチ等を適切に適用する等を行うことが求められる。

②オープンなネットワークで接続する場合

インターネットによる接続形態である。この場合、通信経路上では、「盗聴」、「侵入」、「改ざん」、「妨害」等の様々な脅威が存在するため、十分なセキュリティ対策を実施することが必須である。また、医療情報そのものの暗号化の対策を行わなければならない。すなわち、オブジェクト・セキュリティの考え方に沿った対策を施す必要がある。

オープンなネットワークで接続する場合であっても、電気通信事業者とクラウドサービス事業者が、これらの脅威の対策のためネットワーク経路上のセキュリティを担保した形態でサービス提供することもある。医療機関等がこのようなサービスを利用する場合は、通信経路上の管理責任の大部分をこれらの事業者に委託できる。そのため、契約等で管理責任の分界点を明確にした上で利用することも可能である。

一方で、医療機関等が独自にオープンなネットワークを用いて外部と個人情報を含む医療情報を交換する場合は、管理責任のほとんどは医療機関等に委ねられるため、医療機関等の判断で導入する必要がある。技術的な安全性についても自ら責任を持って担保できるよう、これら脅威に対する十分なセキュリティ対策を実施する必要がある。

オープンなネットワーク接続を用いる場合、ネットワーク経路上のセキュリティの考え方は、「OSI（Open Systems Interconnection）階層モデル※」で定義される 7 階層のうち、どの階層でセキュリティを担保するかによって異なってくる。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 2 月）が参考になる。

※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

IPsec もしくは新たな技術によりそれと同等以上の安全性が担保されている VPN 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 の利用が求められる。

IPsec や TLS を採用する場合でも、その端末にオープンネットワークに対する開放されたポートがある場合には、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）等による攻撃からの防護について、適切な対策を実施する必要がある。

③モバイル端末等を使って医療機関等の外部から接続する場合

ここでは、携帯電話・PHS やノートパソコン、スマートフォン、タブレット等の、モバイル端末を用いて、医療機関等の外部から医療機関等内部のネットワークに接続する場合のセキュリティ要件を整理しておく。

外部からの接続については、6.8 章で述べた保守用途でのアクセス、医療機関等の職員による業務上のアクセス、さらには本節「(4)　患者等に診療情報等を提供する場合のネットワークに関する考え方」で述べた患者等からのアクセス等、様々なケースが想定される。

したがって、実際の接続において利用されるモバイル端末とネットワークの接続サービス及びそれらの組み合わせが、本章で説明する接続形態のどれに該当するかを明確に識別することが重要になる。具体的な接続方法との関係では以下の対応が必要である。

携帯電話・PHS 網を経由して、電気通信事業者の提供するサービスを利用してインターネットへ接続するケースでは、「②オープンなネットワークで接続されている場合」に相当する。したがって、セキュリティ上の要件は、そこでの記述を適用する必要がある。オープンなネットワークを経由するので、「(1)医療機関等における留意事項」で述べたオブジェクト・セキュリティとチャネル・セキュリティを担保するための対策が必要である。

オープンなネットワークを通じて閉域ネットワークへ接続するケースでは、「Ⅰ．クローズドなネットワークで接続する場合」における「③閉域 IP 通信網で接続されている場合」に相当するため、セキュリティ上の要件は、そこでの記述を適用する必要がある。クローズ

なネットワークを経由するため、比較的安全性は高い。

閉域ネットワークに到達するまでにオープンなネットワーク（インターネット）を経由する場合、サービス提供者によってはこの間でのチャネル・セキュリティが確保されないこともあり得る。チャネル・セキュリティの確保を閉域ネットワークの採用に期待してネットワークを構成する場合には、事前にサービス提供者との契約をよく確認して、チャネル・セキュリティが確実に確保されるようにしておく必要がある。

なお、ここで述べたようなモバイル接続形態に関連するセキュリティ要件に加え、医療機関等の外部で情報にアクセスするという行為自体に特有のリスクが存在する。

例えば、機密情報が格納されたモバイル端末の盗難や紛失等の管理面のリスク、さらには公共の場所で情報を閲覧することによる他者からの覗き見等による機密漏えいのリスク等である。

(3) 従業者による外部からのアクセスに関する考え方

医療機関等の職員がテレワークを含めて自宅等から医療情報システムへのアクセスすることを許可することもあり得る。このような場合のネットワークに関わる安全管理の要件は既に述べたが、アクセスに用いる PC 等の機器の安全管理も重要であり、私物の PC のような非管理端末であっても、一定の安全管理が可能な技術的対策を講じられなければならない。加えて、外部からのアクセスに用いる機器の安全管理を運用管理規程で定めることが重要ではあるが、その場合に考慮すべき点が 3 つある。

- PC 等といっても、その安全管理対策を確認するためには一定の知識と技能が必要で、職員にその知識と技能を要求することは難しい。
- 運用管理規程で定めたことが確実に実施されていることを説明するためには適切な運用の点検と監査が必要であるが、外部からのアクセスの状況を点検、監査することは通常は困難である。
- 医療機関等の管理が及ばない私物の PC や、極端な場合は不特定多数の人が使用する PC を使用する場合はもちろん、医療機関等の管理下にある機器を必要に応じて使用する場合であっても、異なる環境で使用していれば想定外の影響を受ける可能性がある。

したがって、医師不足等に伴う医療従事者の過剰労働等に対応するために、従業者による外部からのアクセスを行う場合は、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の導入を検討するとともに、運用等の要件にも相当な厳しさが求められる。

(4) 患者等に診療情報等を提供する場合のネットワークに関する考え方

診療情報等の開示が進む中、ネットワークを介して患者（又は家族等）に診療情報等を提供したり、医療機関内の診療情報等を閲覧させる可能性も出てきた。本ガイドラインは、医療機関等の間における医療情報の交換を想定しているが、患者等に対する診療情報等の提供も十分想定される状況にある。患者等に診療情報等を提供する場合には、ネットワークのセキュリティ対策のみならず、医療機関等内部の医療情報システムのセキュリティ対策、診療情報等の主体者となる患者等へ危険性や提供目的の納得できる説明、また非 IT に関わる各種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した上で実施しなくてはならない。

C. 最低限のガイドライン

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閉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に確認すること。
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. 医療機関等の間の情報通信には、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に確認すること。
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、使用する場合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。

D. 推奨されるガイドライン

1. 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。

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

A. 制度上の要求事項

「電子署名」とは、電磁的記録（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるものをいう。以下同じ。）に記録することができる情報について行われる措置であって、次の要件のいずれにも該当するものをいう。

一　当該情報が当該措置を行った者の作成に係るものであることを示すためのものであること。

二　当該情報について改変が行われていないかどうかを確認することができるものであること。

（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）

B. 考え方

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・保存が可能となった。

近年、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）に加え、リモート署名（クラウド上のサーバに利用者（電子署名法第 2 条第 2 項における自らが行う電子署名についてその業務を利用する者をいう。以下同じ。）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）や、クラウド技術を活用した立会人型電子署名（利用者の指示に基づき電子署名サービス提供事業者（電子署名法に規定する電子署名に関するサービスを提供する者のうち、立会人型電子署名に関するサービスを行う者をいう。以下同じ。）自身の署名鍵による暗号化等を行う電子署名）を用いたサービスが登場しているが、A 項の要件を満たすものについては、電子署名法における電子署名に該当する。なお、利用者と認証局あるいは電子署名サービス提供事業者の間で行われる本人確認（利用者の実在性、本人性、利用者個人の申請意思の確認及び当人認証）等のレベルや電子署名サービス提供事業者内部で行われるプロセスのセキュリティレベルは様々であることから、各サービスの利用に当たっては、当該各サービスを利用して締結する契約等の性質や、利用者間で必要とする本人確認レベルに応じて、適切なサービスを選択することが求められる。立会人型電子署名の選択に当たっては、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）」も参照すること。

また、7 章及び 9 章の対象となる文書は、正当な権限で作成された記録であり、虚偽入力、書換え、消去及び混同が防止され、かつ、第三者から見て作成の責任の所在が明確であるこ

とが求められる。電子署名法第3条では、電子文書（デジタル情報）について、本人すなわち当該電子文書の作成名義人による電子署名（これを行うために必要な符号及び物件を適正に管理することにより、本人だけが行うことができることとなるものに限る。）が行われていると認められる場合には、当該作成名義人が当該電子文書を作成したことが推定されることを定めている。

医療分野における電子署名に係る争訟が生じた場合に備え、立証責任を軽減したい医療機関等においては、十分な暗号強度を有し他人が容易に同一の鍵を作成できないものであることや、電子署名が本人の意思に基づき行われたものであること等の措置を講ずる手段も存在することに留意すること。立会人型電子署名の選択に当たっては、総務省・法務省・経済産業省から令和2年9月4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3条に関するQ&A）」も参照すること。

さらに、医療分野においては、処方箋のように、医師等の有資格者に作成が求められる文書が医師法等の法令で定められている場合がある。これらに関しては、多くはその証明として記名・押印が求められており、記名・押印をすることは、本人の証明だけでなく、有資格者としての当該行為に対する責務も示すことになる。当該資格者による行為であることの証明を電子的に担保する場合の考え方を「Nonrepudiation（否認防止）」と呼び、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で、それを担保することが可能となる。

また特に、医療に係る文書では一定期間、信頼性を持って署名を検証できることが必要である。電子署名は紙媒体への署名や記名・押印と異なり、「A. 制度上の要求事項」の一、二は厳密に検証することが可能である反面、電子証明書等の有効期限が過ぎたり、失効させた場合は検証できないという特徴がある。さらに、電子署名の技術的な基礎となっている暗号技術は、解読法やコンピュータの演算速度の進歩につれて次第に脆弱化が進み、中長期的にはより強固な暗号アルゴリズムへ移行することも求められる。

したがって、電子署名を付与する際はこのような点を考慮し、電子証明書の有効期間や失効、また暗号アルゴリズムの脆弱化の有無によらず、法定保存期間等の一定の期間、電子署名の検証が継続できる必要がある。また、対象文書は行政の監視等の対象であり、施した電子署名が行政機関等によっても検証できる必要がある。デジタルタイムスタンプ技術を利用した長期署名方式の標準化が進み、長期的な署名検証の継続が可能となり、ISO規格として制定されている（ISO 14533-1：2014 CMS利用電子署名(CAdES)の長期署名プロファイル、ISO 14533-2:2021 XML 署名利用電子署名(XAdES)の長期署名プロファイル、ISO 14533-3:2017 PDF長期署名プロファイル(PAdES)、ISO 14533-4:2019 proof of existence objects)。

医療情報の保存期間は、生物由来製剤に係る文書として20年以上の長期にわたるものもあり、システム更新や検証システムの互換性等の観点からも、標準技術を用いる等して適切に保存することが望ましい。したがって、例えば、前述の標準技術を用い、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にすることが重要である。

C. 最低限のガイドライン

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。

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）。

- 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ておくこと。④の場合、次に掲げる事項が適切に行われていることについて事業者が確認を行うこと。

－　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できることが必要である。

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。

7. 電子保存の要求事項について

本章の規定は、3.1 章において、7 章及び 9 章の対象として挙げられている文書等を電子保存する場合に適用される。

法的に保存義務のある文書等を電子的に保存するためには、日常の診療や監査等において、電子化した文書を支障なく取り扱えることが当然担保されなければならないことに加え、その内容の正確さについても訴訟等における証拠能力を有する程度のレベルを担保することが要求される。誤った診療情報は、患者の生死に関わることであるので、電子化した診療情報の正確さの確保には最大限の努力が必要である。また、診療に係る文書等の保存期間について各種の法令に規定されているため、所定の期間において安全に保存されていなくてはならない。

これら法的に保存義務のある文書等の電子保存の要件として、真正性、見読性及び保存性の確保の 3 つの基準が示されている。それらの要件に対する対応は運用面と技術面の両方で行う必要がある。運用面、技術面のどちらかに偏重すると、高コストの割に要求事項が充分満たされなかったり、煩わしさばかりが大きくなったりすることが想定されるため、両者のバランスが取れた総合的な対策が重要である。各医療機関等は、自らの機関の規模や各部門システム、既存システムの特性を良く見極めた上で、最も効果的に要求を満たすよう、運用面と技術面の対応を検討すること。

7.1. 真正性の確保について

A. 制度上の要求事項

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。

（e-文書法省令　第 4 条第 4 項第 2 号）

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。

（施行通知　第 2　2（3）②）

「診療録等の記録の真正性、見読性及び保存性の確保の基準を満たさなければならないこと。」

（外部保存改正通知　第２　１（1））

B. 考え方

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をいう。

また、ネットワークを通じて外部に保存を行う場合、委託元の医療機関等から委託先の外部保存施設への転送途中で、診療録等が書換えや消去されないように、また他の情報との混同が発生しないよう、注意する必要がある。

したがって、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は、医療機関等に保存する場合の真正性の確保に加えて、ネットワーク特有のリスクにも留意しなくてはならない。

具体的には、虚偽入力、書換え、消去及び混同を防止するためには、故意又は過失、使用する機器・ソフトウェアなどそれぞれの原因に対して、運用も含めて対応すること。

また作成の責任の所在を明確にすることも求められる。具体的には入力者及び確定者の識別・認証、記録の確定、識別情報の記録、更新履歴の保存において、対策を講じる必要がある（代行入力を行う場合には、確定者の識別・認証において留意が必要である）。

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。

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。

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。

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。

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。

【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】

医療機関等に保存する場合の最低限のガイドラインに加え、次の事項が必要となる。

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。

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。

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。

なお、これらの具体的要件については、6.11 章「外部のネットワーク等を通じた個人情報を含む医療情報の交換に当たっての安全管理」を参照すること。

7.2. 見読性の確保について

A. 制度上の要求事項

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。

（e-文書法省令　第4条第4項第1号）

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。

（施行通知　第2　2（3）①）

「診療録等の記録の真正性、見読性及び保存性の確保の基準を満たさなければならないこと。」

（外部保存改正通知　第2　1（1））

B. 考え方

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である。e-文書法の精神によれば、画面上での見読性が確保されていることが求められているが、要求によっては対象の情報の内容を直ちに書面に表示できることが求められることもあるため、必要に応じてこれに対応することを考慮する必要がある。

また、何らかのシステム障害が発生した場合においても、診療に重大な支障がない最低限の見読性を確保する対策も考慮に含める必要がある。特に、災害等の非常時には、システムが完全に停止してしまうおそれもあるため、定期的なバックアップを実施して、診療録等に記載された患者情報を確認できるようにしておくことが望ましい。

保存していた情報が毀損した場合等は、可能な限り速やかな復旧に努め、「診療」、「患者への説明」、「監査」、「訴訟」等の要求に応える見読性の確保を図らなければならない。

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。

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。

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。

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。

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。

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すること。

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。

【ネットワークを通じて外部に保存する場合】

医療機関等に保存する場合の推奨されるガイドラインに加え、次の事項が必要となる。

4. 緊急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

緊急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すること。

5. 緊急に必要になるとまではいえない診療録等の見読性の確保

緊急に必要になる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。

7.3. 保存性の確保について

A. 制度上の要求事項

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。

（e-文書法省令　第4条第4項第3号）

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。

（施行通知　第2　2（3）③）

「診療録等の記録の真正性、見読性及び保存性の確保の基準を満たさなければならないこと。」

（外部保存改正通知　第2　1（1））

B. 考え方

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をいう。

診療録等の情報を電子的に保存する場合に、保存性を脅かす原因として、例えば下記のものが考えられる。

・コンピュータウイルスや不適切なソフトウェア等による情報の破壊及び混同等
・不適切な保管・取扱いによる情報の滅失、破壊
・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
・媒体・機器・ソフトウェアの不整合による情報の復元不能
・障害等によるデータ保存時の不整合

保存性の確保に対するこれらの脅威をなくすために、それぞれの原因に対する技術面及び運用面での各種対策を施す必要がある。

具体的には、不正ソフトウェアによる情報の破壊及び混同等、不適切な保管・取扱いによる情報の滅失、破壊、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、媒体・機器・ソフトウェアの不整合による情報の復元不能、障害等によるデータ保存時の不整合など原因に対する技術面及び運用面での対策が求められる。

なおサイバー攻撃等については、6.10章を参照すること。

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。
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。
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ら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。
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らない機能を備えること。

【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】

医療機関等に保存する場合の最低限のガイドラインに加え、次の事項が必要となる。

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は対応を維持しなくてはならない。

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。

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。

8. 診療録及び診療諸記録を外部に保存する際の基準

※ 本章の規定は、3.2 章において、8 章の対象として挙げられている文書等を電子保存する場合に適用される。

診療録等の保存場所に関する基準は、2 つの場合に分けて考える必要がある。一つは電子媒体により外部保存を行う場合で、もう一つは紙媒体のままで外部保存を行う場合である。さらに、電子媒体の場合、ネットワークを通じて外部保存を行う場合が特に規定されていることから、実際には次の 3 つに分けて考える必要がある。

(1) 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
(2) 電子媒体による外部保存を磁気テープ、CD-R、DVD-R 等の可搬媒体で行う場合
(3) 紙やフィルム等の媒体で外部保存を行う場合

このうち電子媒体による外部保存を、可搬媒体を用いて行う場合については、付則 1 へ移動したのでそちらを参照すること。

また紙媒体のままで外部保存を行う場合については、付則 2 へ移動したのでそちらを参照すること。

ネットワークを経由して診療録等を電子媒体によって外部に保存する場合は、6.11 章を参照し、安全管理に関して医療機関等が主体的に責任を負い適切に推進することが求められる。

8.1. 電子保存の 3 基準の遵守

3 基準の記載については、7.1 章、7.2 章及び 7.3 章にそれぞれ統合したので、そちらを参照すること

8.2. 運用管理規程

A. 制度上の要求事項

外部保存を行う病院､診療所等の管理者は､運用管理規程を定め､これに従い実施すること。

（外部保存改正通知　第３　1）

B. 考え方

外部保存に係る運用管理規程を定めることが求められており、考え方及び具体的なガイドラインは、6.3 章の項を参照すること。

また、その際の責任のあり方については、4 章を参照すること。

なお､既に電子保存の運用管理規程を定めている場合には､外部保存に対する項目を適宜修正・追加等すれば足りると考えられる。

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

A. 制度上の要求事項

（安全管理措置）

個人情報取扱事業者は、その取り扱う個人データの漏えい、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。

（個人情報保護法　第 23 条）

電気通信回線を通じて外部保存を行う場合にあっては、保存に係るホストコンピュータ、サーバ等の情報処理機器が医療法第 1 条の 5 第 1 項に規定する病院又は同条第 2 項に規定する診療所その他これに準ずるものとして医療法人等が適切に管理する場所、行政機関等が開設したデータセンター等、及び医療機関等が民間事業者等との契約に基づいて確保した安全な場所に置かれるものであること。

（外部保存改正通知　第２　１　(2)）

B. 考え方

特に「２　医療機関等が外部の事業者に対して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」には、データセンター等の情報処理を受託する事業者が総務省・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」の要求事項を満たしていることを確認し、契約等でその遵守状況を明らかにしなくてはならない。なお、データセンターについては、個人情報保護法の改正により、民間事業者においても安全管理に関する法律上の義務が生じるようになったことから、行政機関等が開設したデータセンター等と契約に基づいて確保した安全な場所である民間事業者が開設したデータセンターとは区別せず、同一の要求事項が求められる。

外部保存を受託する事業者の選定基準や情報の扱い、情報の提供にあたっては、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、又は医療機関等が外部の事業者等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のそれぞれにおいて、適切に対応する必要がある。

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）が起こら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に、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）が起こら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。

(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

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。

8.4. 個人情報の保護

A. 制度上の要求事項

（安全管理措置）

個人情報取扱事業者は、その取り扱う個人データの漏えい、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。

（委託先の監督）

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。

（個人情報保護法　第 23 条、第 25 条）

患者のプライバシー保護に十分留意し、個人情報の保護が担保されること。

（外部保存改正通知　第２　１（3））

B. 考え方

ネットワークを通じて外部に保存する場合、医療機関等の管理者の権限や責任の範囲が、自機関等の施設とは異なる施設や電気通信事業者にも及ぶために、より一層、個人情報の保護に配慮することが必要となる。

なお、患者の個人情報の保護等に関する事項は、診療録等の法的な保存期間が終了した場合や、外部保存を受託する事業者との契約期間が終了した場合でも、個人情報が存在する限り配慮する必要がある。また、バックアップ情報における個人情報の取扱いについても、同様の運用体制が求められる。

ネットワークを通過する際の個人情報保護は、通信手段の種類によって個別に考える必要がある。通信手段の違いによる情報の秘匿性確保に関しては 6.11 章「 (2)選択すべきネットワークのセキュリティの考え方」で触れているので、そちらを参照すること。

C. 最低限のガイドライン

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。

8.5. 責任の明確化

A. 制度上の要求事項

外部保存は、診療録等の保存の義務を有する病院、診療所等の責任において行うこと。また、事故等が発生した場合における責任の所在を明確にしておくこと。

（外部保存改正通知　第２　１（4））

本項の記載は、4 章及び 6.11 章に考え方を集約したため、それらを参照すること。

8.5.1. 留意事項

ネットワークを通じて外部保存を行い、これを外部保存を受託する事業者において可搬媒体に保存する場合にあっては、付則 1 に掲げる事項についても十分留意すること。

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

※ 本章の規定は、「3.1　7 章及び 9 章の対象となる文書について」において、7 章及び 9 章の対象として挙げられている文書等をスキャナ等により電子化して保存する場合に適用される。

本章は法令等で作成又は保存を義務付けられている診療録等を一旦紙等の媒体で作成されたものを受領又は保存又は運用した後に、スキャナ等で電子化し、保存又は運用する場合の取扱いについて記載している。電子カルテ等へシェーマ（人体図）を入力する際に、紙に描画しスキャナやデジタルカメラで入力する場合等は本章の対象ではないため、7 章の真正性の確保を参照すること。

A. 制度上の要求事項

民間事業者等が、法第三条第一項の規定に基づき、別表第一の一及び二の表の上欄に掲げる法令のこれらの表の下欄に掲げる書面の保存に代えて当該書面に係る電磁的記録の保存を行う場合並びに別表第一の四の表の上欄に掲げる法令の同表の下欄に掲げる電磁的記録による保存を行う場合は、次に掲げる方法のいずれかにより行わなければならない。

一　（略）

二　書面に記載されている事項をスキャナ（これに準ずる画像読取装置を含む。）により読み取ってできた電磁的記録を民間事業者等の使用に係る電子計算機に備えられたファイル又は磁気ディスク等をもって調製するファイルにより保存する方法

（e-文書法省令　第 4 条）

9.1. 共通の要件

B. 考え方

スキャナ等による電子化を行う具体的事例は、次の 2 つの場面を想定することができる。

(1) **電子カルテ等の運用において、診療の大部分が電子化された状態で行われている一方、他院から紙やフィルムでの診療情報提供書等の受け入れが避けられない事情がある場合**

紙の調剤済み処方箋も、これに相当する。

(2) **電子カルテ等の運用を開始し、電子保存を施行したが、施行前の診療録等が紙やフィルムで残り、一貫した運用ができない場合、又はオーダエントリシステムや医事システムのみの運用であって、紙等の保管に窮している場合**

この節では、この上記のいずれにも該当する、つまり「診療等の都度スキャナ等で電子化して保存する場合」及び「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」に共通の対策を記載する。

なお、スキャナ等で電子化した場合、どのように精密な技術を用いても、元の紙等の媒体の記録と同等にはならない。また、スキャニングにより、保存できない有用な情報などがある場合もある。したがって、一旦紙等の媒体で運用された情報をスキャナ等で電子化することは慎重に行う必要がある。電子情報と紙等の情報が混在することで、運用上著しく障害がある場合等に限定すべきである。その一方で、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極めて有効であり、可能であれば外部への保存も含めて検討されるべきである。このような場合の対策に関しては、9.5 章で述べる。

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。

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

B. 考え方

電子カルテ等の運用において、診療の大部分が電子化された状態で行われていながら、他院から紙やフィルムの媒体による診療情報提供書等を受け入れることが避けられない事情がある場合、媒体が混在することにより医療安全上の問題が生じるおそれがある。このような場合等に、診療等の都度スキャナ等による電子化が実施されることが想定される。

この場合、「9.1　共通の要件」を満たした上で、さらに改ざん動機が生じないと考えられる時間内に、適切に電子化が行われることが求められる。

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。

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

B. 考え方

電子カルテ等の運用を開始し、電子保存を施行したが、施行前の診療録等が紙やフィルムの媒体で残り、一貫した運用ができない場合が想定される。このような場合、改ざん動機の生じる可能性の低い、9.2 章の「診療等の都度スキャナ等で電子化して保存する場合」の状況と異なり、説明責任を果たすために相応の対策を行うことが求められる。そのため、9.1 章の要求を全て満たした上で、患者等の事前の同意を得て、厳格な監査を実施することが必要である。

C. 最低限のガイドライン

9.1 章の対策に加えて、以下の対策を実施すること。

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。
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
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。
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。

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

B. 考え方

紙の調剤済み処方箋の電子化とは、紙の処方箋に記名押印又は署名を行い調剤済みとしたものを電子化することをいう。

なお、紙の処方箋を薬局で受け取った場合、調剤済みとなるまでは電子化したものを原本としてはならない（誤った運用例：薬局で紙の処方箋を受け付けた時点で電子化し、それを原本として調剤を行い、薬剤師の電子署名をもって調剤済みとする等）。

なお、調剤終了時までは特段の問題なく経過した処方箋であっても、その後に内容の修正が発生することを完全には否定できない（例：記載事項を確認したものの修正を忘れた場合等）。そのため、一旦電子化した紙の調剤済み処方箋であっても、その修正が発生する可能性がある。

C. 最低限のガイドライン

9.1 章の対策に加えて、次に掲げる対策を実施すること。

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。
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。

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

B. 考え方

紙等の媒体で扱うことが著しく利便性を欠くためにスキャナ等で電子化するが、紙等の媒体の保存は継続して行う場合、電子化した情報はあくまでも参照情報であり、保存義務等の要件は課せられない。しかしながら、個人情報保護上の配慮は同等に行う必要があり、またスキャナ等による電子化の際に医療に関する業務等に差し支えない精度の確保も必要である。

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。

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。
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。

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。

10. 運用管理について

「運用管理」において運用管理規程は管理責任や説明責任を果たすために極めて重要であり、運用管理規程は必ず定めなければならない。

A. 制度上の要求事項

(1) 「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」

Ⅰ　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

ーーー個人情報の取扱いに関する明確かつ適正な規則を策定し、それらを対外的に公表することが求められる。

ーーー個人情報の取扱いに関する規則においては、個人情報に係る安全管理措置の概要、本人等からの開示等の手続き、第三者提供の取扱い、苦情への対応等について具体的に定めることが考えられる。

Ⅳ　7（2）①個人情報保護に関する規程の整備、公表

ーーー個人情報保護に関する規程を整備し、ーーー。

個人データを取り扱う情報システムの安全管理措置に関する規程等についても同様に整備を行うこと。

(2) その他の要求事項

診療録等の電子保存を行う場合の留意事項

1　施設の管理者は診療録等の電子保存に係る運用管理規程を定め、これに従い実施すること。

2　運用管理規程には以下の事項を定めること。

(1) 運用管理を総括する組織・体制・設備に関する事項

(2) 患者のプライバシー保護に関する事項

(3) その他適正な運用管理を行うために必要な事項

（施行通知　第 3）

電子媒体により外部保存を行う際の留意事項

1　外部保存を行う病院、診療所等の管理者は運用管理規程を定め、これに従い実施すること。なお、既に診療録等の電子保存に係る運用管理規程を定めている場合は、適宜これを修正すること。

2　1 の運用管理規程の策定にあたっては、診療録等の電子保存に係る運用管理規程で必要とされている事項を定めること。

（外部保存改正通知　第 3）

B. 考え方

医療機関等には規模、業務内容等に応じて様々な形態があり、運用管理規程もそれに伴い様々な様式・内容があると考えられるので、ここでは、本書の 4 章から 9 章の記載に従い、定めるべき管理項目を記載している。1.に電子保存する・しないに拘らず必要な一般管理事項を、2.に電子保存のための運用管理事項を、3.に外部保存のための運用管理事項を、4.にスキャナ等を利用した電子化、5.に運用管理規程の作成に当たっての手順を記載している。

電子保存を行う医療機関等は 1.、2.及び 4.の管理事項を、電子保存に加えて外部保存をする医療機関等では、さらに 3.の管理事項を合わせて採用する必要がある。

運用管理規程等の作成に際しては、以下の文書を参照することが有用である。

- 監査証跡の取り組み方については、「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）を参考にすること。
- 技術的対応の検討のための情報収集には、6.2 章 B で紹介している「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　チェックリスト」を参考にすること。

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

(1)　総則

a　理念（基本方針と管理目的の表明）

b　対象情報

(a) 医療情報システムで扱う全ての情報のリストアップ

(b) 安全管理上の重要度に応じた分類

(c) 医療リスク分析

c　医療情報システムにおいて採用し変更をフォローすべき標準規格

(2)　管理体制

a　システム管理者、機器管理者、運用責任者、安全管理者、個人情報保護責任者等

b　マニュアル・契約書等の文書の管理体制

c　監査体制と監査責任者

d　患者及びシステム利用者からの苦情・質問の受け付け体制

e　事故対策時の責任体制

f　システム利用者への教育・訓練等の周知体制

(3)　管理者及び利用者の責務

a　システム管理者や機器管理者、運用責任者の責務

b　監査責任者の責務

c　利用者の責務

(a) 監査証跡の取り組み方については、「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）を参考にすること。

(4)　一般管理における運用管理事項

a　来訪者の記録・識別、入退の制限等の入退管理規程

b　情報保存装置、アクセス機器の設置区画の管理・監視規程

c　情報へのアクセス権限の決定方針

d　個人情報を含む記録媒体の管理（保管・授受等）規程

e　個人情報を含む媒体の廃棄の規程

f　リスクに対する予防措置、発生時の対応方法

g　医療情報システムの安全に関する技術的と運用的対策の分担を定めた文書の管理規程

h　システムの導入に際して、技術的に対応するか、運用によって対応するかを判定し、その内容を文書化し管理する旨の規程

(a) 技術的対応の検討のための情報収集には、6.2 章 B で紹介している「『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』ガイドチェックリスト」を参考にすること。

i　技術的安全対策規程

(a) 利用者識別と認証の方法

(b) IC カード等セキュリティ・デバイス配布の方法

(c) 情報区分とアクセス権限管理及び人事異動等に伴う見直し

(d) アクセスログ取得と監査の手順

(e) 時刻同期の方法

(f) 不正ソフトウェア対策

(g) ネットワークからの不正アクセス対策

(h) パスワードの管理

j　IoT 機器の利用に関する事項

(a) IoT 機器の貸し出しに関するリスク受容の合意

(b) 異常時の患者及び医療機関等の役割、連絡先

(c) 異常の検知方法

(d) セキュリティ上重要なアップデートの方法

(e) 使用終了後又は停止中の不正接続対策

k　無線 LAN に関する事項

(a) 無線 LAN 設定（アクセス制限、暗号化等）

(b) 電波障害のおそれがある機器の使用制限

l 電子署名・タイムスタンプに関する規程

(a) 対象となる発行文書、電子署名付き受領文書の取扱規程、日常的運用管理規程

(5) 業務委託（システムの運用・保守・改造）の安全管理措置

a 業務委託契約における安全管理・守秘条項

b 再委託の場合の安全管理措置事項

c システム改造及び保守での医療機関等関係者による作業管理・監督、作業報告確認

(a) 保守要員専用のアカウントの作成及び運用管理

(b) 作業時のデータアクセス範囲の確認

(c) アクセスログの採取と確認

※ リモートメンテナンスには下記(7)も参照。

(6) 情報及び情報機器の持ち出しについて

a 持ち出し対象となる情報及び情報機器の規程

b 持ち出した情報及び情報機器の運用管理規程

c 持ち出した情報及び情報機器への安全管理措置

d 盗難、紛失時の対応策

e 利用者への周知徹底方法

(7) 外部の機関と医療情報を提供・委託・交換する場合

a 安全を技術的、運用的面から確認する規程

b リスク対策の検討文書の管理規程

c 情報処理を受託する事業者等との通常運用時、事故対処時それぞれでの責任分界点を定めた契約文書の管理と契約状態の維持管理規程

d リモートメンテナンスの基本方針

(a) 保守事業者によるリモートメンテナンス体制の安全性確認

e 従業者による医療機関等の外部からアクセスする場合の運用管理規程

(a) アクセスに用いる機器の安全管理

(8) 災害、サイバー攻撃等の非常時の対応

a BCP の規程における医療情報システムの項

b システムの縮退運用管理規程

c 非常時の機能と運用管理規程

d 報告先と内容一覧

(9) 教育と訓練

a マニュアルの整備

b　定期又は不定期なシステムの取扱い及びプライバシー保護やセキュリティ意識向上に関する研修

c　従業者に対する人的安全管理措置

(a) 医療従事者以外との守秘契約

(b) 従事者退職後の個人情報保護規程

(10) 監査

a　監査の内容

b　監査責任者の任務

c　アクセスログの監査

(11) 規程の見直し

a　運用管理規程の定期的見直し手順

2.　電子保存のための運用管理事項

(1)　真正性確保

a　入力者及び確定者の識別・認証

b　記録の確定手順と、識別情報の記録

c　更新履歴の保存

d　代行入力の承認記録

e　機器・ソフトウェアの品質管理、動作状況の内部監査規程

(2)　見読性確保

a　情報の所在管理

b　見読化手段の管理

c　見読目的に応じた応答時間とスループット

d　システム障害対策

(a) 冗長性

(b) バックアップ

(c) 緊急対応

(3)　保存性確保

a　ソフトウェア・機器・媒体の管理（例えば、設置場所、施錠管理、定期点検、不正ソフトウェアチェック等）

(a) 不正ソフトウェアによる情報の破壊及び混同等の防止策

b　不適切な保管・取扱いによる情報の滅失、破壊の防止策

(a) バックアップ、作業履歴管理

c　記録媒体、設備の劣化による読み取り不能又は不完全な読み取りの防止策

d　媒体・機器・ソフトウェアの不整合による復元不能の防止策

(a) システムの移行時のデータベースの不整合、機器・媒体の互換性不備に備えたシステム変更・移行時の業務計画の作成規約

(4)　相互運用性確保

a システムの改修に当たっての、データ互換性の確保策

b システムの更新に当たっての、データ互換性の確保策

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。

(1)　管理体制と責任

a　委託する事業者選定規約、選定時に「適合」と判断した根拠記載の規程

(a) 受託事業者が医療機関等以外の場合には、8.3 章に記された要件を参照すること。

(b) 医療機関等以外の外部の事業者に対して契約に基づいて確保した安全な場所に保存する場合には、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」に準拠していることを確認する規程

b　医療機関等における管理責任者

c　受託事業者への監査体制

d　受託事業者、回線事業者等との責任分界点

e　受託事業者、回線事業者等の管理責任、説明責任、定期的に見直し必要に応じて改善を行う責任の範囲を明文化した契約書等の文書作成と保管

f　不都合な事態が発生した場合における対処責任、障害部位を切り分ける責任所在を明文化した契約書等の文書作成と保管

(a) 受託事業者が医療機関等以外の場合には、「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」に記された要件を参照すること。

g　外部に保存を委託する文書の選定基準

(2)　外部保存契約終了時の処理

a　受託事業者に診療録等が残ることがない処理方法の規程

(a) 受託事業者に診療録等が残ることがないことの契約、管理者による確認

(3)　真正性確保

a　相互認証機能の採用

b　電気通信回線上で「改ざん」されていないことの保証機能

(4)　見読性確保

a　施設内保存と同項目 2（2）の確認

b　緊急に必要になることが予測される医療情報の見読性の確保手段（推奨）

c　緊急に必要になるとまではいえない医療情報の見読性の確保手段（推奨）

(5)　保存性確保

a　外部保存を受託する事業者での保存確認機能

b　施設内保存と同項目 2（3）(4)の確認

c　標準的なデータ形式及び転送プロトコルの採用（推奨）

d　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確保

(6)　診療録等の個人情報を電気通信回線で伝送する間の個人情報の保護

a　秘匿性の確保のための適切な暗号化

b　通信の起点・終点識別のための認証

(7)　診療録等の外部保存を受託する事業者内での個人情報の保護

a　外部保存を受託する事業者における個人情報保護

b　外部保存を受託する事業者における診療録等へのアクセス禁止

受託する事業者が医療機関等以外の場合には、8.3 章に記された要件を参照すること。

c　障害対策時のアクセス通知

d　アクセスログの完全性とアクセス禁止

(8)　患者への説明

a　診療開始前の説明方法

b　患者本人の理解を得ることが困難であるが診療上の緊急性がある場合の説明方法

c　患者本人の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の説明方法

(9)　受託事業者に対する監査項目

a　保存記録（内容、期間等）

b　受託事業者における管理策とその実施状況監査

4.　スキャナ等により電子化して保存する場合

(1)　スキャナ読み取りの対象文書の規程

(2)　スキャナ読み取り電子情報と原本と同等であることを担保する情報作成管理者の任命

(3)　スキャナ読み取り電子情報への作業責任者（実施者又は情報作成管理者）の電子署名法に適合した電子署名

(4)　診療等の都度、スキャンするタイミングに関する規程

(5)　過去に蓄積された文書を電子化する場合の、実施手順規程

5.　運用管理規程の作成に当たって

運用管理規程は、システムの運用を適正に行うためにその医療機関等ごとに策定されるものである。すなわち、各々の医療機関等の状況に応じて自主的な判断の下に策定されるものである。もちろん、独自に一から作成することも可能であるが、記載すべき事項の網羅性を確保することが困難なことが予想されるため、付表 1～付表 3 に運用管理規程文案

を添付する。

付表 1 は電子保存する・しないに拘らず一般的な運用管理の実施項目例、付表 2 は電子保存における運用管理の実施項目例であり、付表 3 はさらに外部保存の場合において追加すべき運用管理の実施項目例である。

したがって、外部保存の場合は、付表 1 から付表 3 の項目を運用管理規程に盛り込むことが必要となる。

「運用管理規程」が 1 冊の独立した文書である必要性はない。実際の運用に当たって使用される管理規程を定めた文書類の中に、本ガイドラインで記載され本章にまとめられた内容が記載されていれば良い。しかし、日常運用及び見直し・改定のことを考慮し、業務単位に分かりやすくまとまっていることが大事である。

運用管理規程書を作成する場合の推奨手順は以下のとおりである。

ステップ 1：全体の構成及び目次の作成

全体の章立てと節の構成を決める場合に、本章の項目と付表の「運用管理項目」、「実施項目」を参照し、医療機関等ごとの独自性を考慮する方法で全体の構成を作成する。

この際、電子保存及び外部保存のシステムに関する運用管理規程だけではなく、医療情報システム全体の総合的な運用管理規程の構成とすることが重要である。

ステップ 2：運用管理規程文の作成

運用管理規程文の作成には、付表の「運用管理規程文例」を参考にして作成する。

特に、大規模／中規模病院用と小規模病院／診療所用では、運用管理規程文の表現が大きく異なることを想定して、付表に「対象区分」欄を設けている。大規模／中規模病院の場合は、対象区分の A と B の運用管理規程文例を選択し、小規模病院／診療所の場合は、対象区分の A と C の運用管理規程文例を選択することを推奨する。

ステップ 3：全体の見直し及び確認評価

運用管理規程の全体が作成された段階で、医療機関等の内部の関係者等にレビューを行い、総合的視点で実施運用が可能か評価し改善する。

なお、運用管理規程は単に策定すれば良いというものではなく、策定（Plan）された管理規程に基づいた運用（Do）を行い、適切な監査（Check）を実施し、必要に応じて改善（Action）していかねばならない。この PDCA サイクルを適切に廻しながら、改善活動を伴う継続的な運用を行うことが重要である。

付則１　電子媒体による外部保存を可搬媒体を用いて行う場合

電子媒体による外部保存を可搬媒体を用いて行う場合、委託する医療機関等と受託する事業者はネットワークで結ばれないため、ネットワーク上の脅威に基づくなりすましや盗聴、改ざん等による情報の大量漏えいや大幅な書換え等の危険性は少なく、注意深く運用すれば真正性の確保が容易になる可能性がある。

可搬媒体による保存の安全性は、紙やフィルムによる保存の安全性と比べて概ね優れているといえる。媒体を目視しても内容が見えるわけではないので、搬送時の機密性は比較的確保しやすい。暗号化機能を有する可搬媒体等のパスワードによるアクセス制限が可能な媒体を用いればさらに機密性は増す。

したがって、一般的には付則 2 の紙媒体による外部保存の基準に準拠していれば大きな問題はないと考えられる。しかしながら、可搬媒体の耐久性の経年変化については、慎重に対応する必要がある。また、一媒体あたりに保存される情報量が極めて多いことから、媒体を遺失した際に紛失、漏えいする情報量も多くなるため、より慎重な取扱いが必要である。

なお、診療録等のバックアップ等、法令で定められている保存義務を伴わない文書を外部に保存する場合についても、個人情報保護の観点から保存義務のある文書と同等に扱うべきである。

付則 1.1　電子保存の 3 基準の遵守

A. 制度上の要求事項

診療録等の記録の真正性、見読性及び保存性の確保の基準を満たさなければならないこと。

（外部保存改正通知　第２　１（1））

B. 考え方

診療録等を医療機関等の内部に電子的に保存する場合に必要とされる真正性、見読性、保存性を確保することで概ね対応が可能と考えられるが、これに加え、搬送時や外部保存を受託する事業者における取扱いに注意する必要がある。

具体的には、以下について対応が求められる。

(1) 搬送時や外部保存を受託する事業者の障害等に対する真正性の確保
(2) 搬送時や外部保存を受託する事業者の障害等に対する見読性の確保
(3) 搬送時や外部保存を受託する事業者の障害等に対する保存性の確保

C. 最低限のガイドライン

1. 搬送時や外部保存を受託する事業者の障害等に対する真正性の確保

(1) 可搬媒体を授受する際に、明確な記録を行うこと。

可搬媒体の授受及び保存状況を確実に記録し、事故､紛失や窃盗を防止することが必要である。また、他の保存文書等との区別を行うことにより、混同を防止しなければならない。

(2) 媒体を変更したり､更新したりする際に、明確な記録を行うこと

2. 搬送時や外部保存を受託する事業者の障害等に対する見読性の確保

(1) 診療に支障が生じないようにすること

患者の情報を可搬媒体で外部に保存する場合、情報のアクセスに一定の搬送時間が必要であるが、患者の病態の急変や救急対応等に備え、緊急に診療録等の情報が必要になる場合も想定しておく必要がある。

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ることから、患者の診療情報が緊急に必要になることが予測され、搬送に要する時間が問題になるような診療に関する情報は、内部に保存するか、外部に保存するとしても、保存情報の複製又はそれと実質的に同等の内容を持つ情報を、委託する医療機関等の内部に保存しておかなければならない。

(2) 監査等に差し支えないようにすること

監査等は概ね事前に予定が判明しており、緊急性を求められるものではないことから､搬送に著しく時間を要する遠方に外部保存しない限り､問題がないと考えられる。

3. 搬送時や外部保存を受託する事業者の障害等における保存性の確保

(1) 標準的なデータ形式の採用

システムの更新等に伴う相互運用性を確保するために、データの移行が確実にできるように、標準的なデータ形式を用いることが望ましい。

(2) 媒体の劣化対策

媒体の保存条件を考慮し、例えば、磁気テープの場合、定期的な読み書きを行う等の劣化対策が必要である。

(3) 媒体及び機器の陳腐化対策

媒体や機器が陳腐化した場合、記録された情報を読み出すことに支障が生じるおそれがある。したがって、媒体や機器の陳腐化に対応して、新たな媒体又は機器に移行することが望ましい。

付則 1.2 個人情報の保護

A. 制度上の要求事項

(安全管理措置)

個人情報取扱事業者は、その取り扱う個人データの漏えい、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。

(委託先の監督)

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。
（個人情報保護法　第 23 条、第 25 条）

患者のプライバシー保護に十分留意し、個人情報の保護が担保されること。
（外部保存改正通知　第 2　1（3））

B. 考え方

平成 27 年度改正個人情報保護法が成立し、医療等分野において「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」が策定された。医療において扱われる健康情報は極めてプライバシーに機微な情報であるため、上記ガイダンスを参照し、十分な安全管理策を実施することが必要である。

診療録等が医療機関等の内部で保存されている場合は、医療機関等の管理者の統括によって、個人情報が保護されている。

しかし、可搬媒体を用いて外部に保存する場合、委託する医療機関等の管理者の権限や責任の範囲が、自施設とは異なる他施設に及ぶため、より一層の個人情報保護への配慮が必要である。

なお、患者の個人情報の保護等に関する事項は、診療録等の法的な保存期間が終了した場合や、外部保存を受託する事業者との契約期間が終了した場合でも、個人情報が存在する限り配慮する必要がある。また、バックアップ情報における個人情報の取扱いについても、同様の運用体制が求められる。

具体的には、以下についての対応が求められる。

(1) 診療録等の記録された可搬媒体が搬送される際の個人情報保護
(2) 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

C. 最低限のガイドライン

1. 診療録等の記録された可搬媒体が搬送される際の個人情報保護

診療録等を可搬媒体に記録して搬送する場合は、可搬媒体の遺失や他の搬送物との混同に注意する必要がある。

(1) 診療録等を記録した可搬媒体の遺失防止

運搬用車両を施錠する等、搬送用ケースを封印する等の処置を施すことによって、遺失の危険性を軽減すること。

(2) 診療録等を記録した可搬媒体と他の搬送物との混同の防止

他の搬送物との混同が予測される場合には、他の搬送物と別のケースや系統に分けたり、同時に搬送しないことによって、その危険性を軽減すること。

(3)　搬送業者との守秘義務に関する契約

外部保存を委託する医療機関等は保存を受託する事業者、搬送業者に対して個人情報保護法を遵守させる管理義務を負う。したがって両者の間での責任分担を明確化するとともに、守秘義務に関する事項等を契約上明記すること。

2.　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

外部保存を受託する事業者が、委託する医療機関等からの求めに応じて、保存を受託した診療録等における個人情報を検索し、その結果等を返送するサービスを行う場合や、診療録等の記録された可搬媒体の授受を記録する場合、受託する事業者に障害の発生した場合等に、診療録等にアクセスをする必要が発生する可能性がある。このような場合には、次の事項に注意する必要がある。

(1)　外部保存を受託する事業者における医療情報へのアクセスの禁止

診療録等の外部保存を受託する事業者においては、診療録等の個人情報の保護を厳格に行う必要がある。受託する事業者の管理者であっても、保存を受託した個人情報に、正当な理由なくアクセスできない仕組みが必要である。

(2)　障害発生時のアクセス通知

診療録等を保存している設備に障害が発生した場合等で、やむを得ず診療録等にアクセスをする必要がある場合も、医療機関等における診療録等の個人情報と同様の秘密保持を行うと同時に、外部保存を委託した医療機関等に許可を求めなければならない。

(3)　外部保存を受託する事業者との守秘義務に関する契約

診療録等の外部保存を受託する事業者は、法令上の守秘義務を負っていることからも、委託する医療機関等と受託する事業者、搬送業者との間での責任分担を明確化するとともに、守秘義務に関する事項等を契約に明記する必要がある。

(4)　外部保存を委託する医療機関等の責任

診療録等の個人情報の保護に関しては、最終的に診療録等の保存義務のある医療機関等が責任を負わなければならない。したがって、委託する医療機関等は、受託する事業者における個人情報の保護の対策が実施されることを契約等で要請し、その実施状況を監督する必要がある。

D. 推奨されるガイドライン

「C. 最低限のガイドライン」に加えて以下の対策を行うことが推奨される。

1.　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、診療を開始する必要がある。

(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の同意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る。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。

付則 1.3　責任の明確化

A. 制度上の要求事項

外部保存は、診療録等の保存の義務を有する病院、診療所等の責任において行うこと。また、事故等が発生した場合における責任の所在を明確にしておくこと。

（外部保存改正通知　第２　１（4））

B. 考え方

診療録等を電子的に記録した可搬媒体で外部の機関に保存する場合であっても、責任に対する考え方は 4.1 章や 4.2 章と同様に整理する必要がある。

これらの考え方に則れば、実際の管理や部分的な説明の一部を委託先の機関や搬送業者との間で分担して問題がないと考えられる。

また、万一事故が起きた場合に、患者に対する責任は、4.1 章における事後責任となり、説明責任は委託する医療機関等が負うものである。ただし、適切に善後策を講ずる責任を果たし、あらかじめ 4.2 章の責任分界点を明確にしておけば、受託する事業者や搬送業者等は、委託する医療機関等に対して契約等で定められた責任を負うことは当然であるし、法令に違反した場合はその責任も負うことになる。

具体的には、以下についての対応が求められる。

(1) 通常運用における責任の明確化
(2) 事後責任の明確化

C. 最低限のガイドライン

1. 通常運用における責任の明確化

(1) 説明責任

利用者を含めた保存システムの管理運用体制について、患者や社会に対して十分に説明する責任については委託する医療機関等が主体になって対応するという前提で、個人情報の保護について留意しつつ、実際の説明を、搬送業者や受託する事業者にさせることは問題がない。

(2) 管理責任

媒体への記録や保存等に用いる装置の選定、導入、及び利用者を含めた運用及び管理等に関する責任については委託する医療機関等が主体になって対応するという前提で、個人情報の保護について留意しつつ、実際の管理を、搬送業者や受託する事業者に行わせることは問題がない。

(3) 定期的に見直し必要に応じて改善を行う責任

可搬媒体で搬送し、外部に保存したままにするのではなく、運用管理の状況を定期的に監査し、問題点を洗い出し、改善すべき点があれば改善していかなくてはならない。

したがって、医療機関等の管理者は、現行の運用管理全般の再評価・再検討を常にこころがけておく必要がある。

2. 事後責任の明確化

診療録等の外部保存に関して、委託する医療機関等、受託する事業者及び搬送業者の間で「4.2 委託と第三者提供における責任分界」を参照しつつ、管理・責任体制を明確に規定して、次に掲げる事項を契約等で交わすこと。

(1) 委託する医療機関等で発生した診療録等を、外部に保存するタイミングの決定と一連の外部保存に関連する操作を開始する動作
(2) 委託する医療機関等と搬送（業）者で可搬媒体を授受する場合の方法と管理方法
(3) 事故等で可搬媒体の搬送に支障が生じた場合の対処方法
(4) 搬送中に情報漏えいがあった場合の対処方法
(5) 受託する事業者と搬送（業）者で可搬媒体を授受する場合の方法と管理方法
(6) 受託する事業者で個人情報を用いた検索サービスを行う場合、作業記録と監査方法、取扱い従業者等の退職後も含めた秘密保持に関する規定、情報漏えいに関して患者からの照会があった場合の責任関係
(7) 受託する事業者が、委託する医療機関等の求めに応じて可搬媒体を返送すること

ができなくなった場合の対処方法

(8) 外部保存を受託する事業者に、患者から直接、照会や苦情、開示の要求があった場合の対処方法

付則 1.4　外部保存契約終了時の処理について

診療録等が高度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、委託する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らない。

外部保存の開始には何らかの期限が示されているはずであり、外部保存の終了もこの前提に基づいて行われなければならない。期限には具体的な期日が指定されている場合もあり得るし、一連の診療の終了後〇〇年といった一定の条件が示されていることもあり得る。

いずれにしても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、処理が厳正に執り行われたかを監査しなくてはならない。また、受託する事業者も、委託する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、処理を行った旨を委託する医療機関等に明確に示す必要がある。

当然のことであるが、これらの廃棄に関わる規定は、外部保存を開始する前に委託する医療機関等と受託する事業者との間で取り交わす契約書にも明記をしておく必要がある。また、実際の廃棄に備えて、事前にソフトウェアの廃棄等の手順を明確化したものを作成しておくべきである。

委託する医療機関等及び受託する事業者双方に厳正な取扱いを求めるのは、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、そのことに十分なことに留意しなければならない。

また、患者の個人情報に関する検索サービスを実施している場合は、検索のための台帳やそれに代わるもの、及び検索記録も機密保持できる状態で廃棄しなければならない。

さらに、委託する医療機関等及び受託する事業者が負う責任は、先に述べたとおりであり、可搬媒体で保存しているからという理由で、廃棄に伴う責任を免れるのものではないことに十分留意する必要がある。

付則２　紙媒体のままで外部保存を行う場合

紙媒体とは、紙だけを指すのではなく、X線フィルム等の電子媒体ではない物理媒体も含む。検査技術の進歩等によって、医療機関等では保存しなければならない診療録等が増加しており、その保存場所の確保が困難な場合も多い。本来、法令に定められた診療録等の保存は、証拠性と同時に、有効に活用されることを目指すものであり、整然と保存されるべきものである。

一定の条件の下では、従来の紙媒体のままの診療録等を当該医療機関等以外の場所に保存することが可能になっているが、この場合の保存場所も可搬媒体による保存と同様、医療機関等に限定されていない。

しかしながら、診療録等は機密性の高い個人情報を含んでおり、また必要な時に遅滞なく利用できる必要がある。保存場所が当該医療機関等以外になることは、個人情報が存在する場所が拡大することになり、外部保存に係る運用管理体制を明確にしておく必要がある。また、保存場所が離れるほど、診療録等を搬送して利用可能な状態にするのに時間がかかるのは当然であり、診療に差し障りのないように配慮しなければならない。

さらに、紙やフィルムの搬送は注意深く行う必要がある。可搬媒体は内容を見るために何らかの装置を必要とするが、紙やフィルムは単に露出するだけで、個人情報が容易に漏出するからである。

付則 2.1　利用性の確保

A. 制度上の要求事項

診療録等の記録が診療の用に供するものであることにかんがみ、必要に応じて直ちに利用できる体制を確保しておくこと。

（外部保存改正通知　第２　２（1））

B. 考え方

一般に、診療録等は、患者の診療や説明、監査、訴訟等のために利用するが、あらゆる場合を想定して、診療録等をいつでも直ちに利用できるようにすると解釈すれば、事実上、外部保存は不可能となる。

診療の用に供するという観点から考えれば、直ちに特定の診療録等が必要な場合としては、継続して診療を行っている患者等、緊急に必要になることが容易に予測される場合が挙げられる。具体的には、以下について対応が求められる。

(1) 診療録等の搬送時間
(2) 保存方法及び環境

C. 最低限のガイドライン

1. 診療録等の搬送時間

外部保存された診療録等を診療に用いる場合、搬送の遅れによって診療に支障が生じないようにする対策が必要である。

(1) 外部保存の場所

搬送に長時間を要する機関に外部保存を行わないこと。

(2) 複製や要約の保存

継続して診療を行っている場合等で、緊急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、外部に保存する場合でも、診療に支障が生じないようコピーや要約等を内部で利用可能にしておくこと。

また、継続して診療している場合であっても、例えば入院加療が終了し、適切な退院時要約が作成され、それが利用可能であれば、入院時の診療録等自体が緊急に必要になる可能性は低下する。ある程度時間が経過すれば外部に保存しても診療に支障をきたすことはないと考えられる。

2. 保存方法及び環境

(1) 診療録等の他の保存文書等との混同防止

診療録等を必要な利用単位で選択できるよう、他の保存文書等と区別して保存し、管理しなければならない。

(2) 適切な保存環境の構築

診療録等の劣化、損傷、紛失、窃盗等を防止するために、適切な保存環境・条件を構築・維持しなくてはならない。

付則 2.2 個人情報の保護

A. 制度上の要求事項

(安全管理措置)

個人情報取扱事業者は、その取り扱う個人データの漏えい、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。

(委託先の監督)

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。

(個人情報保護法　第 23 条、第 25 条)

患者のプライバシー保護に十分留意し、個人情報の保護が担保されること。

(外部保存改正通知　第 2　2 (2))

B. 考え方

平成 27 年度改正個人情報保護法が成立し、医療等分野において「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」が策定された。医療において扱われる健康情報は極めて機微なプライバシー情報であるため、上記ガイダンスを参照し、十分な安全管理対策を実施することが必要である。

診療録等が医療機関等の内部で保存されている場合は、医療機関等の管理者（院長等）の統括によって、個人情報が保護されている。しかし、紙やフィルム等の媒体のままで外部に保存する場合、委託する医療機関等の管理者の権限や責任の範囲が、自施設とは異なる他施設に及ぶため、より一層の個人情報保護への配慮が必要である。

なお、患者の個人情報の保護等に関する事項は、診療録等の法的な保存期間が終了した場合や、外部保存を受託する事業者との契約期間が終了した場合でも、個人情報が存在する限り配慮する必要がある。また、バックアップ情報における個人情報の取扱いについても、同様の運用体制が求められる。

具体的には、以下についての対応が求められる。

(1) 診療録等が搬送される際の個人情報保護
(2) 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

C. 最低限のガイドライン

1. 診療録等が搬送される際の個人情報保護

診療録等の搬送は遺失や他の搬送物との混同について、注意する必要がある。

(1) 診療録等の封印と遺失防止

診療録等は、目視による情報の漏出を防ぐため、運搬用車両を施錠する等、搬送用ケースを封印すること。また、診療録等の授受の記録を取る等の処置を取ることによって、その危険性を軽減すること。

(2) 診療録等の搬送物との混同の防止

他の搬送物と別のケースや系統に分けたり、同時に搬送しないことによって、混同の危険性を軽減すること。

(3) 搬送業者との守秘義務に関する契約

診療録等を搬送する業者は、個人情報保護法上の守秘義務を負うことからも、委託する医療機関等と受託する事業者、搬送業者の間での責任分担を明確化するとともに、守秘義務に関する事項等を契約上、明記すること。

2. 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

診療録等の外部保存を受託する事業者においては、委託する医療機関等からの求めに応じて、診療録等の検索を行い、必要な情報を返送するサービスを実施する場合、また、診療録等の授受の記録を取る場合等に、診療録等の内容を確認したり、患者の個人情報を閲覧する可能性が生じる。

(1)　外部保存を受託する事業者内で、患者の個人情報を閲覧する可能性のある場合

診療録等の外部保存を受託し、検索サービス等を行う機関は、サービスの実施に最小限必要な情報の閲覧にとどめ、その他の情報は、閲覧してはならない。また、情報を閲覧する者は特定の担当者に限ることとし、その他の者が閲覧してはならない。

さらに、外部保存を受託する事業者は、個人情報保護法による安全管理義務の面から、委託する医療機関等と搬送業者との間で、守秘義務に関する事項や、支障があった場合の責任体制等について、契約を結ぶ必要がある。

(2)　外部保存を受託する事業者内で、患者の個人情報を閲覧する可能性のない場合

診療録等の外部保存を受託する事業者は、専ら搬送ケースや保管ケースの管理のみを実施すべきであり、診療録等の内容を確認したり、患者の個人情報を閲覧してはならない。また、これらの事項について、委託する医療機関等と搬送業者との間で契約を結ぶ必要がある。

(3)　外部保存を委託する医療機関等の責任

診療録等の個人情報の保護に関しては、最終的に診療録等の保存義務のある医療機関等が責任を負わなければならない。したがって、委託する医療機関等は、受託する事業者における個人情報の保護の対策が実施されることを契約等で要請し、その実施状況を監督する必要がある。

D. 推奨されるガイドライン

1.　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る。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。

付則 2.3　責任の明確化

A. 制度上の要求事項

外部保存は、診療録等の保存の義務を有する病院、診療所等の責任において行うこと。また、事故等が発生した場合における責任の所在を明確にしておくこと。

（外部保存改正通知　第２　２（3））

B. 考え方

診療録等を外部の機関に保存する場合であっても、責任に対する考え方は 4.1 章や 4.2 章と同様に整理する必要がある。

これらの考え方に則れば、実際の管理や部分的な説明の一部を委託先の機関や搬送業者との間で分担して問題がないと考えられる。

また、万一事故が起きた場合に、患者に対する責任は、4.1 章における事後責任となり、説明責任は委託する医療機関等が負うものである。ただし、適切に善後策を講ずる責任を果たし、あらかじめ 4.2 章の責任分界点を明確にしておけば、受託する事業者や搬送業者等は、委託する医療機関等に対して契約等で定められた責任を負うことは当然であるし、法令に違反した場合はその責任も負うことになる。

具体的には、以下についての対応が求められる。

(1) 通常運用における責任の明確化

(2) 事後責任の明確化

C. 最低限のガイドライン

1.　通常運用における責任の明確化

(1)　説明責任

利用者を含めた管理運用体制について、患者や社会に対して十分に説明する責任については委託する医療機関等が主体になって対応するという前提で、個人情報の保護について留意しつつ、実際の説明を、搬送業者や委託先の機関にさせることは問題がない。

(2)　管理責任

診療録等の外部保存の運用及び管理等に関する責任については委託する医療機関等が主体になって対応するという前提で、個人情報の保護について留意しつつ、実際の管理を、搬送業者や受託する事業者に行わせることは問題がない。

(3)　定期的に見直し必要に応じて改善を行う責任

診療録等を搬送し、外部に保存したままにするのではなく、運用管理の状況を定期的に監査し、問題点を洗い出し、改善すべき点があれば改善していかなくてはならない。

したがって、医療機関等の管理者は、現行の運用管理全般の再評価・再検討を常にこころがけておく必要がある。

2.　事後責任の明確化

診療録等の外部保存に関して、委託する医療機関等、受託する事業者及び搬送業者の間で、「4.2　委託と第三者提供における責任分界」を参照しつつ、管理・責任体制を明確に規定して、次に掲げる事項を契約等で交わすこと。

(1)　委託する医療機関等で発生した診療録等を、外部に保存するタイミングの決定と一連の外部保存に関連する操作を開始する動作
(2)　委託する医療機関等と搬送（業）者で診療録等を授受する場合の方法と管理方法
(3)　事故等で診療録等の搬送に支障が生じた場合の対処方法
(4)　搬送中に情報漏えいがあった場合の対処方法
(5)　受託する事業者と搬送（業）者で診療録等を授受する場合の方法と管理方法。
(6)　受託する事業者で個人情報を用いた検索サービスを行う場合、作業記録と監査方法
(7)　取扱い従業者等の退職後も含めた秘密保持に関する規定、情報漏えいに関して患者から照会があった場合の責任関係
(8)　受託する事業者が、委託する医療機関等の求めに応じて診療録等を返送することができなくなった場合の対処方法
(9)　外部保存を受託する事業者に、患者から直接、照会や苦情、開示の要求があった場合の対処方法

付則 2.4　外部保存契約終了時の処理について

診療録等が高度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、委託する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らない。

外部保存の開始には何らかの期限が示されているはずであり、外部保存の終了もこの前提に基づいて行われなければならない。期限には具体的な期日が指定されている場合もあり得るし、一連の診療の終了後○○年といった一定の条件が示されていることもあり得る。

いずれにしても、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、処理が厳正に執り行われたかを監査しなくてはならない。また、受託する事業者も、委託する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、処理を行った旨を委託する医療機関等に明確に示す必要がある。

当然のことであるが、これらの廃棄に関わる規定は、外部保存を開始する前に委託する医療機関等と受託する事業者との間で取り交わす契約書にも明記をしておく必要がある。また、実際の廃棄に備えて、事前にソフトウェアの廃棄等の手順を明確化したものを作成しておくべきである。

委託する医療機関等及び受託する事業者双方に厳正な取扱いを求めるのは、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、そのことに十分なことに留意しなければならない。

また、患者の個人情報に関する検索サービスを実施している場合は、検索のための台帳やそれに代わるもの、及び検索記録も機密保持できる状態で廃棄しなければならない。

さらに、委託する医療機関等及び受託する事業者が負う責任は、先に述べたとおりであり、紙媒体で保存しているからという理由で、廃棄に伴う責任を免れるのものではないことに十分留意する必要がある。