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版

平成２９年５月

厚生労働省

改定履歴

版数	日付	内容
第 1 版	平成 17 年 3 月	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」、及び平成 14 年 3 月通知「診療録等の保存を行う場所について」に基づき作成された各ガイドラインを統合。 新規に、法令に保存義務が規定されている診療録及び診療諸記録の電子媒体による保存に関するガイドライン（紙等の媒体による外部保存を含む。）及び医療・介護関連機関における個人情報保護のための情報システム運用管理ガイドラインを含んだガイドラインとして作成。
第 2 版	平成 19 年 3 月	平成 18 年 1 月の高度情報通信技術戦略本部（IT 戦略本部）から発表された「IT 新改革戦略」（平成 18 年 1 月）において、「安全なネットワーク基盤の確立」が掲げられたこと、及び平成 17 年 9 月に情報セキュリティ政策会議により決定された「重要インフラの情報セキュリティ対策に係る基本的考え方」において、医療を IT 基盤の重大な障害によりサービスの低下、停止を招いた場合、国民の生活に深刻な影響を及ぼす「重要インフラ」と位置付け、医療における IT 基盤の災害、サイバー攻撃等への対応を体系づけ、明確化することが求められたことを踏まえ、 （1）医療機関等で用いるのに適したネットワークに関するセキュリティ要件定義について、想定される用途、ネットワーク上に存在する脅威、その脅威への対抗策、普及方策とその課題等、様々な観点から医療に関わる諸機関間を結ぶ際に適したネットワークの要件を定義し、「6.10　外部と個人情報を含む医療情報を交換する場合の安全管理」として取りまとめる等の改定を実施。 （2）自然災害・サイバー攻撃による IT 障害対策等について、医療の IT への依存度等も適切に評価しながら、医療における災害、サイバー攻撃対策に対する指針として「6.9　災害等の非常時の対応」を新設して取りまとめる等の改定を実施。

第 3 版	平成 20 年 3 月	第 2 版改定後、さらに医療に関連する個人情報を取り扱う種々の施策等の議論が進行している状況を踏まえ、 (1) 「医療情報の取扱に関する事項」について、医療・健康情報を取り扱う際の責任のあり方とルールを策定し、「4　電子的な医療情報を扱う際の責任のあり方」に取りまとめる等の改定を実施。また、この考え方の整理に基づき「8.1.2　外部保存を受託する機関の選定基準及び情報の取扱いに関する基準」を改定。 (2) 「無線・モバイルを利用する際の技術的要件に関する事項」について、無線 LAN を扱う際の留意点及びモバイルアクセスで利用するネットワークの接続形態毎の脅威分析に基づき、対応指針を 6 章と 10 章の関連する個所に追記。特にモバイルで用いるネットワークについては、「6.11　外部と個人情報を含む医療情報を交換する場合の安全管理」に要件を追加。さらに、情報を格納して外部に持ち出す際の新たなリスクに対して「6.9　情報及び情報機器の持ち出しについて」を新設し、留意点を記載。
第 4 版	平成 21 年 3 月	第 3 版改定後、「医療機関や医療従事者等にとって、医療情報の安全管理には、情報技術に関する専門的知識が必要であり、さらに多大な設備投資等の経済的な負担も伴う」、「昨今の厳しい医療提供体制を鑑みれば、限りある人的・経済的医療資源は、医療機関及び医療従事者の本来業務である良質な医療の提供のために費やされるべきであり、情報化に対して過大な労力や資源が費やされるべきではない」、「他方、近年の医療の情報化の進展に伴い、個人自らが医療情報を閲覧・収集・提示することによって、自らの健康増進へ役立てることが期待されている」等の指摘がなされたことを踏まえ、より適切な医療等分野の情報基盤構築のため、 ・ 「医療分野における電子化された情報管理の在り方に関する事項」について、各所より医療情報に関するガイドラインの整合を図ることが求められていること、また、技術進歩に合わせた医療情報の取扱い方策について、物理的所在のみならず医療情報を基軸とし

		た安全管理及び運用方策等をさらに体系的に検討し、読みやすさにも配慮することとして、「3.3　取扱いに注意を要する文書等」を新設し留意点を明記、5 章を全般的に見直し「5　情報の相互運用性と標準化について」として全面改定、「6.1　方針の制定を公表」、「6.2　医療機関における情報セキュリティマネジメントシステム（ISMS）の実践」に C 項及び D 項を設置、「6.11　外部と個人情報を含む医療情報を交換する場合の安全管理」に外部からのアクセスに関する事項を追加、「7　電子保存の要求事項について」の B 項、C 項及び D 項を 7 章全体で大幅に見直し、「8.1.2 外部保存を受託する機関の選定基準及び情報の取扱いに関する基準」に情報受託者が民間事業者である場合には、経済産業省及び総務省が発出しているガイドラインに準拠することを明記、その他、技術的要件の見直し、各種省令・通知等と A 項の関係性整理等、全般的な改定を実施。
第 4.1 版	平成 22 年 2 月	平成 21 年 11 月の医療情報ネットワーク基盤検討会において、診療録等の保存を行う場所について、各ガイドラインの要求事項の遵守を前提として「「民間事業者等との契約に基づいて確保した安全な場所」へと改定すべき」とする提言が取りまとめられたことを受けて、外部保存通知の改正を行い、本ガイドラインにおいても関連する 4 章、8 章、10 章の一部を中心に改定を実施した。 4 章では「4.3　例示による責任分界点の考え方の整理」に「(4) オンライン外部保存を委託する場合」を追加した。 8 章では、「8.1.2　外部保存を受託する機関の選定基準及び情報の取扱いに関する基準」の「③医療機関等の委託を受けて情報を保管する民間等のデータセンターに保存する場合」を「③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保存する場合」とし、内容を通知に合わせて改定した。 10 章は、これらの改定に合わせて内容の整合性を図っている。

第4.2版	平成25年10月	平成25年3月に外部保存通知の一部改正が行われ、調剤済み処方せん及び調剤録等の外部保存が認められたことから、本ガイドラインにおいても関連する3章、8章、9章の一部を改定。 また、モバイル端末の普及に鑑み、機器の取扱いについて明確化するとともに、災害等の非常時の対応について、大規模災害時を想定した考え方について追記するため6章の一部を改定。 さらに、医療情報の相互運用性と標準化について、最新の技術等への対応として、5章を改定。 3章では、「3.3　調剤済み処方せんと調剤録の電子化・外部保存について」を追加した。 5章では、「5.1.1　厚生労働省標準規格」を追加した。 6章では、「6.9　情報及び情報機器の持ち出しについて」を明確化するとともに「6.10　災害等の非常時の対応」に大規模災害時を想定した考え方を追加した。 8章では、調剤済み処方せんの外部保存に関する記述を追加した。 9章では、「9.4　調剤済み処方せんをスキャナ等で電子化し保存する場合について」を追加した。
第4.3版	平成28年3月	平成28年3月に「電子処方せんの運用ガイドライン」が発出されたことを踏まえ、本ガイドラインで関連する3章、8章、9章の一部を改正した。
第5版	平成29年5月	医療機関等を対象とするサイバー攻撃の多様化・巧妙化、地域医療連携や医療介護連携等の推進、IoT 等の新技術やサービス等の普及への対応として、関連する1章、6章等を改定するとともに、第4.2版の公表以降に追加された標準規格等への対応を行った。 また、改正個人情報保護法や「医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス」等への対応を行った。（本ガイドライン6章、8章、付則1及び付則2の記載事項については、「医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス」Ⅲの 4の（4）「医療情報システムの導入及びそれに伴う情報の外部保存を行う場合の取扱い」において、本ガイドラインによることとされている。）

		1 章では、ガイドラインの対象に病院、一般診療所、歯科診療所、助産所、薬局、訪問看護ステーション、介護事業者、医療情報連携ネットワーク運営事業者等における電子的な医療情報の取扱いに係る責任者が含まれる旨を明確化した。また、改正個人情報保護法や「医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス」等を踏まえた修正を行った。 3 章では、1 章の改定を踏まえ、7 章及び 9 章の対象になり得る介護事業者の文書等について追記した。 4 章では、関連する改正個人情報保護法や「医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス」等の規定を参照した。 5 章では、厚生労働省標準規格や JAHIS 標準規約等を追加し、所要の改定を行った。 6 章では、規格の更新を受け、「6.1　方針の制定と公表」及び「6.2　医療機関等における情報セキュリティマネジメントシステム（ISMS）の実践」において所要の改定を行った。6.2 章では、「『製造業者による医療情報セキュリティ開示書』ガイド」に係る追記を行った。また、「6.5　技術的安全対策」では、利用者の識別・認証について B 項、C 項、D 項の内容を改定するとともに、上述の IoT について「(6) 医療等分野における IoT 機器の利用」を設け、C 項及び D 項を追加した。「6.6　人的安全対策」及び「6.10　災害、サイバー攻撃等の非常時の対応」では、サイバー攻撃に事前・事後の対応について、改定を行った。このことに併せて、6.10 章の章題も改定している。「6.9　情報及び情報機器の持ち出しについて」では、公衆無線 LAN や個人所有又は個人の管理下にある端末の業務利用（BYOD）の取扱い等、モバイル端末の使用時における規定を改定した。「6.11　外部と個人情報を含む医療情報を交換する場合の安全管理」では、オープンなネットワークを介した SSL/TLS 接続について C 項を追加した。「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」では、国家資格の証明が求められる文書に対する考え方や取扱いについて追記を行った。 7 章では、電子カルテ等の入力における関係者の役割や責

		任を明確化するとともに、代行入力に係る取扱いについて、「7.1　真正性の確保について」を改定した。また、将来における互換性の確保について、「7.3 保存性の確保について」改定した。 10 章は、これらの改定に合わせて所要の改定を行った。 分かりやすさの観点から、全般的な表現の修正を行った。

【目次】

1　はじめに 3
2　本指針の読み方 13
3　本ガイドラインの対象システム及び対象情報 15
3.1　7 章及び 9 章の対象となる文書について 15
3.2　8 章の対象となる文書等について 18
3.3　紙の調剤済み処方せんと調剤録の電子化・外部保存について 19
3.4　取扱いに注意を要する文書等 19
4 電子的な医療情報を扱う際の責任のあり方 21
4.1　医療機関等の管理者の情報保護責任について 22
4.2　委託と第三者提供における責任分界 23
4.2.1　委託における責任分界 24
4.2.2　第三者提供における責任分界 26
4.3　例示による責任分界点の考え方の整理 26
4.4　技術的対策と運用による対策における責任分界点 31
5　情報の相互運用性と標準化について 32
5.1　基本データセットや標準的な用語集、コードセットの利用 33
5.1.1　厚生労働省標準規格 33
5.1.2　基本データセット 34
5.1.3　用語集・コードセット 35
5.2　データ交換のための国際的な標準規格への準拠 35
5.3　標準規格の適用に関わるその他の事項 36
6　情報システムの基本的な安全管理 38
6.1　方針の制定と公表 38
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 38
6.2.1　 ISMS 構築の手順 40
6.2.2　取扱い情報の把握 42
6.2.3　リスク分析 42
6.3　組織的安全管理対策（体制、運用管理規程） 45
6.4　物理的安全対策 47
6.5　技術的安全対策 48
6.6　人的安全対策 59
6.7　情報の破棄 61
6.8　情報システムの改造と保守 62

6.9　情報及び情報機器の持ち出しについて 64
6.10　災害、サイバー攻撃等の非常時の対応 68
6.11　外部と個人情報を含む医療情報を交換する場合の安全管理 72
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 91
7　電子保存の要求事項について 94
7.1　真正性の確保について 94
7.2　見読性の確保について 103
7.3　保存性の確保について 106
8　診療録及び診療諸記録を外部に保存する際の基準 111
8.1　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 111
8.1.1　電子保存の 3 基準の遵守 111
8.1.2　外部保存を受託する機関の選定基準及び情報の取扱いに関する基準 113
8.1.3　個人情報の保護 121
8.1.4　責任の明確化 123
8.1.5　留意事項 123
8.2　電子媒体による外部保存を可搬媒体を用いて行う場合 123
8.3　紙媒体のままで外部保存を行う場合 123
8.4　外部保存全般の留意事項について 124
8.4.1　運用管理規程 124
8.4.2　外部保存契約終了時の処理について 124
8.4.3　保存義務のない診療録等の外部保存について 125
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 126
9.1　共通の要件 126
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 129
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 130
9.4　紙の調剤済み処方せんをスキャナ等で電子化し保存する場合について 131
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 131
10　運用管理について 133
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 142
付則 2　紙媒体のままで外部保存を行う場合 150
付表 1　一般管理における運用管理の実施項目例
付表 2　電子保存における運用管理の実施項目例
付表 3　外部保存における運用管理の例
付録　（参考）外部機関と診療情報等を連携する場合に取り決めるべき内容

1　はじめに

平成 11 年 4 月の通知「診療録等の電子媒体による保存について」（平成 11 年 4 月 22 日付け健政発第 517 号・医薬発第 587 号・保発第 82 号厚生省健康政策局長・医薬安全局長・保険局長連名通知）、平成 14 年 3 月通知「診療録等の保存を行う場所について」（平成 14 年 3 月 29 日付け医政発 0329003 号・保発第 0329001 号厚生労働省医政局長・保険局長連名通知、平成 17 年 3 月 31 日改正、医政発第 0331010 号、保発第 0331006 号）により、診療録等の電子保存及び保存場所に関する要件等が明確化された。その後、情報技術の進歩は目覚しく、社会的にも e-Japan 戦略・計画を始めとする情報化の要請はさらに高まりつつある。平成 16 年 11 月に成立した「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律」（平成 16 年法律第 149 号。以下「e-文書法」という。）によって原則として法令等で作成又は保存が義務付けられている書面は電子的に取り扱うことが可能となった。医療情報においても「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。）が発出された。

平成 15 年 6 月より厚生労働省医政局に設置された「医療情報ネットワーク基盤検討会」においては、医療情報の電子化についてその技術的側面及び運用管理上の課題解決や推進のための制度基盤について検討を行い、平成 16 年 9 月最終報告が取りまとめられた。

上記のような情勢に対応するために、これまでの「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ガイドライン」（平成 11 年 4 月 22 日付け健政発第 517 号・医薬発第 587 号・保発第 82 号厚生省健康政策局長・医薬安全局長・保険局長連名通知に添付。）、「診療録等の外部保存に関するガイドライン」（平成 14 年 5 月 31 日付け医政発第 0531005 号厚生労働省医政局長通知）を見直し、さらに、個人情報保護に資する情報システムの運用管理に関わる指針と e-文書法への適切な対応を行うための指針を統合的に作成することとした。平成 16 年 12 月には「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ドライン」が公表され、平成 17 年 4 月の「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。）の全面実施に際しての指針が示された。これらの事情を踏まえ、本ガイドライン初版が平成 17 年 3 月に公開された。

また、平成29年5月に、改正個人情報保護法が全面施行されることとなり、これに伴って個人情報保護委員会が「個人情報の保護に関する法律についてのガイドライン（通則編）」（平成28年個人情報保護委員会告示第6号。以下「通則ガイドライン」という。）を公表した。この通則ガイドラインを踏まえ、医療・介護分野における個人情報の取扱いに係る具体的な留意点や事例等が「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」（個人情報保護委員会、厚生労働省；平成29年4月14日）において示された。同ガイダンスでは、医療情報システムの導入及びそれに伴う外部保存を行う場合の取扱いにおいては本ガイドラインによることとされている。（本ガイドラインの6章、8章、付則1、

及び付則2が該当）

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。従って、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されたい。

本ガイドラインは、医療情報システムの安全管理やe-文書法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、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。従って、本ガイドラインを使用する場合、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、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。

改定概要

【第 2 版】

本ガイドライン初版公開（平成 17 年 3 月）後の平成 18 年 1 月、高度情報通信技術戦略本部（IT 戦略本部）から、「IT 新改革戦略」が発表された。IT 新改革戦略では、「e-Japan 戦略」に比べて医療情報の活用が重視されている。様々な医療情報による連携がメリットをもたらすものと謳い、連携の手法、またその要素技術について種々の提言がなされており、その一つに「安全なネットワーク基盤の確立」が掲げられている。

他方、平成 17 年 9 月に情報セキュリティ政策会議により決定された「重要インフラの情報セキュリティ対策に係る基本的考え方」において、医療を IT 基盤の重大な障害によりサービスの低下、停止を招いた場合、国民の生活に深刻な影響を及ぼす「重要インフラ」と位置付け、医療における IT 基盤の災害、サイバー攻撃等への対応を体系づけ、明確化することが求められた。

これらの状況を踏まえ、医療情報ネットワーク基盤検討会では、「(1) 医療機関等で用いるのに適したネットワークに関するセキュリティ要件定義」、「(2) 自然災害・サイバー攻撃による IT 障害対策等」の検討を行い、本ガイドラインの改定を実施した。

「(1) 医療機関等で用いるのに適したネットワークに関するセキュリティ要件定義」では、想定される用途、ネットワーク上に存在する脅威、その脅威への対抗策、普及方策とその課題等、様々な観点から医療に関わる諸機関間を結ぶ際に適したネットワークの要件を定義し、「6.10　外部と個人情報を含む医療情報を交換する場合の安全管理」として取りまとめている。さらには、関連個所として「8　診療録及び診療諸記録を外部に保存する際の基準」の中のネットワーク関連の要件について 6.10 章を参照すること、医療機関等における当該ネットワークの運用の指針となる「10　運用管理について」の一部改定を実施している。

また、「(2) 自然災害・サイバー攻撃による IT 障害対策等」では、医療の IT への依存度等も適切に評価しながら、医療における災害、サイバー攻撃対策に対する指針として「6.9　災害等の非常時の対応」を新設して取りまとめ、情報セキュリティを実践的に運用していくための考え方として「6.2　医療機関における情報セキュリティマネージメント（ISMS）の実践」の概念を取り入れ、「10　運用管理について」も該当個所の一部追記を行った。

なお、本ガイドライン公開後に発出、改正等がなされた省令・通知等についても制度上の要求事項として置き換えを実施している。基本的要件について変更はないが、制度上要求される法令等が変更されている点に注意されたい。

【第 3 版】

本ガイドライン第 2 版の公開により、ネットワーク基盤における安全性確保のための指標は示されたが、その後、さらに医療に関連する個人情報を取り扱う種々の施策等の議論が進行している。このような状況下においては、従来のように医療従事者のみが限定的に情報に触れるとは限らない事態も想定される。例えば、ネットワークを通じて医療情報を交換する際に、一時的に情報を蓄積するような情報処理関連事業者等が想定される。このような事業者が関係する際には明確な情報の取扱いルールが必要となる。

また、業務体系の多様化により、医療機関等の施設内だけでなく、ネットワークを通じて医療機関等の外部で業務を行うシーンも現実的なものとなってきている。

これらの状況を踏まえ、医療情報ネットワーク基盤検討会では「(1) 医療情報の取扱に関する事項」、「(2) 処方せんの電子化に関する事項」、「(3) 無線・モバイルを利用する際の技術的要件に関する事項」の検討を行い、(1) 及び (3) の検討結果をガイドライン第 3 版として盛り込んだ。

「(1) 医療情報の取扱に関する事項」では、従来、免許資格等に則り守秘義務を科せられていた医療従事者が取り扱っていた医療・健康情報が、情報技術の進展により必ずしもそれら資格保有者が取り扱うとは限らない状況が生まれてきていることに対し、取扱いのルールを策定するための検討を実施した。

もちろん、医療・健康情報を本人や取扱いが許されている医師等以外の者が分析等を実施することは許されるものではないが、情報化によって様々な関係者が関わる以上、各関係者の責任を明確にして、その責任の分岐点となる責任分界点を明確にする必要がある。

今般の検討では、その責任のあり方についての検討結果を「4　電子的な医療情報を扱う際の責任のあり方」に取りまとめた。また、この考え方の整理に基づき「8.1.2　外部保存を受託する機関の選定基準及び情報の取扱いに関する基準」を改定している。

一方、昨今の業務体系の多様化にも対応ができるように「(3) 無線・モバイルを利用する際の技術的要件に関する事項」も併せて検討を実施している。

無線 LAN は電波を用いてネットワークに接続し場所の縛られることなく利用できる半面、利用の仕方によっては盗聴や不正アクセス、電波干渉による通信障害等の脅威が存在する。また、モバイルネットワークは施設外から自施設の情報システムに接続ができ、施設外で業務を遂行できる等、利便性が高まる。しかし、モバイルアクセスで利用できるネットワークは様々存在するため、それらの接続形態ごとの脅威を分析した。

これらの検討を踏まえた対応指針を 6 章の関連する個所に追記し、特にネットワークのあり方については「6.11　外部と個人情報を含む医療情報を交換する場合の安全管理」に取りまとめを行った。

さらに、モバイル端末や可搬媒体に情報を格納して外部に持ち出すと、盗難や紛失といった新たなリスクも想定されるため「6.9　情報及び情報機器の持ち出しについて」を新設し、その留意点を述べている。

【第 4 版】

本ガイドライン第 3 版においては、医療情報を取り扱う様々な職種や事業者に対する明確な情報の取扱いルールを規定し、特に責任分界点を明確化にした。このことにより情報化の更なる進展は期待できるが、一方で医療機関や医療従事者等にとって、医療情報の安全管理には、情報技術に関する専門的知識が必要であり、さらに多大な設備投資等の経済的な負担も伴うこと、昨今の厳しい医療提供体制を鑑みれば、限りある人的・経済的医療資源は、医療機関及び医療従事者の本来業務である良質な医療の提供のために費やされるべきであり、情報化に対して過大な労力や資源が費やされるべきではないこと、他方、近年の医療の情報化の進展に伴い、個人自らが医療情報を閲覧・収集・提示することによって、自らの健康増進へ役立てることが期待されていること等の指摘がなされ、医療情報ネットワーク基盤検討会では、より適切な医療等分野の情報基盤構築のために、「(1) 医療分野における電子化された情報管理の在り方に関する事項」、「(2) 個人が自らの医療情報を管理・活用するための方策等に関する事項」について検討を行った。

このうち、(1) の「各所より医療情報に関するガイドラインの整合を図ることが求められていること、また、技術進歩に合わせた医療情報の取扱い方策について、物理的所在のみならず医療情報を基軸とした安全管理及び運用方策等をさらに体系的に検討し、読みやすさにも配慮した医療情報ガイドラインの改定を行う」事項についての検討結果をガイドライン第 4 版に盛り込んだ。概略は次のとおりである。

体系的な見直しの一環として、3 章において従前の記載では明確ではなかった「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)」等について本ガイドラインに準じて取り扱うものとして、「3.3　取扱いに注意を要する文書等」を新設している。

また、医療情報の相互運用性や標準化の重要性に鑑み、体系的な見直し及び最新の技術等への対応として従来の 5 章を全面的に見直し「5　情報の相互運用性と標準化について」として全面的な改定を加えた。

6 章では、「6.1　方針の制定と公表」において JIS Q 15001:2006 の引用によって公表すべき基本方針の項目を明示し、JIS Q 27001:2006 の引用によって安全管理方針を具体的に説明した上で「C　最低限のガイドライン」を新設した。同様に、「6.2　医療機関における情報セキュリティマネジメントシステム（ISMS）の実践」においても「C　最低限のガイドライン」及び「D　推奨されるガイドライン」を新設している。「6.11　外部と個人情報を含む医療情報を交換する場合の安全管理」においては、B 項及び D 項に従業者による外部からのアクセスに関する事項を追加している。

7 章では、電子保存に前文を追加し、要件と対策の原則を述べ、7 章全体の A 項において厚生労働省令と通知の関係を明確にした。「7.1　真正性の確保について」では、B 項の記載

を大幅に簡略化、C 項の見直しを実施し D 項を全て削除した。「7.2　見読性の確保について」でも B 項を簡略し、C 項の保存場所の区分による記載を取りやめ、整理の上、D 項に緊急に必要となることが予想される場合を追加している。「7.3　保存性の確保について」も同様に C 項、D 項で大幅な見直しを実施している。このように 7 章については、C 項、D 項において、見直し、修正が数多くなされているため注意願いたい。

また、各所より医療情報に関するガイドラインの整合を図ることが求められていることに対しては、医療情報の外部保存に関して民間事業者が実施する場合において、危機管理上の目的でという要件に変更はないが、情報受託者の事業者に対して 8 章の「診療録及び診療諸記録を外部の保存する際の基準」の中に、経済産業省及び総務省から発出されているガイドラインに準拠することを条件にして、運用と情報管理のあり方を明確化している。

その他、9 章のスキャナの要件を変更する等、全体的に技術進歩に合わせた改定、読みやすさに配慮した記述にする等して第 4 版としている。

【第 4.1 版】

本ガイドライン第 4 版の公開後、平成 21 年 7 月に総務省が「ASP・SaaS 事業者が医療情報を取り扱う際の安全管理に関するガイドライン」を策定した。加えて、平成 20 年 7 月に経済産業省が告示した「医療情報を受託管理する情報処理事業者向けガイドライン」（平成 20 年 7 月 24 日経済産業省告示第 167 号）の整備等により、外部保存に対する対応方法が明確になったとの指摘がなされ、医療情報ネットワーク基盤検討会で外部保存先の基準に関する検討を行った。

検討の結果、各ガイドラインの要求事項の遵守を前提として「「民間事業者等との契約に基づいて確保した安全な場所」へと改定すべき」とする「診療録等の保存を行う場所に関する提言」を取りまとめた。

これを受けて、外部保存通知の改正を行い、本ガイドラインにおいても関連する 4 章、8 章、10 章の一部を中心に改定を実施した。

4 章では「4.3　例示による責任分界点の考え方の整理」に「(4) オンライン外部保存を委託する場合」を追加し、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の資料や説明の提供を委託契約で定め、医療機関等としても理解する努力が必要であること、監督が必須であること、定期的に安全管理に関する状況の報告を受ける必要があることを記載した。

8 章では、「8.1.2　外部保存を受託する機関の選定基準及び情報の取扱いに関する基準」の「③医療機関等の委託を受けて情報を保管する民間等のデータセンターに保存する場合」を「③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保存する場合」とし、内容を通知に合わせて改定した。

10 章は、これらの改定に合わせて所要の改定を行った。

今般の改定は、軽微なものであるため、第 5 版とはせず第 4.1 版とした。

【第 4.2 版】

本ガイドライン第 4.1 版の公開後、平成 25 年 3 月に「診療録等の保存を行う場所について」（平成 14 年 3 月 29 日付け医政発第 0329003 号・保発第 0329001 号厚生労働省医政局長・保険局長連名通知）の一部改正がなされ、調剤済み処方せん及び調剤録等の外部保存が認められたことから、これを踏まえ、本ガイドラインにおいても、関連する 3 章、8 章、9 章の一部を改正した。

また、モバイル端末の普及に鑑み、機器の取扱いについて明確化するとともに、災害等の非常時の対応について大規模災害時を想定した考え方について追記するため 6 章の一部を改定し、さらに、医療情報の相互運用性と標準化について、最新の技術等への対応として、5 章の一部を改定した。

3 章では、調剤録（薬剤師法第 28 条第 2 項に基づき調剤録への記入が不要とされた場合の調剤済み処方せんを含む。）を外部保存する場合においても、従前と同様に薬局開設者の責任において行うことや、他薬局の調剤録と明確に区分し、薬局ごと、個別に管理する必要がある旨を記載した。

また、「3.3　調剤済み処方せんと調剤録の電子化・外部保存について」の事項を追加し、現在、処方せんの電子的な発行は認められていないことから、調剤済み処方せんの電子化については、必然的に、紙の処方せんに記名押印又は署名を行い調剤済みとしたものを、9 章に示すスキャナ等により電子化して保存する方法となることを明確化した。

さらに、電子保存の対象が「調剤済み処方せん」のみであることから、紙の処方せんを薬局で受け取った後においても、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ことを明確化した。

なお、調剤終了後に修正が発生した場合、既に電子化された調剤済み処方せんに対して、過去の電子署名の検証が可能な状態で、電子的に修正し、薬剤師の電子署名を付すことが必要となることを明確化した。

5 章では、最新の技術等へ対応するため「5.1.1　厚生労働省標準規格」の事項を追加し、厚生労働省標準規格について追記するほか、所要の改定を行った。

6 章では「6.9　情報及び情報機器の持ち出しについて」の事項に、スマートフォンやタブレットのようなモバイル端末の普及を鑑み、機器を取り扱う際の要件を明確化する記述を追加するとともに「6.10　災害等の非常時の対応」の事項に、大規模災害時を想定した事業継続計画（BCP：Business Continuity Plan）の作成等の考え方について記述した。

8 章では、現在、処方せんの電子的な発行は認められていないことから、調剤済み処方せんを紙媒体のままで外部保存する場合のほか、9 章に示すスキャナ等により電子化して保存する場合は、電子媒体による外部保存が可能となる旨を記述した。

9 章では、「9.4　調剤済み処方せんをスキャナ等で電子化し保存する場合について」の事項を追加し、3 章の改定に合わせて所要の記述を追記した。

今般の改定は、軽微なものであるため、第 5 版とはせず第 4.2 版とした。

【第 4.3 版】

平成 28 年 3 月「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）の一部を改正し、処方せんの電磁的記録による保存、作成及び交付を可能とするとともに、電子処方せんの運用や地域医療連携の取組みを進め、できるだけ早く国民がそのメリットを享受できるように「電子処方せんの運用ガイドライン」を策定した。

これを踏まえ、処方せんの電磁的記録による取扱いの運用は、「電子処方せんの運用ガイドライン」を参照するものとし、本ガイドラインで処方せんに関連する記述がある 3 章、8 章、9 章の一部を改正した。

3 章では、これまで処方せんの電子的発行は認められていない旨、記述していたが、省令の改正に合わせて該当部分を削除した。これに伴い、調剤済み処方せんの取扱いを定めた 3.3 章を「紙」の調剤済み処方せんの扱いとして明確にした。また、電子化された調剤済み処方せんの外部保存は 8 章で、紙媒体をスキャンして保存する場合は 9.4 章での取扱いとなるため、一部記載を改定の上、その旨を追記している。

今般の改定は、処方せんの電磁的記録による保存、作成及び交付等が可能となったことに伴う限定的な改定であるため、第 5 版とはせず第 4.3 版とした。

【第 5 版】

本ガイドライン第 4 版の公表以降、医療等分野並びに医療情報システムを取り巻く環境は大きく変化している。個人や組織に関する情報や金銭等の窃取を目的としたサイバー攻撃が多様化・巧妙化し、医療機関等がその標的となる事例も現れるようになった。また、地域医療連携や医療介護連携等の推進を背景に、これまで医療情報に触れる機会の少なかった組織や団体が電子的な医療情報を日常的に取り扱うようになっている。「IoT（モノのインターネット）」と称される新技術やサービス等の普及も著しく、今後の技術の進展が期待されるものの、医療等分野は新たなセキュリティリスクに直面している。

こうした動向を踏まえ、このたび本ガイドラインにおいても、関連する 1 章や 6 章を改定するとともに、第 4.2 版の公表以降に追加された標準規格等への対応を行った。

また、改正個人情報保護法及びその関連法令等が平成 29 年 5 月に全面施行されることを踏まえ、本ガイドラインにおける参照記述を修正する等、上記法令等や「医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス」への対応を行った。

1 章では、本ガイドラインの対象に、病院、一般診療所、歯科診療所、助産所、薬局、訪問看護ステーション、介護事業者、医療情報連携ネットワーク運営事業者等における電子的な医療情報の取扱いに係る責任者が含まれることを明確化した。また、改正個人情報保護法及びその関連法令等並びに「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」踏まえた改定を行う。

3 章では、1 章の改定を踏まえ、介護事業者が取り扱う文書が 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場合には、7 章及び 9 章の対象となる旨を追記し、該当し得る文書等を列挙した。

4 章では、改正個人情報保護法で新たに規定された事項について、関係資料を参照する。また、「4.2.2　第三者提供における責任分界」において、改正個人情報保護法で新たに規定された義務について関係資料を参照する。

5 章では、新たに加わった厚生労働省標準規格や JAHIS 標準規約等を追記した。「5.3　標準規格の適用に関わるその他の事項」では、日本 IHE 協会の「地域医療連携における情報連携基盤技術仕様」について記述を設けた。

6 章では、規格の更新を受け、「6.1　方針の制定と公表」及び「6.2　医療機関等における情報セキュリティマネジメントシステム (ISMS) の実践」において所要の改定を行った。併せて、6.2 章ではリスク分析等の参考として「『製造業者による医療情報セキュリティ開示書』ガイド」に関する記述を加えた。また、「6.5　技術的安全対策」では、攻撃手法の高度化により、ID・パスワードのみの組み合わせによる認証では十分な安全性を確保できない現状に鑑みて、認証に係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 2 要素認証を実装することを求め、かつパスワード要件について追記したほか、上述の IoT について「(6) 医療等分野における IoT 機器の利用」を設け、情報セキュリティの観点から医療機関等が順守すべき事項を規定した。

「6.6　人的安全対策」及び「6.10　災害、サイバー攻撃等の非常時の対応」では、医療機関等を対象とするサイバー攻撃のリスクが顕在化していることへの対応として、サイバー攻撃等への事前及び事後の対応や連絡先等について規定を設けた。このことに併せて、6.10 章の章題も改定している。

在宅医療や訪問看護等、医療機関等の職員が業務にモバイル端末を用いる機会が増加していることを踏まえ、「6.9　情報及び情報機器の持ち出しについて」において、公衆無線 LAN、個人所有又は個人の管理下にある端末の業務利用（BYOD）の取扱い等、モバイル端末の使用時における順守事項を明確化した。

「6.11　外部と個人情報を含む医療情報を交換する場合の安全管理」では、オープンなネットワークを介した SSL/TLS 接続における順守事項や留意点を示した。

「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」では、国家資格の証明が求められる文書に対する考え方や取扱いについて追記を行った。

7 章では、「7.1　真正性の確保について」において、電子カルテ等の入力における関係者の役割や責任をより明確にするとともに、代行入力を行う場合の記録確定に当たって順守すべき事項を追記した。また、「7.3　保存性の確保について」において、医療機関等が文書を保存する際の将来の互換性の確保について、規定を設けた。

10 章は、これらの改定に合わせて所要の改定を行った。

このほか、分かりやすさの観点から、全般的な表現の修正を行った。

2　本指針の読み方

本指針は次のような構成になっている。医療機関等の責任者、情報システム管理者、またシステム導入業者が、それぞれ関連する個所を理解した上で、個々の対策を実施することを期待する。

なお、本指針では医療情報、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】

個人情報を含むデータを扱う全ての医療機関等で参照される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の指針を含んでいる。

【8 章】

保存義務のある診療録等を医療機関等の外部に保存する場合の指針を含んでいる。

【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。

【10 章】

運用管理規程に関する事項について記載されている。

なお、本指針の大部分は法律、厚生労働省通知、他の指針等の要求事項に対して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、以下の項目に分けて説明をしている。

A.　制度上の要求事項

法律、通知、他の指針等を踏まえた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について記載している。

C.　最低限のガイドライン

A 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事項を記載している。

この項の対策にあっては、医療機関等の規模により実際の対策が異なる可能性や、幾つかの対策の中の一つを選択する場合もあるが、付表の運用管理表を活用し、適切な具体的対策を採用する等して、実施しなければならない。

D. 推奨されるガイドライン

実施しなくても要求事項を満たすことは可能であるが、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、最低限のシステムでは使用されていない技術で、その技術を使用する上で一定の留意が必要となる場合についての記載も含んでいる。

なお、巻末の 3 つの付表は安全管理上の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く、採用した技術的対策に対して、相応した運用的な対策を行う必要がある。付表は以下の項目からなる。

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

各機関等は実施項目に対して採用した技術的対策に応じた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運用されていることを確認することで、実施項目が達成されることになる。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、自らの機関等で運用可能な範囲の技術的対策を選択することが可能である。一般に運用的対策の比重を大きくすれば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。従って、適切なバランスを求めることは非常に重要なので、これらの付表を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

本ガイドラインは保存システムだけではなく、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」は対象となる文書等が一部限定されている。

3.1　7 章及び 9 章の対象となる文書について

医療に関する文書は、法令等によって保存、作成及び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 章の対象となる文書は、法令による保存、作成及び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、e-文書法省令、「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 28 年 3 月 31 日付け医政発 0331 第 31 号・薬生発 0331 第 11 号・保発 0331 第 27 号・政社発 0331 第 2 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。）で定められた下記の文書等を対象としている。

なお、※で示す処方せんについては施行通知第二　2（4）の要件を充足する必要がある。

1　医師法（昭和 23 年法律第 201 号）第 24 条の診療録
2　歯科医師法（昭和 23 年法律第 202 号）第 23 条の診療録
3　保健師助産師看護師法（昭和 23 年法律第 203 号）第 42 条の助産録
4　医療法（昭和 23 年法律第 205 号）第 51 条の 2 第 1 項及び第 2 項の規定による事業報告書等及び監事の監査報告書の備置き
5　歯科技工士法（昭和 30 年法律第 168 号）第 19 条の指示書
6　薬剤師法（昭和 35 年法律第 146 号）第 28 条の調剤録
7　外国医師又は外国歯科医師が行う臨床修練に係る医師法第 17 条及び歯科医師法第 17 条の特例等に関する法律（昭和 62 年法律第 29 号）第 11 条の診療録
8　救急救命士法（平成 3 年法律第 36 号）第 46 条の救急救命処置録
9　医療法施行規則（昭和 23 年厚生省令第 50 号）第 30 条の 23 第 1 項及び第 2 項の帳簿
10　保険医療機関及び保険医療養担当規則（昭和 32 年厚生省令第 15 号）第 9 条の診療録等（作成については、同規則第 22 条）
11　保険薬局及び保険薬剤師療養担当規則（昭和 32 年厚生省令第 16 号）第 6 条の調剤録（作成については、同規則第 5 条）
12　臨床検査技師等に関する法律施行規則（昭和 33 年厚生省令第 24 号）第 12 条の 3 の書類（作成については、同規則第 12 条第 14 号及び第 15 号）

13　医療法（昭和 23 年法律第 205 号）第 21 条第 1 項の記録（同項第 9 号に規定する診療に関する諸記録のうち医療法施行規則第 20 条第 10 号に規定する処方せんに限る。）、第 22 条の記録(同条第 2 号に規定する診療に関する諸記録のうち医療法施行規則第 21 条の 5 第 2 号に規定する処方せんに限る。)、同法第 22 条の 2 の記録（同条第 3 号に規定する診療に関する諸記録のうち医療法施行規則第 22 条の 3 第 2 号に規定する処方せんに限る。)、及び同法第 22 条の 3 の記録（同条第 3 号に規定する診療及び臨床研究に関する諸記録のうち医療法施行規則第 22 条の 7 第 2 号に規定する処方せんに限る。）※

14　薬剤師法（昭和 35 年法律第 146 号）第 26 条、第 27 条の処方せん※

15　保険薬局及び保険薬剤師療養担当規則（昭和 32 年厚生省令第 16 号）第 6 条の処方せん※

16　医療法（昭和 23 年法律第 205 号）第 21 条第 1 項の記録（医療法施行規則第 20 条第 10 号に規定する処方せんを除く。)、同法第 22 条の記録（医療法施行規則第 21 条の 5 第 2 号に規定する処方せんを除く。)、同法第 22 条の 2 の記録（医療法施行規則第 22 条の 3 第 2 号に規定する処方せんを除く。）及び同法第 22 条の 3 の記録（医療法施行規則第 22 条の 7 第 2 号に規定する処方せんを除く。）

17　麻薬及び向精神薬取締法（昭和 28 年法律第 14 号）第 27 条第 6 項の処方せん※

18　歯科衛生士法施行規則（平成元年厚生省令第 46 号）第 18 条の歯科衛生士の業務記録

19　医師法（昭和 23 年法律第 201 号）第 22 条の処方せん※

20　歯科医師法（昭和 23 年法律第 202 号）第 21 条の処方せん※

21　保険医療機関及び保険医療養担当規則（昭和 32 年厚生省令第 15 号）第 23 条第 1 項の処方せん※

22　診療放射線技師法（昭和 26 年法律第 226 号）第 28 条第 1 項の規定による照射録

また、介護事業者が取り扱う以下の文書は、e-文書の対象範囲であり、文書の内容に医療情報が含まれることがある。以下に挙げた文書に限らず、介護事業者が取り扱う文書が 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場合には、7 章及び 9 章の規定を遵守する必要がある。

1　指定居宅サービス等の事業の人員、設備及び運営に関する基準（平成 11 年厚生省令第 37 号）第 73 条の 2 第 2 項の規定による訪問看護計画書及び訪問看護報告書

2　指定居宅サービス等の事業の人員、設備及び運営に関する基準（平成 11 年厚生省令第 37 号）第 154 条の 2 第 2 項（第 155 条の 12 において準用する場合を含む。）の規定による短期入所療養介護計画

3　指定居宅サービス等の事業の人員、設備及び運営に関する基準（平成 11 年厚生省令第 37 号）第 191 条の 2 第 2 項及び第 192 条の 11 第 2 項の規定による特定施設サービス

計画

4　指定介護老人福祉施設の人員、設備及び運営に関する基準（平成 11 年厚生省令第 39 号）第 37 条第 2 項の規定による施設サービス計画

5　介護老人保健施設の人員、施設及び設備並びに運営に関する基準（平成 11 年厚生省令第 40 号）第 38 条第 2 項の規定による施設サービス計画

6　指定訪問看護の事業の人員及び運営に関する基準（平成 12 年厚生省令第 80 号）第 30 条第 2 項の規定による訪問看護指示書、特別訪問看護指示書、精神科訪問看護指示書、精神科特別訪問看護指示書及び在宅患者訪問点滴注射指示書

7　指定介護予防サービス等の事業の人員、設備及び運営並びに指定介護予防サービス等に係る介護予防のための効果的な支援の方法に関する基準（平成 18 年厚生労働省令第 35 号）第 73 条第 2 項の規定による介護予防訪問看護計画書及び介護予防訪問看護報告書

8　指定介護予防サービス等の事業の人員、設備及び運営並びに指定介護予防サービス等に係る介護予防のための効果的な支援の方法に関する基準（平成 18 年厚生労働省令第 35 号）第 194 条第 2 項（第 210 条において準用する場合を含む。）の規定による介護予防短期入所療養介護計画

9　指定介護予防サービス等の事業の人員、設備及び運営並びに指定介護予防サービス等に係る介護予防のための効果的な支援の方法に関する基準（平成 18 年厚生労働省令第 35 号）第 244 条第 2 項及び第 261 条第 2 項の規定による介護予防特定施設サービス計画

10　指定地域密着型サービスの事業の人員、設備及び運営に関する基準（平成 18 年厚生労働省令第 34 号）第 3 条の 40 第 2 項の規定による定期巡回・随時対応型訪問介護看護計画及び訪問看護報告書

11　指定地域密着型サービスの事業の人員、設備及び運営に関する基準（平成 18 年厚生労働省令第 34 号）第 40 条の 15 第 2 項の規定による療養通所介護計画

12　指定地域密着型サービスの事業の人員、設備及び運営に関する基準（平成 18 年厚生労働省令第 34 号）第 128 条第 2 項の規定による地域密着型特定施設サービス計画

13　指定地域密着型サービスの事業の人員、設備及び運営に関する基準（平成 18 年厚生労働省令第 34 号）第 156 条第 2 項（第 169 条において準用する場合を含む。）の規定による地域密着型施設サービス計画

14　指定地域密着型サービスの事業の人員、設備及び運営に関する基準（平成 18 年厚生労働省令第 34 号）第 181 条第 2 項の規定による居宅サービス計画、看護小規模多機能型居宅介護計画及び看護小規模多機能型居宅介護報告書

なお、法令等による作成や保存が定められている文書のうち、e-文書法の対象範囲となっていない医療関係文書等については、例え電子化したとしても、その電子化した文書等を

法令等による作成や保存が定められた文書として扱うことはできないため、別途作成・保存が義務付けられる。

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。）で定められた下記の文書等を対象としている。

1　医師法（昭和 23 年法律第 201 号）第 24 条に規定されている診療録
2　歯科医師法（昭和 23 年法律第 202 号）第 23 条に規定されている診療録
3　保健師助産師看護師法（昭和 23 年法律 203 号）第 42 条に規定されている助産録
4　医療法（昭和 23 年法律第 205 号）第 46 条第 2 項に規定されている財産目録、同法第 51 条の 2 第 1 項に規定されている事業報告書等、監事の監査報告書及び定款又は寄附行為、同条第 2 項に規定されている書類及び公認会計士等の監査報告書並びに同法第 54 条の 7 において読み替えて準用する会社法（平成 17 年法律第 86 号）第 684 条第 1 項に規定されている社会医療法人債原簿及び同法第 731 条第 2 項に規定されている議事録
5　医療法（昭和 23 年法律第 205 号）第 21 条、第 22 条及び第 22 条の 2 に規定されている診療に関する諸記録及び同法第 22 条及び第 22 条の 2 に規定されている病院の管理及び運営に関する諸記録
6　診療放射線技師法（昭和 26 年法律第 226 号）第 28 条に規定されている照射録
7　歯科技工士法(昭和 30 年法律第 168 号)第 19 条に規定されている指示書
8　薬剤師法（昭和 35 年法律第 146 号）第 27 条に規定されている調剤済みの処方せん
9　薬剤師法第 28 条に規定されている調剤録
10　外国医師等が行う臨床修練に係る医師法第 17 条等の特例等に関する法律（昭和 62 年法律第 29 号）第 11 条に規定されている診療録
11　救急救命士法（平成 3 年法律第 36 号）第 46 条に規定されている救急救命処置録
12　医療法施行規則（昭和 23 年厚生省令第 50 号）第 30 条の 23 第 1 項及び第 2 項に規定されている帳簿
13　保険医療機関及び保険医療養担当規則（昭和 32 年厚生省令第 15 号）第 9 条に規定されている診療録等
14　保険薬局及び保険薬剤師療養担当規則（昭和 32 年厚生省令第 16 号）第 6 条に規定されている調剤済みの処方せん及び調剤録
15　臨床検査技師等に関する法律施行規則（昭和 33 年厚生省令第 24 号）第 12 条の 3 に規定されている書類

16　歯科衛生士法施行規則（平成元年厚生省令第 46 号）第 18 条に規定されている歯科衛生士の業務記録
17　高齢者の医療の確保に関する法律の規定による療養の給付の取扱い及び担当に関する基準（昭和 58 年厚生省告示第 14 号）第 9 条に規定されている診療録等
18　高齢者の医療の確保に関する法律の規定による療養の給付の取扱い及び担当に関する基準第 28 条に規定されている調剤済みの処方せん及び調剤録

なお、調剤録（薬剤師法第 28 条第 2 項に基づき調剤録への記入が不要とされた場合の調剤済み処方せんを含む。）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において行う必要がある。また、調剤録は当該薬局に備えることとされており、当該薬局の調剤録を外部保存する場合には、他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　紙の調剤済み処方せんと調剤録の電子化・外部保存について

紙の調剤済み処方せん（薬剤師法第 28 条第 2 項に基づき調剤録への記入が不要とされた場合の調剤済み処方せんを含む。）の電子化については、紙の処方せんに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電子化することとなる。

紙の処方せん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：薬局で紙の処方せん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せんであっても、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せんであっても、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せんに対して、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、電子処方せんを（電子的な）調剤済み処方せんとした場合には 7 章を、さらにそれを外部保存する場合には、8 章を参照されたい。

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、医療において個人情報の保護について留意しなければならない文書等には、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 章の安全管理等を参照し、情報管理体制確保の観点からも、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は、7 章及び 9 章に準じて取り扱う必要がある。

なお、「9.5（捕捉）　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、適宜参照されたい。

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場合にも、外部保存を実施（継続）する場合には、8 章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

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ある。このことから、収集、保管、破棄を通じて刑法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、診療情報の扱いに関わる法令、通知、指針等により定められている要件を満たすために適切な取扱いが求められる。

平成29年5月に施行した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」等が定められているため、関連する規定を遵守し、適切な措置を講じられたい。

故意及び重過失をもって、これらの要件に反する行為を行えば刑法上の秘密漏示罪で犯罪として処罰される場合があるが、診療情報等については過失による漏えいや目的外利用も同様に大きな問題となり得る。そのような事態が生じないよう適切な管理をする必要がある。そのためには管理者に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、その具体的内容は、扱う情報や状況によって異なるものである。

本来、医療情報の価値と重要性はその媒体によって変化するものではなく、医療機関等の管理者は、そもそも紙やフィルムによる記録を院内に保存する場合と電子化して保存する場合とでは、少なくとも同等の善管注意義務を負うと考えられる。

ただし、電子化された情報は、次のような固有の特殊性もある。

- 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高い
- さらに医療従事者が情報取扱いの専門家とは限らないため、その安全な保護に慣れていないケースが多い

従って、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、導入するシステムの機能や運用方法を選択して、それに対し求められる安全基準等への対応を決める必要がある。

また、電子化された医療情報が医療機関等の施設内だけにとどまって存在するという状況のみならず、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が負うだけでなく、ネットワーク上のサービスを提供する事業者やネットワークを提供する通信事業者等にもまたがるようになる。

本章では、これらの関係者間での電子的な医療情報の取扱いについて「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」の責任のあり方として責任分界という概念を用いて整理した。

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、通常の運用時において医療情報保護の体制を構築し管理する局面での責任と、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、医療情報の適切な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

電子的に医療情報を取り扱うシステムの機能や運用方法が、そ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する責任である。これを果たすためには、以下のことが必要である。

- システムの仕様や運用方法を明確に文書化すること
- 仕様や運用方法が当初の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

医療情報を取り扱うシステムの運用管理を行う責任であり、当該システムの管理を請負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。

- 少なくとも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等の監督を行うこと

さらに、個人情報保護法上は、以下の事項を定め、請負事業者との対応に当たる必

要がある。

・ 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るため、情報保護体制が陳腐化するおそれがあり、それを適宜見直して改善するためには以下の責任を果たさなくてはならない。

・ 当該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

そのために医療機関等の管理者は、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必要がある。

(2) 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 Ⅲ 4. (5)」では、個人データの漏えい等の問題発生時における二次被害防止に向けた取組みについて規定していることから、参照されたい。

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、以下のことが必要である。

・ 医療機関等の管理者はその事態発生を公表すること
・ 原因とそれに対していかなる対処を行うかについて説明すること

② 善後策を講ずる責任

また、医療機関等の管理者には善後策を講ずる責任も発生する。その責任は以下に分けられる。

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

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 種類があるため、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、前項に従い整理して示す。

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、前項に掲げた「説明責任」・「管理責任」・「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」と「善後策を講ずる責任」を果たす必要があり、委託管理契約で委託先の義務を明記すべきである。

ただし、これとは別に、受託する事業者の責任による不都合な事態が生じた場合については、善後策を講ずる責任を医療機関等と受託する事業者との間でいかに分担するか、委託契約で明記しておくべき事項である。

以下に医療機関等が管理責任を果たすために必要な委託先との契約の原則を掲げる。

(1) 通常運用における責任について

① 説明責任

患者等に対し、いかなる内容の医療情報保護の仕組みが構築されどのように機能しているかの説明責任は、いうまでもなく医療機関等の管理者にある。

ただし、医療機関等の管理者が説明責任を果たすためには、受託する事業者による情報提供が不可欠の場合があり、受託する事業者は医療機関等の管理者に対し説明責任を負うといってよい。

従って、受託する事業者に対し適切な情報提供義務・説明義務を委託契約事項に含め、その履行を確保しておく必要がある。

② 管理責任

管理責任を負う主体はやはり医療機関等の管理者にある。しかし、現実に情報処理に当たりその安全な保守作業等を行うのは、委託先事業者である場面が多いと考えられる。医療機関等の管理者としては、委託先事業者の管理の実態を理解し、その監督を適切に行う仕組みを作る必要があり、契約事項に含めるべきである。

③ 定期的に見直し必要に応じて改善を行う責任

当該システムの運用管理の状況に対する定期的な監査により問題点を洗い出し、改善すべき点があれば改善していく責任の分担、また、情報保護に関する技術進展に配慮した定期的な再評価・再検討を実施し、その結果に基づき対策を行う際の医療機関

等との協議について、委託先事業者との契約事項に含めるべきである。

(2) 事後責任について

① 説明責任

前項で述べたように、医療情報について何らかの不都合な事態が生じた場合、医療機関等の管理者にはその事態発生を公表し、その原因といかなる対処法をとるかについて説明する責任が求められている。

しかし、情報に関する事故は、説明に際して受託する事業者の情報提供や分析が不可欠な場合が多いと考えられる。そのため、あらかじめ可能な限りの事態を予想し、受託する事業者との間で、説明責任についての分担を契約事項に含めるべきである。

② 善後策を講ずる責任

医療情報について何らかの事故が生じた場合、医療機関等の管理者には善後策を講ずる責任が発生することは前項で述べた。しかし、事故が医療情報の処理を委託した事業者の責任による場合、適切な委託契約に基づき、受託する事業者の選任・監督に適切な注意を払っていれば、法律上、医療機関等の管理者の善管注意義務は果たされていると解される。

ただし、本章冒頭に述べたように、医療機関等では医療情報の管理を医療機関等の管理者の責任において行うことが求められている。よって、医療情報に関する事故の原因究明、被害者への損害填補、さらに再発防止について、少なくとも責任の一端を負わなければならない。また、現実的にも、受託する事業者が医療情報の全てを管理しているとは限らないため、事故を契機として、医療情報保護の仕組み全体について善後策を講ずる責任は、医療機関等の管理者が負わざるを得ない。

上記のように、医療機関等の管理者は、患者に対して、「原因を追及し明らかにする責任」、「損害を生じさせた場合にはその損害填補責任」、「再発防止策を講ずる責任」等、善後策を講ずる責任を免れるものではない。

ただし、医療機関等の管理者の、患者等に対する全ての責任が免ぜられることはないとしても、受託する事業者との間での責任分担はそれとは別の問題である。特に、事故が受託する事業者の責任で生じた場合、医療機関等の管理者が全ての責任を負うことは、原則としてあり得ない。

しかし、医療情報について何らかの事故が生じた場合、医療機関等と受託する事業者の間で責任の分担について争うことに優先して、まず原因を追及し明らかにすること、そして再発防止策を講ずることが重要である。

そのためには、委託契約に、医療機関等と受託する事業者が協力してこれらの措置を優先させることを明記しておく必要がある。

委託内容によっては、より詳しく受託する事業者の責任での原因追及と再発防止策の提案義務を明記することも考えられる。

損害填補責任の分担については、事故の原因が受託する事業者にある場合、最終的には受託する事業者が負うのが原則である。ただし、この点は、原因の種類や複雑さによっては原因究明が困難になること、また損害填補責任分担の定め方によっては原因究明の妨げになるおそれがあること、あるいは保険による損害分散の可能性等、考慮すべき様々な要素がある。それらを考慮した上で、委託契約において損害填補責任の分担を明記することが必要である。

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について第三者提供を行う場合、個人情報保護法及び関連する個人情報保護法についてのガイドライン並びに「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」等を遵守する必要がある。

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あり、原則として医療機関等の管理者にとってはその正当性だけが問題となる。適切な第三者提供がなされる限り、その後の情報保護に関する責任は医療機関等の管理者から離れることになり、提供を受けた第三者に生ずる。

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するような場合は、提供元の医療機関等の責任が追及される可能性がある。

一方、電子化された情報の特殊性に着目すると、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、当該情報を保存している状態と何ら変わりがない。従って、その情報に関して適切な情報管理責任がなお残ることはいうまでもない。

医療情報が電子化され、ネットワーク等を通じて送受信して情報を提供する場合、第三者提供の際にも、医療機関等から受信側へ直接情報が提供されるわけではなく、情報処理関連事業者が介在することがある。この場合、いつの時点で、第三者提供が成立するのか、すなわち情報処理関連事業者との責任分界点の明確化というべき概念が発生する。

一旦適切・適法に提供された医療情報については送信側の医療機関等に責任はないことは先に述べたとおりであるが、第三者提供の主体は送信側の医療機関等であることからみて、患者に対する関係では、少なくとも情報が受信側に到達するまで、原則として送信側の医療機関等に責任があると考えることができる。その上で、前項にいうところの善後策を講ずる責任をいかに分担するかは、情報処理関連事業者及び送信側との間で、あらかじめ協議し明確にしておくことが望ましい。選任監督義務を果たしており、特に明記されていない場合で情報処理関連事業者の過失によるものである場合は、情報処理関連事業者が全ての責任を負うのが原則である。

4.3　例示による責任分界点の考え方の整理

本項では責任分界点について、幾つか例を挙げて解説する。ただし、本項は考え方を例として挙げているため、医療情報システムの安全管理や外部接続時のネットワークの考え方、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は、それぞれ6章、7章、8章を参照する必要がある。

(1) 地域医療連携で「患者情報を交換」する場合

(a) 医療機関等における考え方

① 「情報処理関連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患者情報を交換する場合の責任分界点

ここでいう「情報処理関連事業者の提供するネットワーク」とは、情報処理関連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言う。

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も含めて契約等で合意しておく。

その上で、自らの責任範囲において、情報処理関連事業者と管理責任の分担について責任分界点を定め、委託する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をどの事業者が主体となって行うかを明らかにしておく。

ただし、通常運用における責任並びに事後責任は、委託の場合には、原則として提供元医療機関等にあり、第三者提供の場合には、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。情報処理関連事業者に瑕疵のない場合は、情報処理関連事業者に生じるのは管理責任の一部のみであることに留意する必要がある。

② 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点

ここでいう「独自に接続」とは、情報処理関連事業者のネットワークではあるが、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う。

この場合、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機関等が責務を果たさなければならない。

情報処理関連事業者に対しては、管理責任の分担は発生せず、通信の品質確保は発生するとしても、情報処理関連事業者が提示する約款に示される一般的な責任しか存在しない。

さらに、提供元医療機関等と提供先医療機関等が1対N通信で、提供先医療機関等が一つでも特定できない場合は原則として医療情報を提供できない。ただし、法令で定められている場合等の例外を除く。

(b) 情報処理関連事業者に対する考え方

① 医療情報が発信元／送信先で適切に暗号化／復号される場合の責任分界点

患者情報を送信しようとする医療機関等（発信元）の情報システムにおいて、送信前に患者情報が暗号化され、情報を受け取った医療機関等(送信先)の情報システムにおいて患者情報が復号される場合、情報処理関連事業者は盗聴の脅威に対する個人情報保護上の責務とは無関係であり、責任は限定的になる。

この場合、情報処理関連事業者に存在するのは管理責任であり、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管理責任の範囲やネットワークの可用性等の品質に関して契約で明らかにしておく。

なお、暗号化等のネットワークに係る考え方や最低限のガイドラインについては、「6.11 外部と個人情報を含む医療情報を交換する場合の安全管理」を参照されたい。

② 医療情報が情報処理関連事業者の管理範囲の開始点で適切に暗号化される場合の責任分界点

情報処理関連事業者の中には、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する。

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外部からの情報の盗聴や改ざん、侵入等やサービスの可用性等の品質については事業者に管理責任が発生する。従って、それらの責任については契約で明らかにしておく。

ただし、事業者が提供するネットワーク回線に到達するまでの管理責任やネットワーク回線を流れる情報に対する管理責任は医療機関等に存在するため、「Ⅰ 医療機関等における考え方 ①医療情報の提供元医療機関等と提供先医療機関等の責任分界点」に則った考え方の整理が必要である。

なお、ネットワーク回線上とネットワーク回線を流れる情報に対する考え方や最低限のガイドラインについては、「6.11 外部と個人情報を含む医療情報を交換する場合の安全管理」を参照されたい。

(c) 外部保存機関が介在する場合に対する考え方

この場合、保存する情報は外部保存機関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る。

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ける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る。

また、外部保存機関とは、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。

なお、医療機関等が外部保存機関を通じて患者情報を交換する場合の医療機関等及び外部保存機関に対する考え方は、「8.1.2 外部保存を受託する機関の選定基準及び情報の取扱いに関する基準」で定める保存機関ごとに「2. 情報の取扱い」及び「3. 情報の提供」として、別途詳細に規定しているため、8.1.2章を参照されたい。

(2) 業務の必要に応じて医療機関等の「施設外から情報システムにアクセス」する場合

施設外から情報システムにアクセスする場合のネットワーク全般の考え方については、「6.11 外部と個人情報を含む医療情報を交換する場合の安全管理」の、特に「B-2. 選択すべきネットワークのセキュリティの考え方 Ⅲ. 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」を参照されたい。ここでは特に責任分界点の考え方について述べる。

(a) 自らの機関の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

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も一般的になってきた。

この場合、責任分界の観点では自施設に閉じているが、情報処理関連事業者が間に入って通信回線の両端で一医療機関等の従業者が関わることになる。

さらに、この場合には通信回線がインターネットだけでなく携帯電話網、公衆回線等多彩なものが利用されることになり、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る。

特に、医療機関等の管理責任者でない医療機関等の従業者についても管理責任が問われる事態も発生することに注意を払う必要がある。

この例の場合、責任分界点としては基本的に自施設に閉じているため、責任のあり方の原則としては、「4.1 医療機関等の管理者の情報保護責任について」を参照すべきことに留意しなくてはならない。

(b) 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

この例のような、リモートログインを用いた保守業者の遠隔保守のためのアクセスが考えられる。この場合、適切な情報管理や情報アクセス制御がなされていないと一時保存しているディスク上の個人情報を含む医療情報の不正な読み取りや改ざんが行われる可能性もある。他方、リモートログイン機能を全面的に禁止してしまうと、遠隔保守が不可能となり、保守に要する時間等の保守コストが増大する。

従って、保守の利便性と情報保護との兼ね合いを見極めつつ実施する必要がある。

ただし、この場合でも、当然、医療機関等に対して「通常運用における責任」、「事後責任」が存在するため、管理状況の報告を定期的に受け、管理に関する最終的な責任の所在を明確にする等の監督を行い、管理責任を果たす必要がある。

なお、リモートログインも含めた、保守の考え方については「6.8 情報システムの改造と保守」を参照されたい。

(3) 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

ここでいう委託とは遠隔画像診断、臨床検査等、診療等を目的とした業務の第三者委託であり、これに伴い一時的にせよ情報を第三者が保管することとなる。

医療機関等の管理者は業務委託先に対して、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とともに、情報の保存期間の規定等の管理監督を行う必要がある。

ただし、受託する事業者は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あるが、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を双方協議し明記しておく必要がある。

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、医療情報が外部に提供される場合は、これに準じてあらかじめ治験依頼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を行うことが必要である。

(4) オンライン外部保存を委託する場合

委託先が医療機関等、行政機関、又は民間事業者であるかによって要件は異なるので、本ガイドラインの「8.1.2 外部保存を受託する機関の選定基準及び情報の取扱いに関する基準」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る。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り、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委託契約で定め、医療機関等としても理解する努力は必要である。さらにネットワーク事業者と外部保存を受託する事業者は異なることが多いが、障害が起こった際の対処の責任範囲についても、明確に定めた上で、医療機関等が理解しておく必要がある。

さらに委託先に対する監督も必須であり、定期的に安全管理に関する状況の報告を受ける必要がある。

(5) 法令で定められている場合

法令で定められている場合等の特別な事情により、情報処理関連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、情報処理関連事業者若しくはネットワークにおいて盗聴の脅威に対する対策を施す必要がある。

そのため、当該医療情報の通信経路上の管理責任を負っている医療機関等は、情報処理関連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らない。

また、情報処理関連事業者に対して管理責任の一部若しく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、監督しなければならない。

4.4　技術的対策と運用による対策における責任分界点

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）」の総合的な組み合わせによって達成する必要がある。

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（ベンダ）に求められ、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。

総合的な判断とは、リスク分析に基づき、経済性も加味して装置仕様あるいはシステム要件と運用管理規程により一定レベルの安全性を確保することである。この選択は安全性に対する脅威やその対策に対する技術的変化や医療機関等の組織の変化を含めた社会的環境変化により異なってくるので、その動向に注意を払う必要がある。

総合的な判断を下し、医療機関等が責任を果たすためには、ベンダへ要求する技術要件あるいはベンダが要求する運用条件を明確にして、ベンダとの責任分界点を明確にする必要がある。

運用管理規程は、医療機関等として総合的に作成する場合と医用画像の電子保存のように部門別や装置別に作成される場合がある。基準を満たしているか否かを判断する目安として、10章と付表を参考にして、「基準適合チェックリスト」等を作成して整理しておく必要がある。このようなチェックリストは第三者へ説明責任を果たす際の参考資料に利用できる。

5　情報の相互運用性と標準化について

医療機関等において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、連絡等による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、事務処理の合理化に端を発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ものである。

このような電子化された情報のやりとりを、医療機関等において段階的に導入されたシステム間や、部門ごとに多様なシステムベンダから提供されたシステム間で行う際に必要とされるのが相互運用性の確保である。

一方、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、情報の安全性の重要な要素の一つの「可用性」が挙げられる。ここでいう可用性とは、具体的には必要時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　見読性の確保について」及び「7.3　保存性の確保について」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を意味する。

さらに、地域連携等では、医療機関等間における情報の共有化、蓄積、解析、再構築、返信や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を継続されること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ついての民間主導の取組みとして、医療情報標準化推進協議会（Health Information and Communication Standards Board：HELICS 協議会）がある。各種の標準化団体・規格制定団体等が会員となっている 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、上記の 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」とされ、その実装が強く推奨されており、標準化の一層の推進が期待されるところである。

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、標準に基づく相互運用性の確保の推進に向けては、システムベンダ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。

従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、下記のこと等についてシステムベンダから説明を受ける等して、一定の理解を等しくしておく必要がある。

・標準化に対する基本スタンス
・次項以下に掲げる標準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、現在導入しているシステムの更新や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き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。

5.1　基本データセットや標準的な用語集、コードセットの利用

先述したように標準化に向けた取組みは進捗中であるが、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る。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る。

- 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を以下に示す。

5.1.1　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る。

前述のように、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ある。

平成 29 年 5 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る。

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
HS010 保健医療情報-医療波形フォーマット－第 92001 部：符号化規則
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
HS025 地域医療連携における情報連携基盤技術仕様
HS026 SS-MIX2 ストレージ仕様書および構築ガイドライン

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あるので、必要に応じ、適宜最新版を参照されたい。下記等から参照可能である。

http://www.mhlw.go.jp/seisakunitsuite/bunya/kenkou_iryou/iryou/johoka/index.html

5.1.2 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た。

この基本データセットには以下が含まれる。

・利用者情報
・患者情報（基本情報）
・患者情報（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

基本データセットによりデータの互換性を確保するためのガイドラインは以下を参照されたい。

・JAHIS 基本データセット適用ガイドライン
https://www.jahis.jp/standard/contents_type=33

5.1.3　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る。

なお、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る。

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
http://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るので、適宜利用されたい。

5.2　データ交換のための国際的な標準規格への準拠

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、我が国において利用可能なよう

に定義したものとして、保健医療福祉情報システム工業会（JAHIS）による標準規約化がされている。

主要なものとしては以下が挙げられる（一部は厚生労働省標準規格にも採択されている）。

- 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

これらの規約は以下の URL で取得できる。

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

5.3　標準規格の適用に関わるその他の事項

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 を提案している。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ある。詳細は以下の URL から得られる。

http://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る。

また、注意しなければならない点として外字の問題がある。外字とは個別のシステムにおいて独自に定義した表記文字であるが、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、システムを変更した場合や、他のシステムと情報を交換する場合には表記に齟齬のないように対策する必要がある。

6　情報システムの基本的な安全管理

情報システムの安全管理は、刑法等で定められた医療専門職に対する守秘義務等や個人情報保護関連各法（個人情報保護法、行政機関個人情報保護法及び独立行政法人等個人情報保護法）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。守秘義務は医療専門職や行政機関の職員等の個人に、安全管理・確保は個人情報取扱事業者や行政機関の長等に課せられた責務である。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こと、つまり説明責任を果たすことが求められる。この章での制度上の要求事項は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、滅失又はき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 20 条　第 21 条　第 22 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、この方針の中に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。

個人情報保護に関する方針に盛り込むべき具体的内容について、「JIS Q 15001:2006（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る。

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

b)個人情報の取り扱いに関する法令、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、滅失又はき損の予防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)代表者の氏名

また、情報システムの安全管理については、「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)」5.2 方針で、下記のように定めている。

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。

個人情報を取り扱う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、公開していること。
2. 個人情報を取り扱う情報システムの安全管理に関する方針を策定していること。その方針には、少なくとも情報システムで扱う情報の範囲、取扱いや保存の方法と期間、利用者識別を確実に行い不要・不法なアクセスを防止していること、安全管理の責任者、苦情・質問の窓口を含めること。

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）並びに 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、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おいて、その装置のベンダ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、JAHIS 標準及び日本画像医療システム工業会規格となっている「『製造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「製造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」が参考になる。

このチェックリストは以下の URL で取得できる。

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

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
Act－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 では ISMS 構築の骨格となる文書（基本方針、運用管理規程等）と文書化された ISMS 構築手順を確立する。

D 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 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 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。

上記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 JIPDEC（一般財団法人日本情報経済社会推進協会）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る。

【医療の安全管理の流れ】

事故やミスの発見と報告
「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
- 「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医師が処方せんを出し、②処方せんが薬剤部に送られ、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
- 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 が中心になっている。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自ずと見え、それを実行することで安全が高まる仕組みが出来上がっているためといえる。

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し得る。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。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。

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る。

P のステップを実践するために必要なことは何かについて次に述べる。

6.2.2　取扱い情報の把握

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。このリストは情報システムの安全管理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の影響の大きさと、継続した業務を行う視点からの影響の大きさを考慮する必要がある。このほかに医療機関等の経営上の視点や、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、医療に係る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、利用者の過誤等による脅威を列挙する。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に、同僚等の悪意や過誤を想定することに抵抗がある。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、万一に備えて対策を準備する必要がある。また説明責任を果たすためには、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～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障することであり、これが限界である。従って、人の行為も含めた脅威を想定し、運用管理規程を含めた対策を講じることが重要である。

医療情報システムとして上記の観点で留意すべき点は、システムに格納されている電子データの保護に関してだけでなく、入出力の際に露見等の脅威にさらされるおそれのある個人情報を保護するための方策についても考える必要がある。以下に様々な状況で想定される脅威を列挙する。

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、き損、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、き損、滅失、漏えい
(c) コンピュータウイルス等の不正なソフトウェアによるアクセス、改ざん、き損、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コンピュータウイルス等の不正なソフトウェアによるアクセス、改ざん、き損、滅失、漏えい
(c) ソフトウェア（Winny 等のファイル交換ソフト等）の不適切な取扱いによる情報漏えい
(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

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
- 改ざん
- 不正コマンド実行
- 情報かく乱
- ウイルス攻撃
- サービス不能（DoS：Denial of Service）攻撃
- 情報漏えい　等

(b) 非意図的要因による IT 障害
- システムの仕様やプログラム上の欠陥（バグ）
- 操作ミス
- 故障
- 情報漏えい　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

これらの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. 情報システムで扱う情報を全てリストアップしていること。
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を行い、常に最新の状態を維持していること。
3. このリストは、情報システムの安全管理者が必要に応じて速やかに確認できる状態で管理していること。
4. リストアップした情報に対してリスク分析を実施していること。
5. この分析により得られた脅威に対して、6.3 章～6.12 章に示す対策を行っていること。

D. 推奨されるガイドライン

1. 上記の結果を文書化して管理していること。

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、安全管理に関する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 情報や情報端末の外部持ち出しに関する規則等の整備
⑥ 情報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、その情報端末等の管理規程
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　情報及び情報機器の持ち出しについて」に記載しているので参照されたい。

C. 最低限のガイドライン

1. 情報システム運用責任者の設置及び担当者（システム管理者を含む。）の限定を行うこと。ただし小規模医療機関等において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、入退を制限する等の入退管理を定めること。
3. 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。
   (a) 理念（基本方針と管理目的の表明）
   (b) 医療機関等の体制
   (c) 契約書・マニュアル等の文書の管理

(d) リスクに対する予防、発生時の対応の方法
(e) 機器を用いる場合は機器の管理
(f) 個人情報の記録媒体の管理（保管・授受等）の方法
(g) 患者等への説明と同意を得る方法
(h) 監査
(i) 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、情報システムにおいて個人情報が入力、参照、格納される情報端末やコンピュータ、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、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

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　情報及び情報機器の持ち出しについて」に記載しているので参照されたい。

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等、運用管理規程に基づき許可された者以外立ち入ることができない対策を講じること。ただし、本対策項目と同等レベルの他の取り得る手段がある場合はこの限りではない。
3. 個人情報の物理的保存を行っている区画への入退管理を実施すること。例えば、以下のことを実施すること。
   - 入退者には名札等の着用を義務付け、台帳等に記入することによって入退の事実を記録する。
   - 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. 個人情報が存在する PC 等の重要な機器に盗難防止用チェーンを設置すること。
5. 覗き見防止の対策を実施すること。

D. 推奨されるガイドライン

1. 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く、一般的に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対策の手段となり得る。ここでは「6.2.3 リスク分析」で列挙した脅威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）利用者の識別及び認証
（2）情報の区分管理とアクセス権限の管理
（3）アクセスの記録（アクセスログ）
（4）不正ソフトウェア対策
（5）ネットワーク上からの不正アクセス
（6）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　情報及び情報機器の持ち出しについて」に記載しているので参照されたい。

(1)　利用者の識別及び認証

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、情報システムは利用者の識別と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、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。

このような本人の識別・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。例えば、本人の識別・認証に用いられる情報が第三者に漏れないように以下のようなリスクに対処しなければならない。

- 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。

- 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。
- 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。
- コンピュータウイルスにより、IDやパスワードが盗まれ、悪用される。

＜認証強度の考え方＞

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ある。しかし、ID・パスワードのみによる認証では、上記に列挙したように、その運用によってリスクが大きくなる。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る。

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、その実現可能性の観点からは推奨されない。

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「生体計測」（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ある。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ある。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2つの独立した要素を用いて行う方式（2要素認証）を採用することが望ましい。

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2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。※

※ 認証技術の端末等への実装状況等を鑑み、本ガイドライン第5版の公表から約10年後を目途に「C. 最低限のガイドライン」とすることを想定する。

また、例えば、放射線管理区域のモダリティを扱う又は薬局において薬歴の参照・入力を行う場合等において、情報システムを利用する端末に 2 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 2 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、2 要素認証と同等と考えてよい。

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 2 要素認証を行っていれば、セキュリティは担保されていると考えられる。

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ない。

入力者が端末から長時間、離席する場合には、正当な入力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ある。

なお、パスワードの定期的な変更を強制することにより、「C. 最低限のガイドライン」における「類推し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る。しかしながら、患者情報を取り扱う医療情報システムの性格に鑑み、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必要である。ただし、2 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。

＜IC カード等のセキュリティ・デバイスを配布する場合の留意点＞

利用者の識別や認証、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情報や暗号化鍵、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る。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においても、簡単には利用されないようにしていることが重要である。

従って、利用者の識別や認証、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く、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らない。

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するべきである。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に、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しい。

＜バイオメトリクスを利用する場合の留意点＞

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は、その測定精度にも注意を払う必要がある。医療情報システムで一般的に利用可能と思われる現存する各種のバイオメトリクス機器の測定精度は、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）には十分とはいえず、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る。

従って、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ある。

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る。

・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、特徴値が近似することがある
・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る。

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 2 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る。

これらのことを踏まえ、実際に採用することが想定される 2 要素認証の方式として、下記の例が挙げられる。

2 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

(2)　情報の区分管理とアクセス権限の管理

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。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り、組織の規程で定めなければならない。

(3)　アクセスの記録（アクセスログ）

個人情報を含む資源については、全てのアクセスの記録（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。従って、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。

また、アクセスログの証拠性確保のために、記録する時刻は重要である。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。

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。

(4)　不正ソフトウェア対策

ウイルス、ワーム等と呼ばれる様々な形態を持つ不正なソフトウェアは、電子メール、ネットワーク、可搬媒体等を通して情報システム内に入る可能性がある。これら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、情報の暴露や改ざん、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情報システム内の端末装置、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情報端末や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　情報及び情報端末の持ち出しについて」を参照されたい。

ただし、これらのコンピュータウイルス等も常に変化しており、検出のためにはパターンファイルを常に最新のものに更新しておくことが必須である。

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。対策として、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り、オペレーティング・システム等でセキュリティ・ホールの報告されているものについては、対応版（セキュリティ・パッチと呼ばれるもの）への逐次更新、さらには利用していないサービスや通信ポートの非活性化、マクロ実行の抑制等も効果が大きい。

(5)　ネットワーク上からの不正アクセス

ネットワークからのセキュリティでは、クラッカーやコンピュータウイルスや不正アクセスを目的とするソフトウェアの攻撃から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。

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」等の各種方式がある。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ない。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しい。システム管理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べきである。このことは、医療機関等の外部から医療機関等の情報システムに接続される PC 等の情報端末に対しても同様であるが、その考え方と対策については、「6.9　情報及び情報端末の持ち出しについて」を参照されたい。

不正な攻撃を検知するシステム（IDS：Intrusion Detection System）もあり、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 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、パッチ等の対策を講じておくことも重要である。

無線 LAN や情報コンセントが部外者により、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、ウイルス等を感染させたり、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、不正にネットワーク上のデータを傍受したり改ざんする等が可能となる。不正な PC に対する対策を行う場合、一般的に MAC アドレスを用いて PC を識別する場合が多いが、MAC アドレスは改ざん可能であるため、そのことを念頭に置いた上で対策を行う必要がある。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担保するかが重要であり、特に、“なりすまし”の防止は確実に行わなければならない。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る。

（6）医療等分野における IoT 機器の利用

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る。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る。

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るが、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る。

本項では、IoT 機器（センサ等で自動的に情報を取得し、若しく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順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、以下の通り 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られたい。

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 外部と個人情報を含む医療情報を交換する場合の安全管理」の規定を参照されたい。

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。

IoT 機器により患者情報を取り扱う場合は、医療機器または非医療機器を問わず、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る。

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、機器の機能・性能によって、セキュリティが十分に確保されないおそれがある。よって、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について事前に患者等へ説明し、同意を得る必要がある。また、IoT 機器に異常や不都合が発生した場合の問い合わせ方法等について、患者等に説明する必要がある。

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るので、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る。

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るが、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。IoT 機器を含むシステムが単独でそれぞれの状態を把握できることが望ましいが、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る。この場合、上位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される。

このほか、IoT 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。IoT 機器のネットワーク接続状況を監視する等の対策も考えられるが、使用を

終えた又は停止した機器は電源を切り、接続を遮断する等、運用面での対策も可能である。

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る。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る。

(7) その他

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るので、情報の可用性が阻害されないように留意する必要がある。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ある。

また、電力線搬送通信（PLC：Power Line Communication）を利用する場合、医療機器に対する安全性が確認されておらず、厚生労働省医薬食品局から「広帯域電力線搬送通信機器による医療機器への影響に関する医療関係者等からの照会に対する対応について」（平成 18 年 11 月 9 日付け薬食安発第 1109002 号）の通知が出されているため、可用性の確保と他の医療機器への影響の双方に留意する必要がある。

C. 最低限のガイドライン

1. 情報システムへのアクセスにおける利用者の識別と認証を行うこと。
2. 本人の識別・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には、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行うこと。
3. 本人の識別・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には、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すること。
4. 入力者が端末から長時間、離席する際に、正当な入力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防止策を講じること。
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. 医療従事者、関係職種ごとに、アクセスできる診療録等の範囲を定め、そのレベルに沿ったアクセス管理を行うこと。また、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よう、運用管理規程で定めていること。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担保する必要がある。
7. アクセスの記録及び定期的なログの確認を行うこと。アクセスの記録は少なくと

も利用者のログイン時刻、アクセス時間、並びにログイン中に操作した患者が特定できること。情報システムにアクセス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で操作の記録（操作者及び操作内容等）を必ず行うこと。

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講じること。
9. アクセスの記録に用いる時刻情報は信頼できるものであること。医療機関等の内部で利用する時刻情報は同期している必要があり、また標準時刻と定期的に一致させる等の手段で標準時と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メディア使用時、外部からの情報受領時にはウイルス等の不正なソフトウェアが混入していないか確認すること。適切に管理されていないと考えられるメディアを利用する際には、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。常時ウイルス等の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。
11. パスワードを利用者識別に使用する場合

    システム管理者は以下の事項に留意すること。

    (1) システム内のパスワードファイルでパスワードは必ず暗号化（可能なら不可逆変換が望ましい）され、適切な手法で管理及び運用が行われること。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) 利用者がパスワードを忘れたり、盗用されたりするおそれがある場合で、システム管理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い、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）し、本人以外が知り得ない方法で再登録を実施すること。

    (3) システム管理者であっても、利用者のパスワードを推定できる手段を防止すること（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）。

    また、利用者は以下の事項に留意すること。

    (1) パスワードは定期的に変更し（最長でも 2 ヶ月以内　※D.5 に規定する 2 要素認証を採用している場合を除く。）、極端に短い文字列を使用しないこと。英数字、記号を混在させた 8 文字以上の文字列が望ましい。

    (2) 類推しやすいパスワードを使用しないこと、かつ類似のパスワードを繰り返し使用しないこと。類推しやすいパスワードには、自身の氏名や生年月日、辞書に記載されている単語が含まれるもの等がある。
12. 無線 LAN を利用する場合

    システム管理者は以下の事項に留意すること。

(1) 利用者以外に無線 LAN の利用を特定されないようにすること。例えば、ステルスモード、ANY 接続拒否等の対策を行うこと。

(2) 不正アクセスの対策を施すこと。少なくとも SSID や MAC アドレスによるアクセス制限を行うこと。

(3) 不正な情報の取得を防止すること。例えば WPA2/AES 等により、通信を暗号化し情報を保護すること。

(4) 電波を発する機器（携帯ゲーム機等）によって電波干渉が起こり得るため、医療機関等の施設内で利用可能とする場合には留意すること。

(5) 無線 LAN の適用に関しては、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」を参考にすること。

13. IoT 機器を利用する場合

システム管理者は以下の事項に留意すること。

(1) IoT 機器により患者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について患者等へ説明し、同意を得ること。また、機器に異常や不都合が発生した場合の問い合わせ先や医療機関等への連絡方法について、患者等に情報提供すること。

(3) IoT 機器には、製品出荷後にファームウェア等に関する脆弱性が発見されることがある。システムやサービスの特徴を踏まえ、IoT 機器のセキュリティ上重要なアップデートを必要なタイミングで適切に実施する方法を検討し、適用すること。

(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、対策を講じること。

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. 離席の場合のクローズ処理等を施すこと（クリアスクリーン：ログオフあるいはパスワード付きスクリーンセーバー等)。
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識別に使用する場合、以下の基準を遵守すること。
   （1）パスワード入力が不成功に終わった場合の再入力に対して一定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は再入力を一定期間受け付けない機構とすること。
5. 認証に用いられる手段としては、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（2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、情報システムを利用する端末に2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2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、2要素認証と同等と考えてよい。
6. 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は、マネジメントの複雑さが増し、侵入の危険が高まることがある。そのような侵入のリスクが高まるような設置をする場合、例えば802.1xや電子証明書を組み合わせたセキュリティ強化をすること。
7. IoT機器を含むシステムの接続状況や異常発生を把握するため、IoT機器・システムが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) システムの保守業者等の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)については、医療機関等の従業者としての人的安全管理措置、(c)については、守秘義務契約を結んだ委託業者としての人的安全管理措置の 2 つに分けて説明する。

(d)の第三者については、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ものであるため、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、いわゆる「外部保存」を受託する機関等に該当するが、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。

(1) 従業者に対する人的安全管理措置

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必要があり、以下の措置をとること。

1. 法令上の守秘義務のある者以外を事務職員等として採用するに当たって、雇用及び契約時に守秘・非開示契約を締結すること等により安全管理を行うこと。
2. 定期的に従業者に対し個人情報の安全管理に関する教育訓練を行うこと。

3. 従業者の退職後の個人情報保護規程を定めること。

D. 推奨されるガイドライン

1. サーバ室等の管理上重要な場所では、モニタリング等により従業者に対する行動の管理を行うこと。

(2) 事務取扱委託業者の監督及び守秘義務契約

C. 最低限のガイドライン

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、医療機関等の内部における適切な個人情報保護が行われるように、以下のような措置を行うこと。

   ① 受託する事業者に対する包括的な罰則を定めた就業規則等で裏付けられた守秘契約を締結すること
   ② 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・作業結果の確認を行うこと。
   ③ 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においても、作業後の定期的なチェックを行うこと。
   ④ 委託事業者が再委託を行うか否かを明確にして、再委託を行う場合は委託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ていることを条件とすること。

2. プログラムの異常等で、保存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外部の保守要員が診療録等の個人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。

6.7　情報の破棄

B. 考え方

医療に係る電子情報は破棄に関しても安全性を確保する必要がある。破棄は確実に行う必要がある。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り、注意しなくてはならない。

実際の破棄に備えて、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. 「6.1　方針の制定と公表」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の特定、具体的な破棄の方法を含めること。
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とし、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機関に破棄を委託した場合は、「6.6　人的安全対策　(2) 事務取扱委託業者の監督及び守秘義務契約」に準じ、さらに委託する医療機関等が確実に情報の破棄が行われたことを確認すること。
4. 運用管理規程において下記の内容を定めること。
   (a) 不要になった個人情報を含む媒体の破棄を定める規程の作成

6.8 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り、十分な対策が必要になる。具体的には以下の脅威が存在する。

- 個人情報保護の点では、修理記録の持ち出しによる暴露、保守センター等で解析中のデータの第三者による覗き見や持ち出し等
- 真正性の点では、管理者権限を悪用した意図的なデータの改ざんや、オペレーションミスによるデータの改変等
- 見読性の点では、意図的なマシンの停止や、オペレーションミスによるサービス停止等
- 保存性の点では、意図的な媒体の破壊及び初期化や、オペレーションミスによる媒体の初期化やデータの上書き等

これらの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。すなわち、①保守会社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会社からさらに外部の事業者に修理等を委託することが考えられるため、保守会社との保守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保守会社と同等の契約を求めることが重要である。

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、明確な守秘義務の設定を行うともに、終了後は確実にデータを消去する等の処理を行うことを求めること。
2. メンテナンスを実施するためにサーバに保守会社の作業員がアクセスする際には、保守要員個人の専用アカウントを使用し、個人情報へのアクセスの有無、及びアクセスした場合は対象個人情報を含む作業記録を残すこと。これはシステム利用者を模して操作確認を行うための識別・認証についても同様である。
3. そのアカウント情報は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対して速やかに保守用アカウントを削除できるよう、保守会社からの報告を義務付け、また、それに応じるアカウント管理体制を

整えておくこと。

5. 保守会社がメンテナンスを実施する際には、日単位に作業申請の事前提出することを求め、終了時の速やかな作業報告書の提出を求めること。それらの書類は医療機関等の責任者が逐一承認すること。
6. 保守会社と守秘義務契約を締結し、これを遵守させること。
7. 保守会社が個人情報を含むデータを組織外に持ち出すことは避けるべきであるが、やむを得ない状況で組織外に持ち出さなければならない場合には、置き忘れ等に対する十分な対策を含む取扱いについて運用管理規程を定めることを求め、医療機関等の責任者が逐一承認すること。
8. リモートメンテナンスによるシステムの改造や保守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作業内容を医療機関等の責任者が確認すること。
9. 再委託が行われる場合は、再委託する事業者にも保守会社の責任で同等の義務を課すこと。

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. 保守作業時には医療機関等の関係者立会いの下で行うこと。
3. 作業員各人と保守会社との守秘義務契約を求めること。
4. 保守会社が個人情報を含むデータを組織外に持ち出すことは避けるべきであるが、やむを得ない状況で組織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ことを求めること。また必要に応じて医療機関等の監査に応じることを求めること。
5. 保守作業に関わるログの確認手段として、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に何回のアクセスが行われたかが確認できる仕組みが備わっていること。

6.9　情報及び情報機器の持ち出しについて

B. 考え方

昨今、医療機関等において医療機関等の従業者や保守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る。

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ることも事実である。

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 メモリのような情報記録可搬媒体が考えられる。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る。

まず重要なことは、「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」の「6.2.2　取扱情報の把握」で述べられているように適切に情報の把握を行い、「6.2.3　リスク分析」を実施することである。

その上で、医療機関等において把握されている情報若しく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る。切り分けを行った後、持ち出してよいとした情報若しくは情報機器に対して対策を立てなくてはならない。

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の管理状況が明確になる。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も管理状況を把握するための方策となる。

一方、自宅等の医療機関等の管轄外のパソコン（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、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（Winny 等）、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。この場合、情報機器が基本的には個人の所有物となるため、情報機器の取扱いについての把握や規制は難しくなるが、情報の取扱いについては医療機関等の情報の管理者の責任において把握する必要性はある。

このようなことから、情報若しく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、組織として情報若しく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といえる。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は必要である。

ただし、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。

従って、情報若しく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、人的安全対策をさらに施す必要がある。

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情報システムにログインする場合においても、2 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 技術的安全対策」の記載を参照されたい。

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）が参考になる。

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、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。）は原則として行うべきではない。上記の要件を実現するためには端末の OS の設定を変更する必要があるが、この機能は管理者に限定されなければならない。管理者以外による設定の変更を技術的あるいは運用管理上、禁止できない限り、BYOD は行えない。
- 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若しくは情報機器の盗難、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し、教育を行うこと。
5. 医療機関等や情報の管理者は、情報が格納された可搬媒体若しくは情報機器の所在について台帳を用いる等して把握すること。
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たり、定期的にパスワードを変更する等の措置を行うこと。
7. 盗難、置き忘れ等に対応する措置として、情報に対して暗号化したりアクセスパスワードを設定する等、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をネットワークに接続したり、他の外部媒体を接続する場合は、コンピュータウイルス対策ソフトの導入やパーソナルファイアウォールを用いる等して、情報端末が情報漏えい、改ざん等の対象にならないような対策を施すこと。なお、ネットワークに接続する場合は「6.11　外部と個人情報を含む医療情報を交換する場合の安全管理」の規定を順守すること。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-11 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、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あるいは停止するか、業務に対して影響がないことを確認して用いること。
10. 個人保有の情報機器（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、管理者は 1～5 の対策を行うとともに、管理者の責任において上記の 6、7、8、9 と同様の要件を順守させること。

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露見を避けるため、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. スマートフォンやタブレットを持ち出して使用する場合、以下の対策を行うこと。
    - BYOD は原則として行わず、機器の設定の変更は管理者のみが可能とすること。
    - 紛失、盗難の可能性を十分考慮し、可能な限り端末内に患者情報を置かないこと。やむを得ず患者情報が端末内に存在するか、当該端末を利用すれば容易に患者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は端末を初期化する等の対策を行うこと。

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。このような事態に可能な限り対応するためには、普段からあらゆるレベルの異常時を想定し、対策を立て、文書化し、訓練を繰り返すことが有用である。このような対策を事業継続計画（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「6.2.3　リスク分析」の「⑦医療情報システム」に掲げる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言うまでもない。

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

前者としては、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あるいは全面停止に至り、医療サービス提供に支障発生が想定される場合である。

後者としては、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ある。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る。

(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、可能な限り計画内容を事前演習等で検証することが望ましい。

以下に、BCP としての策定計画と運用に関する一般項目を参考に掲げる。

① BCP として事前に周知しておく必要がある事項

事前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。

(2) 医療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非常時の対応

標的型メール攻撃等により医療情報システムがコンピュータウイルス等に感染した場合、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。

・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

・他の機器への感染拡大の防止や情報漏えいの抑止のための当該感染機器の隔離
・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
・マルウェア等に感染した場合、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取得することが望ましい）

なお、サイバー攻撃を防ぐために実施すべき対策については「6.5 技術的安全対策」、「6.6 人的安全対策」を参照されたい。

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”と判断する仕組み、正常復帰時の手順を設けること。すなわち、判断するための基準、手順、判断者、をあらかじめ決めておくこと。
2. 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規約を用意すること。
3. 非常時の情報システムの運用
   - 「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。
   - 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して、もし使用された場合には使用されたことが多くの人に分かるようにする等、適切に管理及び監査すること。
   - 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出来ないように変更しておくこと。
   - 標的型メール攻撃等により医療情報システムがコンピュータウイルス等に感染した場合、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。
4. サイバー攻撃で広範な地域での一部医療行為の停止等、医療サービス提供体制に支障が発生する場合は、“非常時”と判断した上で所管官庁への連絡を行うこと。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。

   連絡先　厚生労働省 医政局研究開発振興課医療技術情報推進室（03-3595-2430）

   ※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、マル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　外部と個人情報を含む医療情報を交換する場合の安全管理

B. 考え方

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。ここでは、双方向だけではなく、一方向の伝送も含む。外部と診療情報等を交換するケースとしては、地域医療連携で医療機関等や検査会社等と相互に連携してネットワークで診療情報等をやり取りする、診療報酬の請求のために審査支払機関等とネットワークで接続する、ASP・SaaS 型のサービスを利用する、医療機関等の従事者がノートパソコンのようなモバイル型の端末を用いて業務上の必要に応じて医療機関等の情報システムに接続する、患者等による外部からのアクセスを許可する等が考えられる。

医療情報をネットワークを利用して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。

ただし、本ガイドラインでは、これら全ての利用シーンを想定するのではなく、ネットワークを通じて医療情報を交換する際のネットワークの接続方式に関して、いくつかのケースを想定して記述を行う。また、ネットワークが介在する際の情報交換における個人情報保護とネットワークセキュリティは考え方の視点が異なるため、それぞれの考え方について記述する。

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 を参照願いたい。

B-1. 医療機関等における留意事項

ここでは「4.2 委託と提供における責任分界」で述べた責任のうち、ネットワークを通じて診療情報等を含む医療情報を伝送する場合の医療機関等における留意事項を整理する。

まず、医療機関等で強く意識しなくてはならないことは、情報を伝送するまでの医療情報の管理責任は送信元の医療機関等にあるということである。これは、情報の送信元である医療機関等から、情報が通信事業者の提供するネットワークを通じ、適切に送信先の機関に受け渡されるまでの一連の流れにおいて適用される。

ただし、誤解のないように整理すると、ここでいう管理責任とは電子的に記載されている情報の内容に対して負うべきものであり、その記載内容や記載者の正当性の保持（真正性の確保）を指す。つまり、後述する「B-2. 選択すべきネットワークのセキュリティの考え方」とは対処すべき方法が異なる。例えば、同じ「暗号化」を施す処置としても、ここで述べている暗号化とは、医療情報そのものに対する暗号化を施す等して、仮に送信元から送信先への通信経路上で通信データの盗聴があっても、第三者がその情報を判読できな

いようにしておく処置を指す。また、改ざん検知を行うために電子署名を付与することも対策の一つである。このように情報の内容に対するセキュリティをオブジェクト・セキュリティと呼ぶことがある。一方、「B-2. 選択すべきネットワークセキュリティの考え方」で述べる暗号化とはネットワーク回線の経路の暗号化であり、情報の伝送途中で情報を盗み見られない処置を施すことを指す。このような回線上の情報に対するセキュリティをチャネル・セキュリティと呼ぶことがある。

このような視点から、医療機関等において情報を送信しようとする場合には、その情報を適切に保護する責任が発生し、次のような点に留意する必要がある。

①「盗聴」の危険性に対する対応

ネットワークを通じて情報を伝送する場合には、この盗聴に最も留意しなくてはならない。盗聴は様々な局面で発生する。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る。一方、ネットワーク機材の不適切な設定により、意図しない情報漏えいや誤送信等も想定され、このような場合には医療機関等における責任が発生する事例も考えられる。

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る。その一つの方法として医療情報の暗号化が考えられる。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）のことを指している。

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はあるが、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しい。

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ある。その場合、医療機関等は上記のような留意点を保守委託事業者等に確認し、監督する責任を負う。

②「改ざん」の危険性への対応

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らない。情報を暗号化して伝送する場合には改ざんへ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る。また、後述する「B-2. 選択すべきネットワークセキュリティの考え方」の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り、改ざんに対する対処は確実に実施しておく必要がある。なお、改ざんを検知するための方法としては、電子署名を用いる等が想定される。

③「なりすまし」の危険性への対応

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くてはならない。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しなくてはならない。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ある。

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る。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る。

また、上記の危険性がサイバー攻撃による場合の対応は「6.10　災害、サイバー攻撃等の非常時の対応」を参照されたい。

B-2. 選択すべきネットワークのセキュリティの考え方

「B-1. 医療機関等における留意事項」では主に情報内容が脅威に対応するオブジェクト・セキュリティについて解説したが、ここでは通信経路上での脅威への対応であるチャネル・セキュリティについて解説する。

ネットワークを介して外部と医療情報を交換する場合の選択すべきネットワークのセキュリティについては、責任分界点を明確にした上で、医療機関における留意事項とは異なる視点で考え方を整理する必要がある。ここでいうネットワークとは、医療機関等の情報送信元の機関の外部ネットワーク接続点から、情報を受信する機関の外部ネットワーク接続点までや、業務の必要性から並びに患者からのアクセスを許可する等、外部から医療機関等の情報システムにアクセスする接続点までのことを指し、医療機関等の内部で構成される LAN は対象とならない。ただし、「4.2　委託と第三者提供における責任分界」でも触れたとおり、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。

ネットワークを介して外部と医療情報を交換する際のネットワークを構成する場合、まず、医療機関等は交換しようとする情報の機密性の整理をする必要がある。基本的に医療情報をやり取りする場合、確実なセキュリティ対策は必須であるが、例えば、予約システムが扱う再診予約情報のように機密性の高くない情報に対して過度のセキュリティ対策を施すと、高コスト化や現実的でない運用を招く結果となる。つまり、情報セキュリティに

対する分析を行った上で、コスト・運用に対して適切なネットワークを選択する必要がある。この整理を実施した上で、ネットワークにおけるセキュリティの責任の所在がネットワークを提供する事業者となるか、医療機関等になるか、若しくは双方の分担となるかを契約等で明らかにする必要がある。その際の考え方としては、大きく次の 2 つに類型化される。

- **回線事業者とオンラインサービス提供事業者がネットワーク経路上のセキュリティを担保する場合**

  回線事業者とオンラインサービス提供事業者が提供するネットワークサービスのうち、これらの事業者がネットワーク上のセキュリティを担保した形で提供するネットワーク接続形態であり、多くは後述するクローズドなネットワーク接続である。また、現在はオープンなネットワーク接続であっても、Internet-VPN サービスのような通信経路が暗号化されたネットワークとして通信事業者が提供するサービスも存在する。

  このようなネットワークの場合、通信経路上におけるセキュリティに対して医療機関等は管理責任の大部分をこれらの事業者に委託できる。もちろん自らの医療機関等においては、善管注意義務を払い、組織的・物理的・技術的・人的安全管理等の規程に則り、自医療機関等のシステムの安全管理を確認しなくてはならない。

- **回線事業者とオンラインサービス提供事業者がネットワーク経路上のセキュリティを担保しない場合**

  例えば、インターネットを用いて医療機関等同士が同意の上、ネットワーク接続機器を導入して双方を接続する方式が考えられる。この場合、ネットワーク上のセキュリティに対して回線事業者とオンラインサービス提供事業者は責任を負わない。そのため、上述の安全管理に加え、導入したネットワーク接続機器の適切な管理、通信経路の適切な暗号化等の対策を施さなくてはならず、ネットワークに対する正確な知識を持たない者が安易にネットワークを構築して医療情報等を脅威にさらさないように、万全の対策を実施する必要がある。

  そのため、情報の送信元・送信先に導入されるネットワーク接続機器に加え、医療機関等内に設置されている情報端末、当該端末に導入されている機能及び端末の利用者等を確実に確認する手段を確立する必要がある。また、情報をやり取りする機関同士での情報の取扱いに関する契約の締結、（脅威が発生した際に備えて）通信事業者にネットワーク経路上のセキュリティを委託する場合よりも厳密な運用管理規程の作成、専任の担当者の設置等も考慮しなくてはならない。

このように、医療機関等において医療情報をネットワークを通じて交換しようとする場合には、提供サービス形態の視点から責任分界点のあり方を理解した上でネットワークを

選定する必要がある。また、選択するセキュリティ技術の特性を理解し、リスクの受容範囲を認識した上で、必要に応じて説明責任の観点から患者等にもそのリスクを説明する必要がある。

ネットワークの提供サービスの形態は様々存在するため、以降ではいくつかのケースを想定して留意点を述べる。

また、想定するケースの中でも、携帯電話・PHS や可搬型コンピュータ等のいわゆる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は、利用するモバイル端末とネットワークの接続サービス及びその組み合わせによって複数の接続形態が存在するため、特に「Ⅲ　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」を設けて考え方を整理している。

Ⅰ．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、いわゆる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」の危険性は比較的低い。ただし、「B-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、ウイルス対策ソフトのパターン定義ファイルや OS のセキュリティ・パッチ等を適切に適用し、コンピュータシステムの安全性確保にも配慮が必要である。

以下、それぞれの接続方式について特徴を述べる。

①専用線で接続されている場合

専用線接続とは、2 地点間においてネットワーク品質を保ちつつ、常に接続されている契約機関専用のネットワーク接続である。通信事業者によってネットワークの品質と通信速度（以下「帯域」という。）等が保証されているため、拠点間を常時接続し大量の情報や容量の大きな情報を伝送するような場合に活用される。

ただし、品質は高いといえるが、ネットワークの接続形態としては拡張性が乏しく、かつ、一般的に高コストの接続形態であるため、その導入に当たってやり取りされる情報の重要性と情報の量等との兼ね合いを見極める必要がある。

図 B-2-①　専用線で接続されている場合

②公衆網で接続されている場合

公衆網とは ISDN（Integrated Services Digital Network）やダイアルアップ接続等、交換機を介した公衆回線を使って接続する接続形態のことを指す。

ただし、ここで想定する接続はインターネットサービスプロバイダ（以下「ISP」という。）に接続する方法ではなく、情報の送信元が送信先に電話番号を指定して直接接続する方式である。ISP を介して接続する場合は、ISP から先がいわゆるインターネット接続となるため、満たすべき要件としては後述する「Ⅱ．オープンなネットワークで接続する場合」を適用する。

この接続形態の場合、接続先に直接ダイアルしてネットワーク接続を確立するため、ネットワーク接続を確立する前に電話番号を確認する等の仕組みを導入すれば、確実に接続先と通信ができる。

一方で、電話番号を確認する仕組みを用いなかったことによる誤接続や誤送信のリスクがあること、専用線と同様に拡張性が乏しいこと、また、現在のブロードバンド接続と比べ通信速度が遅いため、大量の情報若しくは画像等の容量の大きな情報の送信には不向きであることから、適用範囲を適切に見定める必要がある。

図 B-2-②　公衆網で接続されている場合

③閉域 IP 通信網で接続されている場合

ここで定義する閉域 IP 通信網とは、通信事業者が保有する広域ネットワーク網と医療機関等に設置されている通信機器とを接続する通信回線が他のネットワークサービス等と共用されていない接続方式をいう。このような接続サービスを本ガイドラインでは IP-VPN（Internet Protocol-Virtual Private Network）と呼び、クローズドなネットワークとして

取り扱う。これに適合しない接続形態はオープンなネットワーク接続とする。主な利用形態としては、企業間における本店・支店間での情報共有網を構築する際に、遠隔地も含めた企業内 LAN のように利用され、責任主体が単一のものとして活用されることが多い。

この接続方式は、専用線による接続よりも低コストで導入することができる。また、帯域も契約形態やサービスの種類によっては確保できるため、大量の情報や容量の大きな情報を伝送することが可能である。

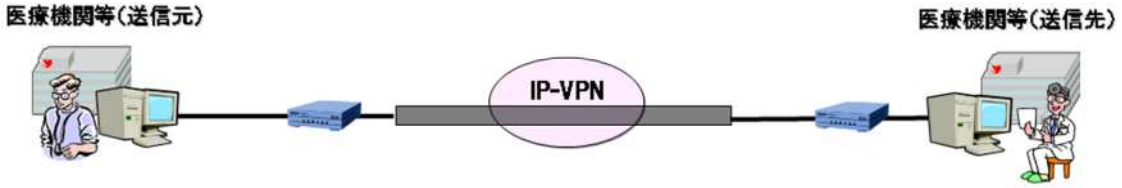

図 B-2-③-a　単一の通信事業者が提供する閉域ネットワークで接続されている場合

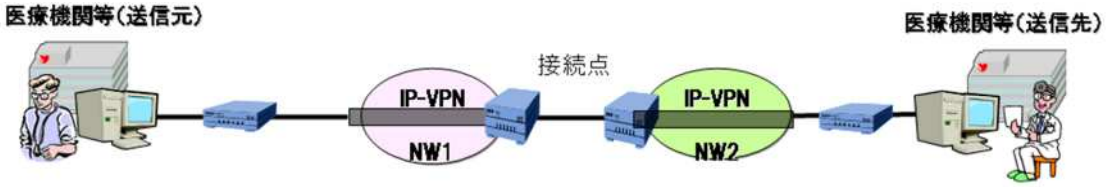

図 B-2-③-b　中間で複数の閉域ネットワークが相互接続して接続されている場合

以上の 3 つのクローズドなネットワークの接続では、クローズドなネットワーク内では外部から侵入される可能性はなく、その意味では安全性は高い。また異なる通信事業者のクローズドなネットワーク同士が接続点を介して相互に接続されている形態も存在し得る。接続点を介して相互に接続される場合、送信元の情報を送信先に送り届けるために、一旦、送信される情報の宛先を接続点で解釈したり新たな情報を付加したりする場合がある。この際、偶発的に情報の中身が漏示する可能性がないとはいえない。電気通信事業法があり、万一偶発的に漏示してもそれ以上の拡散は考えられないが、医療従事者の守秘義務の観点からは避けなければならない。その他、医療機関等から閉域 IP 通信網に接続する点等、一般に責任分界点上では安全性確保の程度が変化することがあり、特段の注意が必要である。

これらの接続サービスでは、一般的に送られる情報そのものに対する暗号化は施されていない。そのため、クローズドなネットワークを選択した場合であっても、「B-1. 医療機関等における留意事項」に則り、送り届ける情報そのものを暗号化して内容が判読できないようにして、改ざんを検知可能な仕組みを導入する等の措置を取る必要がある。

Ⅱ．オープンなネットワークで接続されている場合

いわゆるインターネットによる接続形態である。現在のブロードバンドの普及状況から、オープンなネットワークを用いることで導入コストを削減したり、広範な地域医療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。

ただし、B-2 の冒頭で述べたように、オープンなネットワークで接続する場合であっても、回線事業者とオンラインサービス提供事業者が、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。また、技術的な安全性について自らの責任において担保しなくてはならないことを意味し、その点に留意する必要がある。

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、どこ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 System 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

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ないが、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する。また、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。一方、IPsec を用いる場合は、2 階層目若しくは 3 階層目の「ネットワーク層」といわれる部分より下位の層で経路の暗号化手続きがなされるため、SSL-VPN よりは危険度が低いが、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して、確実にその安全性を確保する必要がある。

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は、HTTPS による暗号化等が求められる。しかし、昨今 SSL/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、SSL/TLS を適切に利用しなければ接続に HTTPS を用いても安全性を確保することができない。SSL/TLS を利用する上での適切な設定方法として、CRYPTREC が作成し情報処理推進機構によって発行された「SSL/TLS 暗号設定ガイドライン」にて指針が示された。「SSL/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、SSL/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る。「SSL/TLS 暗号設定ガイドライン」では 3 段階の設定基準が定められており、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 SSL/TLS への攻撃リスクを低減する必要がある。なお、「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 TLS1.2 に限定する必要があり、サーバ・クライアントともに TLS1.2 をサポートしていることが必須となることに注意されたい。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る。

さらに、オープンネットワークで接続する場合には、ソフトウェア型の IPsec や TLS1.2 によるセッションそのものが安全でも、他のオープンネットワークの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がマルウェアに感染し、遠隔操作が可能になると、IPsec や TLS1.2 によるセッションへの正規のアクセスが発生し得る。

よって、ソフトウェア型の IPsec や TLS1.2 の高セキュリティ型を採用しており、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。

ソフトウェア型の IPsec や TLS1.2 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）の「支払基金等へのレセプトオンライン請求用 IPsec＋IKE サービス」チェックリスト項目集が参考になる。

※「支払基金等へのレセプトオンライン請求用IPsec＋IKEサービス」チェックリスト項目集
http://www.hispro.or.jp/open/pdf/200909OnRece%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る。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、SSL/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る。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ある。

図 B-2-④　オープンネットワークで接続されている場合

Ⅲ．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、いわゆる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　情報システムの改造と保守」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、さらには本章「B-3　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」で述べる患者等からのアクセス等、様々なケースが想定される。

従って、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。

外部から医療機関等の内部ネットワークに接続する場合、現状で利用可能な接続形態の俯瞰図を図 B-2-⑤に示す。

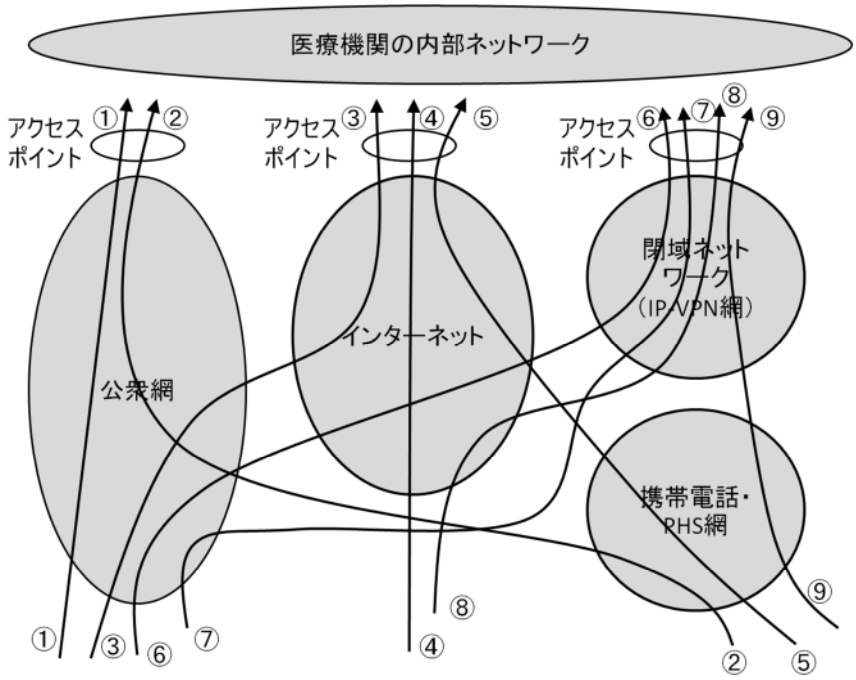

図 B-2-⑤　モバイル環境における接続形態

図 B-2-⑤に示したように、接続形態は下記の 3 つの系統に類型化できる。（括弧内の丸数字はそれぞれ図 B-2-⑤と対応する）

1）公衆網（電話網）を経由して直接ダイアルアップする場合（①、②）
2）インターネットを経由して接続する場合（③、④、⑤）
3）閉域ネットワーク（IP-VPN 網）を経由して接続する場合（⑥、⑦、⑧、⑨）

ここでは、本章の「Ⅰ．クローズドなネットワークで接続する場合」と「Ⅱ．オープンなネットワークで接続する場合」で説明したどのケースに該当するかを示し、それぞれのケースにおけるセキュリティ上の留意点をまとめる。

1）公衆網（電話網）を経由して直接ダイアルアップする場合

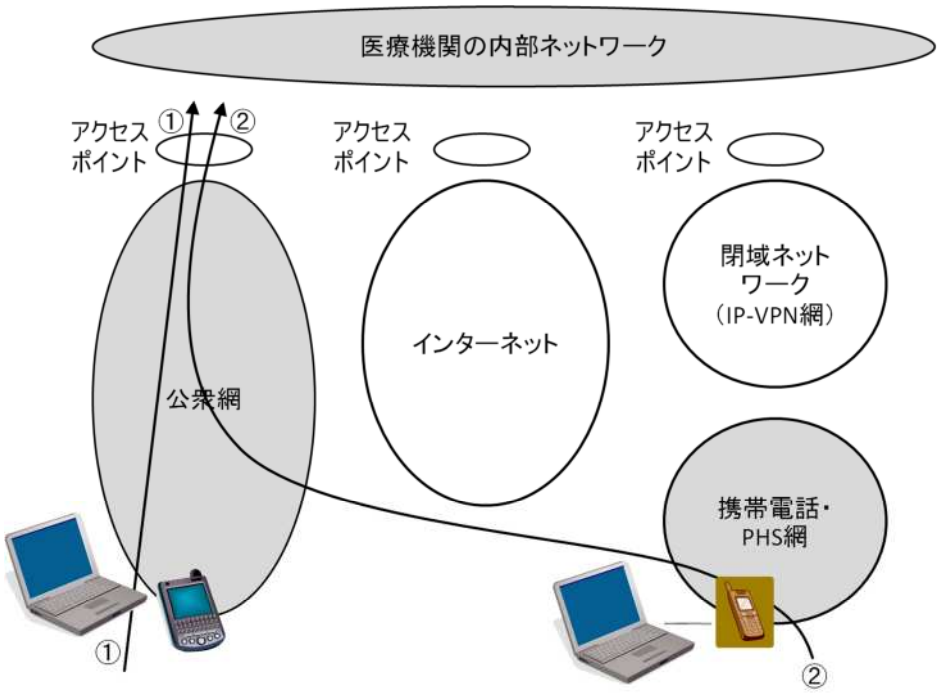

図 B-2-⑥　モバイル環境における接続形態（公衆網経由）

①は自宅やホテル等、通常の電話回線のある場所で、モバイル端末を電話線に接続し、医療機関等内に設けられたアクセスポイントに直接ダイアルアップするケースである。

②は①における電話回線の代わりに、携帯電話・PHS やその搬送波を利用する通信用カード等をモバイル端末に装着して携帯電話・PHS 網に接続ケースである。①と②は携帯電話・PHS 網を経由するかどうかの違いがある。

いずれも「Ⅰ．クローズドなネットワークで接続する場合」における「②公衆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。全て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。

2）インターネットを経由して接続する場合

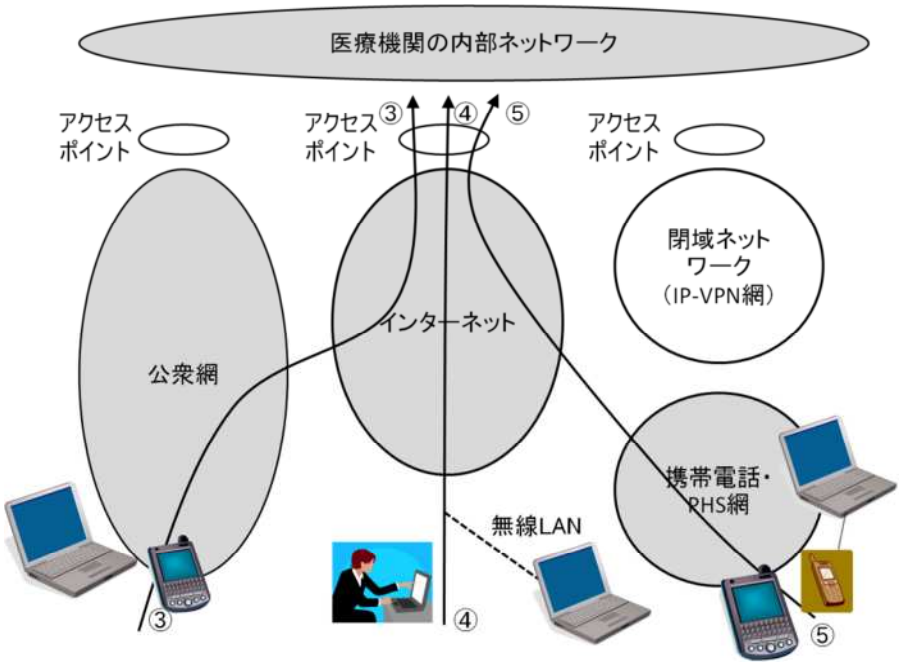

図 B-2-⑦　モバイル環境における接続形態（インターネット経由）

③は自宅やホテル等、通常の電話回線のある場所で、モバイル端末を電話線に接続してインターネットのサービスプロバイダのアクセスポイントにダイアルアップし、インターネット経由で医療機関等のアクセスポイント接続するケースである。

④は③における電話回線の代わりに、自宅やホテル等インターネットへの接続インタフェースのあるところで LAN を使って接続するケースである。LAN として有線の LAN の代わりに無線 LAN を利用するケースもある。いわゆる公衆無線 LAN を利用した接続もこの形態に含まれる。

⑤は携帯電話・PHS 網を経由して、携帯電話・PHS 等のサービス提供会社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ある。

③から⑤のいずれのケースも「Ⅱ．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。従って、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、「B-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。

なお、これらのケースは、いずれも操作者が自分のモバイル端末を用いて接続することを想定しているが、いわゆるネットカフェ等の備え付けの端末を利用して医療機関等内の情報にアクセスするケースも考えられる。このようなアクセス方法はリスクが大きい。

医療機関等が組織の方針として、このようなアクセス形態を認めるかどうかについては、慎重な検討が必要である。

3）閉域ネットワークを経由して接続する場合

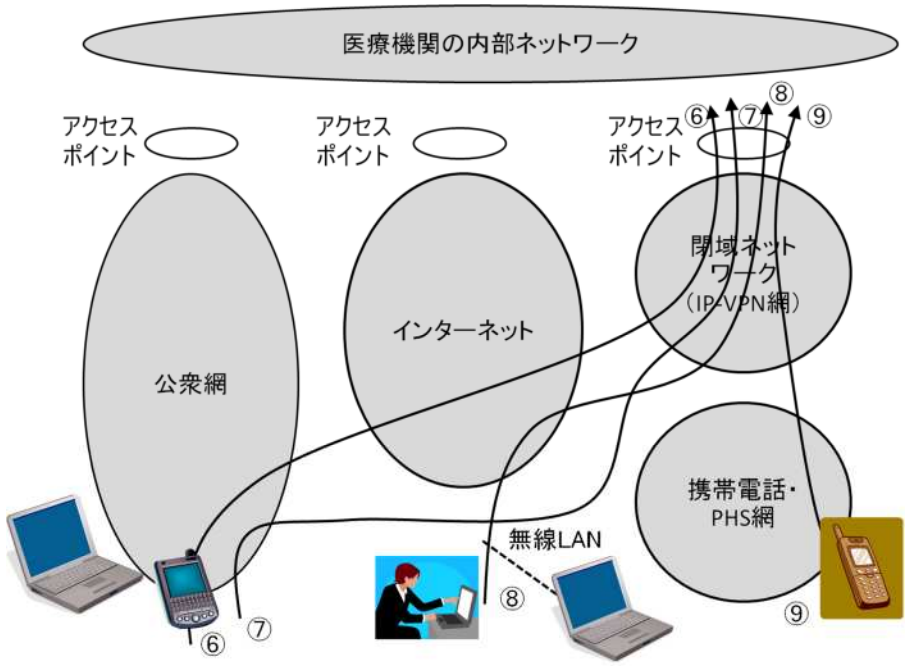

図 B-2-⑧　モバイル環境における接続形態（閉域ネットワーク経由）

⑥と⑦はいずれも自宅やホテル等、通常の電話回線のある場所で、モバイル端末を電話線に接続して閉域ネットワークのサービスプロバイダのアクセスポイントにダイアルアップし、閉域ネットワーク経由で医療機関等のアクセスポイントに接続するケースである。

⑥は⑦とよく似ているが、⑥がダイアルアップする際に一度オープンなネットワーク（インターネット）を提供するプロバイダを経由するのに対して、⑦では閉域ネットワークを提供するプロバイダに直接ダイアルアップするという違いがある。

⑧は⑥における電話回線の代わりに、自宅やホテル等インターネットへの接続インタフェースのあるところで LAN を使って接続するケースである。このケースのバリエーションとして、LAN として有線の LAN の代わりに無線 LAN を利用するケースもあり、いわゆる公衆無線 LAN 等もこのケースに含まれる。

⑨は携帯電話・PHS 網を経由して、閉域ネットワークへ接続するケースである。この場合の携帯電話・PHS 網から閉域ネットワークへの接続は、携帯電話・PHS サービス提供会社によって提供されるサービスである。

いずれも「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。

ただし、⑥と⑧のケースでは、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）を経由するため、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。

これについては「6.9　情報及び情報機器の持ち出しについて」に詳細を記述したので、参照されたい。

B-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は重要ではあるが、考慮すべきことが 3 点ある。

- 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。

従って、通常は行うべきではないが、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、やむを得ず行う場合は、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が普及しており、これらの導入を検討することが重要であるとともに、運用等の要件にも相当な厳しさが求められる。

B-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

提供する、若しくは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、患者に対する情報提供も十分想定される状況にある。ここではその際の考え方について触れる。

ここでの考え方の原則は、医療機関等が患者との同意の上で、自ら実施して患者等に情報を提供する場合であり、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情報提供を行うことはあってはならない。

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、情報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ある。また、一旦情報を提供すれば、その責任の所在は医療機関等ではなく、患者等にも発生する。しかし、セキュリティ知識に大きな差がある以上、情報を提供する医療機関等が患者等の納得のいくまで十分に危険性を説明し、その提供の目的を明確にする責任がある。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、その責任を逃れることはできないことを認識しなくてはならない。

今まで述べてきたような専用線等のネットワーク接続形態で患者等に情報を提供することは、患者等が自宅に専用線を敷設する必要が生じるため現実的ではなく、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になる。この場合、盗聴等の危険性は極めて高く、かつ、その危険を回避する術を患者等に付託することも難しい。

医療機関等における基本的な留意事項は、既に 4 章や B-1 で述べられているが、オープンなネットワーク接続であるため利活用と安全面両者を考慮したセキュリティ対策が必須である。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、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る。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必要がある。

このように、患者等に情報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、医療機関等内部の情報システムのセキュリティ対策、情報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 に関わる各種の法的根拠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、ウイルス混入等の改ざんを防止する対策を行うこと。

   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行うこと。

   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行うこと。

   上記を満たす対策として、例えば IPsec と IKE を利用することによりセキュアな

通信路を確保することが挙げられる。

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、選択するサービスの閉域性の範囲を事業者に確認すること。

2. データ送信元と送信先での、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。認証手段としては 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の容易に解読されない方法を用いるのが望ましい。
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行うこと。これに関しては、「6.5 技術的安全対策」で包括的に述べているので、それを参照すること。
4. 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し、施設内のルータを経由して異なる施設間を結ぶ VPN の間で送受信ができないように経路設定されていること。安全性が確認できる機器とは、例えば、ISO15408 で規定されるセキュリティターゲット若しく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. 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、SSL/TLS の利用、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、通信事業者やシステムインテグレータ、運用委託事業者、遠隔保守を行う機器保守会社等の多くの組織が関連する。そのため、次の事項について、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。
   - 診療情報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又は著しい遅延の場合の対処
   - 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、医療機関内においても次の事項において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の明確化（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の明確化
- 事故発生時における復旧作業・他施設やベンダ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の明確化（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. 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を行って不必要なログインを防止すること。
   また、メンテナンス自体は「6.8　情報システムの改造と保守」を参照すること。
8. 回線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に関して問題がないか確認すること。また、上記 1 及び 4 を満たしていることを確認すること。
9. 患者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、システムやアプリケーションを切り分けし、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た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 に係る以外の法的根拠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。
10. オープンなネットワークを介して HTTPS を利用した接続を行う際、IPsec を用いた VPN 接続等によるセキュリティの担保を行っている場合を除いては、SSL/TLS のプロトコルバージョンを TLS1.2 のみに限定した上で、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。その際、TLS の設定はサーバ/クライアントともに「SSL/TLS 暗号設定ガイドライン」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。いわゆる SSL-VPN は偽サーバへの対策が不十分なものが多いため、原則として使用しないこと。また、ソフトウェア型の IPsec 若しくは TLS1.2 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）等による攻撃からの防護について、適切な対策を実施すること。

D. 推奨されるガイドライン

1. やむを得ず、従業者による外部からのアクセスを許可する場合は、PC の作業環境内に仮想的に安全管理された環境を VPN 技術と組み合わせて実現する仮想デスクトップのような技術を用いるとともに、運用等の要件を設定すること。

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 1 項）

B. 考え方

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等として e-文書法省令において指定された文書等においては、「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。

ただし、医療に係る文書等では一定期間、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。例えば、現在、電子署名に一般的に用いられている暗号方式のRSA 1024bitやハッシュ関数のSHA1は、政府機関の情報システムからの移行スジュールが決まっており、平成20年4月の情報セキュリティ政策会議が決定した「政府機関の情報システムにおいて使用されている暗号アルゴリズムSHA1及びRSA1024に関わる移行指針」（平成24年10月改定）を基に、2014年度以降、RSA 2048bitやSHA2等への移行が進められている。

従って、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。近年、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、JIS規格としても制定された（JIS X 5092:2008 CMS利用電子署名(CAdES)の長期署名プロファイル、JIS X 5093:2008 XML署名利用電子署名(XAdES)の長期署名プロファイル）。

長期署名方式では、下記により、署名検証の継続を可能としている。

- 署名に付与するタイムスタンプにより署名時刻を担保する（署名に付与したタイムスタンプ時刻以前にその署名が存在していたことを証明すること)。
- 署名当時の検証情報（関連する証明書や失効情報等）を保管する。
- 署名対象データ、署名値、検証情報の全体にタイムスタンプを付し、より強固な暗号アルゴリズムで全体を保護する。

医療情報の保存期間は5年以上の長期にわたるものも有り、システム更新や検証システムの互換性等の観点からも、標準技術を用いることが望ましい。従って、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出来るようにすることが重要である。

さらに、医療に係る文書等に関しては、署名の正当性のみならず、処方せんのように、医師等の国家資格が確認できなくてはならない文書も存在する。その場合は、保健医療福祉分野における国家資格の確認も必要である。

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等において、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) 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 認証局若しくは認定特定認証事業者等の発行する電子証明書を用いて電子署名を施すこと

1. 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。従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ことが推奨される。

   ただし、当該電子署名を検証しなければならない者の全てが、国家資格を含めた電子署名の検証が正しくできることが必要である。
2. 電子署名法の規定に基づく認定特定認証事業者の発行する電子証明書を用いなくても A の要件を満たすことは可能であるが、同等の厳密さで本人確認を行い、さらに監視等を行う行政機関等が電子署名を検証可能である必要がある。

3. 「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、行政機関以外に当該電子署名を検証しなければならない者が全て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) 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、「タイムビジネスに係る指針－ネットワークの安心な利用と電子データの 安全な長期保存のために－」（総務省、平成 16 年 11 月）等で示されている時刻認証業務の基準に準拠し、一般財団法人日本データ通信協会が認定した時刻認証事業者のものを使用し、第三者がタイムスタンプを検証することが可能であること。
2. 法定保存期間中のタイムスタンプの有効性を継続できるよう、対策を講じること。
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講じる必要がある。

(3) 上記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

1. 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。本来法的な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　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は各種の法令に規定されており、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、煩わしさばかりが募ったりすることが想定され、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運用面と技術面の対応を検討されたい。

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、正当な権限において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。

従って、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。

B-1. 虚偽入力、書換え、消去及び混同を防止すること

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システム管理者は、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る。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る。

※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り込みが完了することをいう。

故意又は過失による虚偽入力、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る。

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、あるいは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る。

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る。

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る。

(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らない。

1. 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。
2. 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。
3. 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。
4. 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。
5. 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。
6. 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。
7. 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。
8. 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　情報システムの改造と保守」に記載された手続きに従う必要がある。

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る。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る。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個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。

(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る。

1. 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）
2. 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
3. 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
4. ウイルス等の不正なソフトウェアに感染し、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、医療機関等においてシステムの品質管理を率先して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」の記述を参照されたい。

B-2. 作成の責任の所在を明確にすること

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る。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が、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る。

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る。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る。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ある。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る。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らない。

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す。

（1） 入力者及び確定者の識別と認証
（2） 記録の確定

(3) 識別情報の記録
(4) 更新履歴の保存

(1) 入力者及び確定者の識別及び認証

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らない。よって、入力者の識別及び認証は必須となる。また、入力者と確定者が異なる場合は、確定者の識別及び認証が必要となる。

具体的な対策については、「6.5　技術的安全対策　(1) 利用者の識別及び認証」を参照されたい。

＜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なければならない。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、禁止しなくてはならない。

(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くてはならない。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る。

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する。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らない。

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る。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らない。

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若しく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る。

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、取り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ことが必要である。

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）等の特定の装置若しく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る。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る。

（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る。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る。

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する。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ある。

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らない。

（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。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らない。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らない。

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及び認証

a. 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

1. 入力者及び確定者を正しく識別し、認証を行うこと。
2. 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。
3. 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。

b. 臨床検査システム、医用画像ファイリングシステム等、特定の装置若しくはシステムにより記録が作成される場合

1. 装置の管理責任者や操作者が運用管理規程で明確にされ、装置の管理責任者、操作者以外による機器の操作が運用上防止されていること。
2. 当該装置による記録は、いつ・誰が行っ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こと。

(2) 記録の確定手順の確立と、識別情報の記録

a. 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

1. 診療録等の作成・保存を行おうとする場合、システムは確定された情報を登録できる仕組みを備えること。その際、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が含まれること。
2. 「記録の確定」を行うに当たり、内容の十分な確認が実施できるようにすること。
3. 「記録の確定」は、確定を実施できる権限を持った確定者が実施すること。
4. 確定された記録が、故意による虚偽入力、書換え、消去及び混同されることの防止対策を講じておくこと、また原状回復のための手順を検討しておくこと。
5. 一定時間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策定し運用管理規程に明記すること。
6. 確定者が何らかの理由で確定操作ができない場合、例えば医療機関等の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で定め、記録の確定の責任の所在を明確にすること。

b. 臨床検査システム、医用画像ファイリングシステム等、特定の装置若しくはシステムにより記録が作成される場合

1. 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が定義されていること。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が記録に含まれること。
2. 確定された記録が、故意による虚偽入力、書換え、消去及び混同されることの防

止対策を講じておくこと及び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した場合、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こと。
2. 同じ診療録等に対して更新が複数回行われた場合にも、更新の順序性が識別できるように参照できること。

(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適用するか、また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、誰の代行が誰によっていつ行われたかの管理情報が、その代行入力の都度記録されること。
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が明らかにされており、システムの仕様が明確に定義されていること。
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が規定されていること。
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に盛り込み、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。

(1) 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機関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。

(2) 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こと。なお、可逆的な情報の圧縮・解凍並びにセキュリティ確保のためのタグ付けや暗号化・平文化等は改ざんにはあたらない。

(3) リモートログイン機能を制限すること

保守目的等、どうしても必要な場合を除いて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　外部と診療情報等を含む医療情報を交換する場合の安全管理」を参照されたい。

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。

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る。

- 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。
- 複数媒体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。

これらに適切に対応することにより、紙の記録と同等といえる見読性を確保しなければならない。

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。

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、外部保存先の機関の事情により見読性が損なわれることを考慮に含めた十分な配慮が求められる。その際には、「4.2　委託と第三者提供における責任分界」を参考にしつつ、あらかじめ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る。

これらのことに配慮していても、万一、保存していた情報がき損した場合等は、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、患者ごとの情報の全て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は対応づけて管理されていること。また、見読手段である機器、ソフトウェア、関連情報等は常に整備されていること。

(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若しくは書面に表示できること。

(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に、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することができること。

（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することができること。

（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し、そのバックアップデータ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することができること。

【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。

（1） 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、外部に保存しても複製又は同等の内容を医療機関等の内部に保持すること。

（2） 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機関の障害等に対応できるような措置を行っておくこと。

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。

（1） 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
（2） 不適切な保管・取扱いによる情報の滅失、破壊
（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
（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
（5） 障害等によるデータ保存時の不整合

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。

（1） 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

ウイルス又はバグ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る。このため、これらの情報にアクセスするウイルス等の不適切なソフトウェアが動作することを防止しなければならない。

また、情報を操作する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確認しなければならない。

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。

(2) 不適切な保管・取扱いによる情報の滅失、破壊

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る。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らない。

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る。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る。

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る。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。

(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

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る。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る。

(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

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る。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若しくは読み取りができなくなること等である。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る。

(5) 障害等によるデータ保存時の不整合

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にシステムが停止したり、ネットワークに障害が発生したりして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る。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。

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機関において、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) 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の防止

1. いわゆるコンピュータウイルスを含む不適切なソフトウェアによる情報の破壊・混同が起こらないように、システムで利用するソフトウェア、機器及び媒体の管理を行うこと。

(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は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に関係者に教育を行い、周知徹底すること。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示すること。これらを運用管理規程としてまとめて、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施すこと。
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し、管理すること。
5. 各保存場所における情報がき損した時に、バックアップされたデータを用いてき損前の状態に戻せること。もし、き損前と同じ状態に戻せない場合は、損なわ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以前に情報を新たな記録媒体又は記録機器に複写すること。記録する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して、使用開始日、使用終了日を管理して、月に一回程度の頻度でチェックを行い、使用終了日が近づいた記録媒体又は記録機器については、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まとめて記載し、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、診療録等のデータを標準形式が存在する項目に関しては標準形式で、標準形式が存在しない項目では変換が容易なデータ形式にて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ていること。

【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。

（1） 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機関は、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。

（2） ネットワークや外部保存を受託する機関の設備の劣化対策を行うこと

ネットワークや外部保存を受託する機関の設備の条件を考慮し、回線や設備が劣化した際にはそれらを更新する等の対策を行うこと。

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. 記録媒体及び記録機器、サーバの保管は、許可された者しか入ることができない部屋に保管し、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に、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し、その内容に対して改ざん等による情報の破壊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 若しくは RAID-6 相当以上のディスク障害に対する対策を行うこと。

【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】

（1） ネットワークや外部保存を受託する機関の設備の互換性を確保すること

1. 回線や設備を新たなものに更新した場合、旧来のシステムに対応した機器が入手困難となり、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。従って、外部保存を受託する機関は、回線や設備の選定の際は将来の互換性を確保するとともに、システム更新の際には旧来のシステムに対応し、安全なデータ保存を保証できるような互換性のある回線や設備に移行すること。

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　8 章の対象となる文書等について」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 つの場合に分けて提示されている。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、電気通信回線（以降ネットワーク）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

調剤済み処方せんは、そのままの形式（紙又は電子）での外部保存のほか、紙媒体の場合には 9 章に示す方法により電子化し、電子媒体での外部保存が可能となる。紙の調剤済み処方せん（薬剤師法第 28 条第 2 項に基づき調剤録への記入が不要とされた場合の調剤済み処方せんを含む。）の電子化については 3 章及び 9 章に、調剤録（薬剤師法第 28 条第 2 項に基づき調剤録への記入が不要とされた場合の調剤済み処方せんを含む。）の外部保存については 3 章に記載があるので参照されたい。

8.1　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

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ある。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、外部保存を委託する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る。

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ある。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ある。

従って、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機関に保存する場合は、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。

8.1.1　電子保存の 3 基準の遵守

3 基準の記載については、「7.1　真正性の確保について」、「7.2　見読性の確保について」、

「7.3　保存性の確保について」にそれぞれ統合したので、そちらを参照されたい。

8.1.2　外部保存を受託する機関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、滅失又はき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 20 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

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る。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る。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る。

さらには、情報の保存を受託する機関等若しくは従業者による、利益を目的とした不当利用の危惧があるのも事実である。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る。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。

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る。従って、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ある。

上記に対応するため、「C. 最低限のガイドライン」で定める「②行政機関等が開設したデータセンター等に保存する場合」、及び適切な機関を選定し、「③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保存する場合」には、C で定める事項を厳守する必要がある。また、データセンター等の情報処理関連事業者が経済産業省の定める「医療情報を受託管理する情報処理事業者向けガイドライン」や、総務省の定める「ASP・SaaS における情報セキュリティ対策ガイドライン」及び「ASP・SaaS 事業者が医療情報を取り扱う際の安全管理に関するガイドライン」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。

本章では「1. 外部保存を受託する機関の選定基準」、「2. 情報の取扱い」、「3. 情報の提供」に分けて考え方を整理する。

「4. 電子的な医療情報を扱う際の責任のあり方」及び「6.11　外部と個人情報を含む医療情報を交換する場合の安全管理」と不可分であるため、実施に当たってはこれらも併せて遵守する必要がある。

1. 外部保存を受託する機関の選定基準

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

病院、診療所が自ら堅牢性の高い設備環境を用意し、近隣の病院、診療所の診療録等を保存する、ASP・SaaS 型のサービスを提供するような場合が該当する。

また、病院、診療所に準ずるものとして医療法人等が適切に管理する場所としては、公益法人である医師会の事務所で複数の医療機関等の管理者が共同責任で管理する場所等がある。

② 行政機関等が開設したデータセンター等に保存する場合

国の機関、独立行政法人、国立大学法人、地方公共団体等が開設したデータセンター等に保存する場合が該当する。

この場合、本章の他の項の要求事項、本ガイドラインの他の章で言及されている責任のあり方、安全管理対策、真正性、見読性、保存性及び C で定める情報管理体制の確保のための全ての要件を満たす必要がある。

③ 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保存する場合

①及び②以外の機関が医療機関等の委託を受けて情報を保存するデータセンター等が該当する。

この場合、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る。

そのため、それらの事業者等が、本章の他の項の要求事項、本ガイドラインの他の章で言及されている、責任のあり方、安全管理対策、真正性、見読性、保存性及び C

で定める情報管理体制の確保のための全ての要件を満たす必要がある。

また、それらのサービス形態によって、経済産業省の定めた「医療情報を受託管理する情報処理事業者向けガイドライン」や総務省が定めた「ASP・SaaS における情報セキュリティ対策ガイドライン」及び「ASP・SaaS 事業者が医療情報を取り扱う際の安全管理に関するガイドライン」の要求事項も満たす必要がある。

2. 情報の取扱い

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

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、不当な営利、利益を目的としない場合に限る。

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る。

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る。

② 行政機関等が開設したデータセンター等に保存する場合

行政機関等に保存する場合、開設主体者が公務員等の守秘義務が課せられた者であることから、情報の取扱いについては一定の規制が存在する。しかし、保存された情報はあくまで医療機関等から委託を受けて保存しているのであり、外部保存を受託する事業者が独自に分析、解析等を行うことは医療機関等及び患者の同意がない限り許されない。

従って、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、若しく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る。

また、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る。

また、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したり、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も考えられる。

③ 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保存する場合

冒頭でも触れたとおり、本項で定める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、不当な営利、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、許されない。

民間等で医療情報の外部保存を受託する事業者に対しては、これらの行為を規制するための指針が外部保存通知にあるとおり経済産業省や総務省で定められている。従って、医療機関等は契約も含め、その遵守状況を十分確認する必要がある。

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る。

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、あるいは情報処理関連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る。

具体的には、「暗号化を行う」、「情報を分散保管する」方法が考えられる。

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い。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る。

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る。分散保管においても同様の可用性の保証が必要である。

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ある。

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らない。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、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。

3. 情報の提供

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

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なくてはならない。

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らない。

② 行政機関等が開設したデータセンター等に保存する場合

いかなる形態であっても、保存された情報を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はならない。

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提供する場合は、あくまで医療機関等同士の同意の上で実施されなくてはならず、当然、患者の同意も得た上で実施する必要がある。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、医療機関等若しくは医療機関等との間で同意を得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らない。

従って、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する必要がある。

③ 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保存する場合

いかなる形態であっても、保存された情報を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はならない。これは匿名化された情報であっても同様である。

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同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る。

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、医療機関等若しくは医療機関等との間で同意を得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らない。

従って、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らない。

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

(ア) 病院や診療所の内部で診療録等を保存すること。

(イ) 保存を受託した診療録等を委託した病院、診療所や患者の許可なく分析等を目的

として取り扱わないこと。

(ウ) 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う場合は、委託した病院、診療所及び患者の同意を得た上で、不当な営利、利益を目的としない場合に限ること。

(エ) 匿名化された情報を取り扱う場合においても、匿名化の妥当性の検証を検証組織で検討することや、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した上で実施すること。

(オ) 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、診療所は適切なアクセス権を規定し、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すること。

(カ) 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こと。

② 行政機関等が開設したデータセンター等に保存する場合

(ア) 法律や条例により、保存業務に従事する個人若しくは従事していた個人に対して、個人情報の内容に係る守秘義務や不当使用等の禁止が規定され、当該規定違反により罰則が適用されること。

(イ) 適切な外部保存に必要な技術及び運用管理能力を有することを、システム監査技術者及び Certified Information Systems Auditor （ISACA 認定）等の適切な能力を持つ監査人の外部監査を受ける等、定期的に確認されていること。

(ウ) 医療機関等は保存された情報を、外部保存を受託する事業者が分析、解析等を実施しないことを確認し、実施させないことを明記した契約書等を取り交わすこと。

(エ) 保存された情報を、外部保存を受託する事業者が独自に提供しないように、医療機関等は契約書等で情報提供について規定すること。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させること。

③ 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保存する場合

(ア) 医療機関等が、外部保存を受託する事業者と、その管理者や電子保存作業従事者等に対する守秘に関連した事項や違反した場合のペナルティも含めた委託契約を取り交わし、保存した情報の取扱いに対して監督を行えること。

(イ) 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の安全性に関しては「6.11　外部と個人情報を含む医療情報を交換する場合の安全管理」を遵守していること。

(ウ) 受託事業者が民間事業者等に課せられた経済産業省の「医療情報を受託管理する情報処理事業者向けガイドライン」や総務省の「ASP・SaaS における情報セキュリティ対策ガイドライン」及び「ASP・SaaS 事業者が医療情報を取り扱う際の安全管理に関するガイドライン」等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。

(エ) 保存された情報を、外部保存を受託する事業者が契約で取り交わした範囲での保守作業に必要な範囲での閲覧を超えて閲覧してはならないこと。なお保守に関しては、「6.8 情報システムの改造と保守」を遵守すること。

(オ) 外部保存を受託する事業者が保存した情報を分析、解析等を実施してはならないこと。匿名化された情報であっても同様であること。これらの事項を契約に明記し、医療機関等において厳守させること。

(カ) 保存された情報を、外部保存を受託する事業者が独自に提供しないように、医療機関等は契約書等で情報提供について規定すること。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させること。

(キ) 医療機関等において（ア）から（カ）を満たした上で、外部保存を受託する事業者の選定基準を定めること。少なくとも以下の 4 点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

(b) 医療情報等の安全管理に係る実施体制の整備

(c) 実績等に基づく個人データ安全管理に関する信用度

(d) 財務諸表等に基づく経営の健全性

D. 推奨されるガイドライン

(ア) 「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」のうち、医療法人等が適切に管理する場所に保管する場合、保存を受託した機関全体としてのより一層の自助努力を患者・国民に示す手段として、それぞれ個人情報保護及び情報セキュリティマネジメントの認定制度である、プライバシーマークや ISMS 認定等の第三者による認定を取得すること。

(イ) 「②行政機関等が開設したデータセンター等に保存する場合」においては、制度上の監視や評価等を受けることになるが、更なる評価の一環として、（ア）で述べた第三者による認定を受けること。

(ウ) 「②行政機関等が開設したデータセンター等に保存する場合」及び「③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こと。

(エ) 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併せ持つこと。

8.1.3　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、滅失又はき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 20 条、第 22 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、自施設とは異なる他施設や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　外部と診療情報等を含む医療情報を交換する場合の安全管理　B-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、そちらを参照されたい。

C. 最低限のガイドライン

(1) 診療録等の外部保存委託先の事業者内における個人情報保護

①　適切な委託先の監督を行うこと

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、適切な管理を行う必要がある。

(2)　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施設は、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外部の施設に送られ、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。

8.1.4　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　電子的な医療情報を扱う際の責任のあり方」及び「6.11　外部と個人情報を含む医療情報を交換する場合の安全管理」へ考え方を集約したため、それらを参照されたい。

8.1.5　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　電子媒体による外部保存を可搬媒体を用いて行う場合」に掲げる事項についても十分留意すること。

8.2　電子媒体による外部保存を可搬媒体を用いて行う場合

付則１へ移動したのでそちらを参照されたい。

8.3　紙媒体のままで外部保存を行う場合

付則２へ移動したのでそちらを参照されたい。

8.4　外部保存全般の留意事項について

8.4.1　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　組織的安全管理対策」の項を参照されたい。

また、その際の責任のあり方については、「4　電子的な医療情報を扱う際の責任のあり方」を参照されたい。

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。

8.4.2　外部保存契約終了時の処理について

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らない。

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らない。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る。

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契約書等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、事前に廃棄プログラム等の手順を明確化した規定を作成しておくべきである。

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らない。

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らない。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ある。

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る。従って、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らない。

8.4.3　保存義務のない診療録等の外部保存について

「3.4　取扱いに注意を要する文書等」を参照されたい。

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く、7 章の真正性の確保の項を参照されたい。

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**

紙の調剤済み処方せん（薬剤師法第 28 条第 2 項に基づき調剤録への記入が不要とされた場合の調剤済み処方せんを含む。）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、及び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

この項では、この上記のいずれにも該当する、つまり「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」、「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」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。従って、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　（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」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たりすることで、スキャンによる電子化で情報が欠落することがないことを確認すること。
   - 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。
   - 放射線フィルム等の高精細な情報に関しては日本医学放射線学会電子情報委員会が「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)」を公表しており、参考にされたい。
   - 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が必要であり、その点に十分配慮すること。
   - 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い精度であること、及び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範囲であることを念頭に行う必要がある。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、医療機関等の管理責任者は以下の措置を講じること。

- スキャナによる読み取りに係る運用管理規程を定めること。
- 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。
- スキャナで読み取った際は、作業責任者（実施者又は管理者）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い、責任を明確にすること。なお、電子署名については「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」を参照すること。

3. 情報作成管理者は、上記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、改ざんを防止するため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。
   - 一定期間とは改ざんの動機が生じないと考えられる 1～2 日程度以内の運用管理規程で定めた期間で、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こととする。

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。改ざん動機の生じる可能性の低い、「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」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。「9.1　共通の要件」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. 電子化を行うに当たって事前に対象となる患者等に、スキャナ等で電子化を行い保存対象とすることを掲示等で周知し、異議の申立てがあった場合はスキャナ等で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。実施計画書は以下の項目を含むこと。
   - 運用管理規程の作成と妥当性の評価（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））
   - 作業責任者の特定
   - 患者等への周知の手段と異議の申立てに対する対応
   - 相互監視を含む実施の体制
   - 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）
   - 事後の監査人の選定と監査項目
   - 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、及び破棄の方法
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の監査を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行うこと。

４. 外部事業者に委託する場合は、9.1 章の要件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て、契約上に十分な安全管理を行うことを具体的に明記すること。

9.4　紙の調剤済み処方せん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

紙の調剤済み処方せん（薬剤師法第 28 条第 2 項に基づき調剤録への記入が不要とされた場合の調剤済み処方せんを含む。）の電子化とは、紙の処方せん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、紙の処方せん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：薬局で紙の処方せん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せんであっても、その後に内容の修正が発生することを完全には否定出来ない（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せんであっても、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、以下の対策を実施すること。

1. 紙の調剤済み処方せんの電子化のタイミングにより、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せん」を修正する場合、「『元の』電子化した紙の調剤済み処方せん」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せん」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せん」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。

    ・ 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。これは紙媒体が別途保存されるものの、電子化情報に比べてアクセスの容易さは低下することは避けられず、場合によっては外部に保存されるかもしれない。従って、運用の利便性のためとはいえ、電子化情報は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。

- 放射線フィルム等の高精細な情報に関しては日本医学放射線学会電子情報委員会が「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)」を公表しており、参考にされたい。
- 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が必要であり、その点に十分配慮すること。
- 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い精度であること、及び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範囲であることを念頭に行う必要がある。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. 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
－－－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。
－－－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。

Ⅲ　4（2）①個人情報保護に関する規程の整備、公表
－－－個人情報保護に関する規程を整備し、－－－。
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) (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。

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。本指針の 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

- 情報システムで扱う全ての情報のリストアップ
- 安全管理上の重要度に応じた分類
- リスク分析

c) 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

- 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）

を参考にされたい。

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、発生時の対応方法

g) 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
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。

- 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」を参考にされたい。

h) 技術的安全対策規程

- 利用者識別と認証の方法
- IC カード等セキュリティ・デバイス配布の方法
- 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
- アクセスログ取得と監査の手順
- 時刻同期の方法
- ウイルス等不正ソフト対策
- ネットワークからの不正アクセス対策
- パスワードの管理

i) IoT 機器の利用に関する事項

- IoT 機器の貸し出しに関するリスク受容の合意
- 異常時の患者及び医療機関等の役割、連絡先
- 異常の検知方法
- セキュリティ上重要なアップデートの方法
- 使用終了後又は停止中の不正接続対策

j) 無線 LAN に関する事項

- 無線 LAN 設定（アクセス制限、暗号化等）
- 電波障害のおそれがある機器の使用制限

k) 電子署名・タイムスタンプに関する規程

- 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
  - 保守要員専用のアカウントの作成及び運用管理
  - 作業時のデータアクセス範囲の確認
  - 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) 情報処理関連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
  - 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
  - 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

- 医療従事者以外との守秘契約
- 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及び認証

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

- 冗長性
- バックアップ
- 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、ウイルスチェック等）

- 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

- 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
- 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
- 受託事業者が医療機関等以外の場合には、「8.1.2　外部保存を受託する機関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されたい。
- 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該当する機関を選定する場合には、データセンター等の情報処理関連事業者が経済産業省が定めた「医療情報を受託管理する情報処理事業者向けガイドライン」や総務省が定めた「ASP・SaaS における情報セキュリティ対策ガイドライン」及び「ASP・SaaS 事業者が医療情報を取り扱う際の安全管理に関するガイドライン」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
- 受託事業者が医療機関等以外の場合には、「8.1.2　外部保存を受託する機関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されたい。

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

・ 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
施設内保存と同項目（2）③④の確認

b) 標準的なデータ形式及び転送プロトコルの採用（推奨）

c) 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機関内での個人情報の保護

a) 外部保存を受託する機関における個人情報保護

b) 外部保存を受託する機関における診療録等へのアクセス禁止
受託事業者が医療機関等以外の場合には、「8.1.2　外部保存を受託する機関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されたい。

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（実施者又は管理者）の電子署名法に適合した電子署名・タイムスタンプ

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。

従って、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、日常運用あるいは見直しと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

可搬媒体に電子的に保存した情報を外部に保存する場合、委託する医療機関等と受託する機関はオンラインで結ばれないために、電気通信回線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は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。セキュリティ MO 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。

従って、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、媒体が遺失すると、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機関における取扱いや事故発生時について、特に注意する必要がある。

具体的には、以下についての対応が求められる。

(1) 搬送時や外部保存を受託する機関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機関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機関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機関の障害等に対する真正性の確保

①　委託する医療機関等、搬送業者及び受託する機関における可搬媒体の授受記録を行う

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機関の障害等に対する見読性の確保

① 診療に支障が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、そのような場合で、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、あらかじめ内部に保存する必要がある。また、外部に保存しても、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はっきりしており、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機関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。従って、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、滅失又はき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 20 条、第 22 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

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（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、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機関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機関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ついて、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機関､搬送業者に対して個人情報保護法を順守させる管理義務を負う。従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機関内における個人情報保護

外部保存を受託する機関が、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、受託する機関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機関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機関においては、診療録等の個人情報の保護を厳格に行う必要がある。受託する機関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機関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機関は、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機関、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。従って、委託する医療機関等は、受託する機関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。

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　医療機関等の管理者の情報保護責任について」や「4.2　委託と第三者提供における責任分界」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、受託する機関や搬送業者等は、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、搬送業者や委託先の機関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機関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。

従って、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、受託する機関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。

- 委託する医療機関等で発生した診療録等を、外部機関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
- 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
- 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
- 搬送中に情報漏えいがあった場合の対処方法
- 受託する機関と搬送（業）者で可搬媒体を授受する場合の方法と管理方法
- 受託する機関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
- 受託する機関が、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
- 外部保存を受託する機関に、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機関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、受託する機関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、受託する機関も、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機関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、事前に廃棄プログラム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機関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機関が負う責任は、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、以下についての対応が求められる。

（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、滅失又はき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 20 条、第 22 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

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機関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機関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機関、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機関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機関においては、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機関内で、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機関は、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機関内で、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機関は、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。従って、委託する医療機関等は、受託する機関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　医療機関等の管理者の情報保護責任について」や「4.2　委託と第三者提供における責任分界」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、受託する機関や搬送業者等は、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機関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。

従って、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、受託する機関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。

- 委託する医療機関等で発生した診療録等を、外部機関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
- 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
- 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
- 搬送中に情報漏えいがあった場合の対処方法
- 受託する機関と搬送（業）者で診療録等を授受する場合の方法と管理方法。
- 受託する機関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

者から照会があった場合の責任関係
- 受託する機関が、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
- 外部保存を受託する機関に、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機関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、受託する機関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、受託する機関も、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機関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、事前に廃棄プログラム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機関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機関が負う責任は、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。