

参考資料 2

医療情報システムの安全管理に関するガイドライン

第 4.1 版

平成 22 年 2 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	<p>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。</p> <p>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。</p>
第 2 版	平成 19 年 3 月	<p>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、</p> <p>(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。</p> <p>(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。</p>

第3版	平成20年3月	<p>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、</p> <p>(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り扱いに関する基準」を改定。</p> <p>(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。</p>
第4版	平成21年3月	<p>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、より適切な医療分野の情報基盤構築のため、</p> <ul style="list-style-type: none"> <li>「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</li> </ul>

		<p>た安全管理及び運用方策等を更に体系的に検討し、読みやすさにも配慮することとして、「3.3 取り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り扱いに関する基準」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。</p>
第4.1版	平成22年2月	<p>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。</p> <p>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。</p> <p>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り扱いに関する基準」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。</p> <p>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。</p>

## 【目次】

1	はじめに	1
2	本指針の読み方	7
3	本ガイドラインの対象システム及び対象情報	9
3.1	7章及び9章の対象となる文書について	9
3.2	8章の対象となる文書等について	10
3.3	取扱いに注意を要する文書等	11
4	電子的な医療情報を扱う際の責任のあり方	12
4.1	医療機関等の管理者の情報保護責任について	13
4.2	委託と第三者提供における責任分界	14
4.2.1	委託における責任分界	14
4.2.2	第三者提供における責任分界	17
4.3	例示による責任分界点の考え方の整理	17
4.4	技術的対策と運用による対策における責任分界点	21
5	情報の相互運用性と標準化について	23
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	24
5.1.1	基本データセット	24
5.1.2	用語集・コードセット	25
5.2	データ交換のための国際的な標準規格への準拠	26
5.3	標準規格の適用に関わるその他の事項	26
6	情報システムの基本的な安全管理	27
6.1	方針の制定と公表	27
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	29
6.2.1	ISMS 構築の手順	29
6.2.2	取扱い情報の把握	31
6.2.3	リスク分析	31
6.3	組織的安全管理対策 (体制、運用管理規程)	34
6.4	物理的安全対策	36
6.5	技術的安全対策	37
6.6	人的安全対策	45
6.7	情報の破棄	47
6.8	情報システムの改造と保守	48
6.9	情報及び情報機器の持ち出しについて	50
6.10	災害等の非常時の対応	52

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	55
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	73
7	電子保存の要求事項について	76
7.1	真正性の確保について	76
7.2	見読性の確保について	84
7.3	保存性の確保について	87
8	診療録及び診療諸記録を外部に保存する際の基準	92
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	92
8.1.1	電子保存の3基準の遵守	92
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り扱いに関する基準	93
8.1.3	個人情報の保護	100
8.1.4	責任の明確化	102
8.1.5	留意事項	102
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	102
8.3	紙媒体のまま外部保存を行う場合	102
8.4	外部保存全般の留意事項について	103
8.4.1	運用管理規程	103
8.4.2	外部保存契約終了時の処理について	103
8.4.3	保存義務のない診療録等の外部保存について	104
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	105
9.1	共通の要件	105
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	108
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	109
9.4 (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	110
10	運用管理について	112
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	121
付則2	紙媒体のまま外部保存を行う場合	128
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また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。なお、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が、この指針では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関しては本ガイドラインで示すとされている。

今回のガイドラインは、病院、診療所、薬局、助産所等（以下「医療機関等」という。）における診療録等の電子保存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。

また、本ガイドラインは「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」と対になるものであるが、個人情報保護は決して情報システムに関わる対策だけで達成されるものではない。従って、本ガイドラインを使用する場合、情報シ

ステムだけ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ドライン」を十分理解し、情報システムにかかわらない部分でも個人情報保護に関する対策が達成さ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、そのひとつに「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、関連箇所として「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行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」も該当箇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り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来ている。

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来ていることに対し、取り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り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、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り扱いに関する基準」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な存在するため、それらの接続形態毎の脅威を分析した。

これらの検討を踏まえた対応指針を6章の関連する箇所を追記し、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。