資料 I

医療情報システムの安全管理に関するガイドライン

第 3 版

平成 20 年 3 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わる基本的考え方」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 章　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 章　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、更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章　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および情報の取り扱いに関する基準」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。更に、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　情報および情報機器の持ち出しについて」を新設し、留意点を記載。

【目次】

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）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。

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かかわる指針と 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かか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わる基本的考え方」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章　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章　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章　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章　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章　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章　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、更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) および (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、免許資格など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係わる以上、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章　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およ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。

更に、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　情報およ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。

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すべ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。主に電子保存や外部保存を行う場合の運用管理規程の作成に関する指針であるが、電子保存や外部保存を行わない場合でも参考にされたい。

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おおむね、以下の項目にわ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かならず実施しなければならない事項を記載している。
この項にはいくつかの対策の中の一つを選択する場合もあるが、選択を明記している場合以外はすべて実施しなければならない対策である。なお、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がある。後述するように付表の運用管理表を活用し、適切な具体的対策を採用されたい。

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ほうが理解が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はじ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、ひと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**：4. の技術的対策をおこな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すべての情報システムと、それらのシステムの導入、運用、利用、保守及び廃棄にかかわる人または組織を対象としている。ただし以下の３つの章は対象となる文書等が一部限定されている。

第７章の「電子保存の要求事項について」、第８章の「診療録及び診療諸記録を外部に保存する際の基準」、及び第９章の「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、e-文書法の対象範囲となる医療関係文書等として、「厚生労働省の所管する法令の規定に基づく民間事業者等が行う書面の保存等における情報通信の技術の利用に関する省令」（平成１７年厚生労働省令第４４号）、「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律等の施行等について」（平成１７年３月３１日付け医政発第 0331009 号・薬食発第 0331020 号・保発第 0331005 号厚生労働省医政局長・医薬食品局長・保険局長連名通知。以下「施行通知」という。）及び「「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１７年３月３１日付け医政発第 0331010 号・保発第 0331006 号厚生労働省医政局長・保険局長連名通知。以下「外部保存改正通知」という。）で定められた文書等を対象としている。

１．第７章及び第９章の対象文書等（但し、※処方せんについては施行通知第二２（４）の要件を充足のこと。）

一　医師法(昭和２３年法律第２０１号)第２４条の規定による診療録
二　歯科医師法(昭和２３年法律第２０２号)第２３条の規定による診療録
三　保健師助産師看護師法(昭和２３年法律第２０３号)第４２条の規定による助産録
四　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
五　歯科技工士法(昭和３０年法律第１６８号)第１９条の規定による指示書
六　薬剤師法(昭和３５年法律第１４６号)第２８条の規定による調剤録
七　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十七条及び歯科医師法第十七条の特例等に関する法律（昭和６２年法律第２９号）第１１条の規定による診療録
八　救急救命士法(平成３年法律第３６号)第４６条の規定による救急救命処置録
九　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項の規定による帳簿
十　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条の規定による診療録等
十一　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条の規定による調剤録
十二　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の規定による書類
十三　医療法（昭和２３年法律第２０５号）第２１条第１項の規定による記録（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条の規定による記録（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。）、及び第２２条の２の規定による記録（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号に処方せんに限る。）※
十四　薬剤師法(昭和３５年法律第１４６号)第２７条の規定による処方せん※
十五　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条の規定による処方せん※
十六　医療法(昭和２３年法律第２０５号)第２１条第１項の規定による記録（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。）、第２２条の規定による記録（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。）、及び第２２条の２の規定による記録（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。）
十七　歯科衛生士法施行規則(平成元年厚生省令第４６号)第１８条の規定による歯科衛生士の業務記録
十八　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

２．第８章の対象文書等

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５１条の２第１項及び第２項に規定されている事業報告書等及び監事の監査報告書の備置き
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　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
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十七条及び歯科医師法第十七条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

8　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
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項に規定されている帳簿
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条に規定されている診療録等
１１　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
１２　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
１３　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

4　電子的な医療情報を扱う際の責任のあり方

医療に関わるすべ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、情報の取扱いも同様である。

情報の取扱いについては、情報が適切に収集され、必要に応じて遅滞なく利用できるように適切に保管され、不要になった場合に適切に廃棄されることで、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および指針の他、診療情報の扱いに係わる法令、通知、指針等により定められている要件を満たすことが求められる。故意に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うるから、いずれにしろ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。問題はいかなる管理が適切であるか否かであるが、法律的な用語では、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る。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り、本ガイドラインは、医療情報を電子的に取り扱う際の善管注意義務をできるだけ具体的に示したものである。

医療情報を電子的に取り扱う場合といっても、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、紙の媒体やフィルムなど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こと、漏えい等の事態が生じた場合に一瞬かつ大量に情報が漏えいする可能性が高いこと、さらに医療従事者が情報取扱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ことなど、固有の特殊性もある。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計画を選択して、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、昨今のブロードバンドに代表されるようなネットワークおよびその技術の進展から、電子化された医療情報が医療機関等の施設内だけに存在するという状況から、空間的境界を越えてネットワーク上に広がって存在することも現実のものとなってきた。

このような状況の下では、医療情報の管理責任が医療機関等の管理ばかりでなく、ネットワーク上の空間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。その際、必要となる新たな概念としては責任分界点が挙げられる。

本章では、電子的な医療情報を取り扱う際の責任のあり方として、医療機関等の管理者の責任の内容と範囲およ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提供する場合と第三者提供した場合の責任分界点について整理する。

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保護するべく善管注意義務を果たすためには、さまざまな局面で注意を払う必要がある。ここでは、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）が生じた場合にいかなる対処をすべきかという意味での責任とに分けて解説する。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に医療機関等の管理者が何をすべきかを示す概念である。それは何よりも適切な情報管理ということになるが、実際には、単に適切な情報管理を行っているばかりでなく、そのような体制が適切にとられていることを患者をはじめとする外部に示す責任（説明責任）と、定期的に情報保護システムを評価し改善を図る責任を含む必要がある。

そこで、本ガイドラインにおける医療機関等の管理者の通常運用における責任は、「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」に３分し、以下にそれぞれの責任内容を整理する。

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計画が、その取り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。

説明責任を果たすためには、システムの仕様や運用計画を明確に文書化する必要がある。また、仕様や計画が当初の方針の通りに機能しているかどうかを定期的に監査し、その結果もあいまいさのない形で文書化し、また監査の結果問題があった場合は、真摯に対応するのはもちろんのこと、その対応の記録も文書化し、第三者が検証可能な状況にすることが必要である。

② 管理責任

当該システムの運用管理を医療機関等が行う責任である。医療情報を取り扱う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。少なくとも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う必要がある。

個人情報保護法上は個人情報保護の担当責任者を定める必要があり、電子情報化された個人情報の保護について一定の知識を有する担当責任者を決めて、請負事業者との対応にあたる必要がある。

③ 定期的に見直し必要に応じて改善を行う責任

当該情報システムの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く責任である。特に、情報保護に関する技術は日進月歩であり、旧態依然の情報保護体制ではすぐに時代遅れになる可能性がある。

従って、医療機関等の管理者は、医療情報保護のシステム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

① 説明責任

医療情報について何らかの事故（典型的には漏えいの事態）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ある。

説明は個々の患者に対するものであると同時に、特に医療機関等は一定の公共性を有しているので、監督機関である行政機関や社会への説明・公表が求められている。

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。

その責任は、１）原因を追及し明らかにする責任、２）損害を生じさせた場合にはその損害填補責任、３）再発防止策を講ずる責任に分けられる。

事故が、適切な委託契約に基づき医療情報の処理を委託した事業者の責任による場合、法律上、医療機関等の管理者の善管注意義務については、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責任はないことになるが、本ガイドラインの下では、患者に対する関係では、選任監督の注意を払っていてもなお上記３つの意味での善後策を講ずる責任を免れるものではない。

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おり、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、管理者の責任を免れさせるのは不適当と考えられるからである。また、現実的にも、受託する事業者が医療情報のすべ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うほかないこともある。

ただし、事故の原因が受託する事業者にある場合に、医療機関等と当該事業者との間の責任分担をどのようにするかはまた別の問題であり、この問題は次の責任分界点の項目で扱う。

4.2 責任分界点について

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種類があり、医療機関等の管理者の責任のあり方には大きな違いがある。

委託の場合、それが第三者委託と呼ばれることがあるにしても、医療情報は医療機関等の管理者の業務遂行目的のために委託されるのであり、大きな意味で管理者の支配下にある。前項で述べたように、本ガイドラインでは、患者に対する関係では、受託する事業者の過失による事故についても医療機関等の管理者が責任を免れるものではないと整理したところでもある。

これに対し、医療情報の第三者提供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、提供された部分の情報については、もはや管理者ではなく第三者に情報を適切に保護する責任が生ずる。医療機関等の管理者にとっては、原則として、第三者提供の正当性だけが問題となり、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る。

ただし、情報の特異な性格のため、医療機関等の側で当該情報を削除しない限り、情報が第三者提供されたからといってなお医療機関等のもとにも残るため、それに関し適切な情報管理責任が残ることはいうまでもない。さらに、情報処理関連事業者の手を経て情報提供が行われる場合には、いかなる時点で、第三者に提供されたことになるかということを明らかにすべきである。

A. 委託

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い、万一、何らかの事故が生じた場合にも、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る。

ただし、これとは別に、受託する事業者の責任による事故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り、以下にその原則を掲げる。

(1) 通常運用における責任について

① 説明責任

医療情報を実際に扱う受託事業者と医療機関等の管理者との間における説明責任の分担については、次のように考えられる。

患者等に対し、いかなる内容の医療情報保護のシステム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。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

同様に、管理責任の分担については、次のように考えられる。

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事故（典型的には漏えいの事態）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。そのため予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

前項で述べたように、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。

その責任は、１）原因を追及し明らかにする責任、２）損害を生じさせた場合にはその損害填補責任、３）再発防止策を講ずる責任に分けられる。

事故が受託する事業者の業務範囲と関係する場合、受託する事業者との協力と責任分担の下に上記の責任を果たす必要がある。

既に述べたように、患者に対する関係では、医療機関等の管理者は、受託する事業者の選任監督に十分な注意を払っている場合でも善後策を講ずる責任を免れることはできない。ただし、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り、

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すべ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押し付け合いをするよりも、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ため、委託契約においては、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など、さまざまに考慮すべき要素があり、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。

B. 第三者提供

医療機関等が医療情報について第三者提供を行う場合、個人情報の保護に関する法律（平成15年5月30日　法律第57号）第２３条および「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」を遵守する必要がある。

いったん適切・適法に提供された医療情報については提供元の医療機関等に責任はない。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。

また、医療情報が電子化され、ネットワーク等を通じて情報を提供する場合、第三者提供の際にも、医療機関等から提供先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、言い換えれば、情報処理関連事業者の処理する段階にある時点で何らかの事故が生じた場合の責任の所在について明らかにする必要が生ずる。

第三者提供の主体は提供元の医療機関等であることからみて、患者に対する関係では、少なくとも情報が提供先に到達するまでは、原則として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、情報処理関連事業者および提供先との間で、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、医療機関等・情報処理関連事業者・提供先の間で予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すべての責任を負うのが原則である。

4.3　例示による考え方の整理

本項では「4.2　責任分界点について」について、いくつか例を挙げて解説する。ただし、本項は4.2の考え方を例として考えた場合であるため、医療情報システムの安全管理や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章を参照すること。

A. 地域医療連携で患者情報を交換する場合

Ⅰ　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

提供元医療機関等と提供先機関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などで合意しておく。

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および、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、事後責任は、委託の場合は、原則として提供元医療機関等にあり、第三者提供において適切に情報が提供された場合は、原則として提供先医療機関等にあり、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について述べる。

この場合、あらかじめ提供先または提供先となる可能性がある機関を特定できる場合は、委託または第三者提供の要件に従って両機関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。

更に、提供元医療機関等と提供先機関が１対Ｎ通信で、提供先機関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。

Ⅱ　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、4.2 で述べた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。

III 外部保存機関が介在する場合の考え方

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およ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および情報の取り扱いに関する基準」で定める保存機関毎に「2. 情報の取り扱い」および「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 を参照されたい。

B. 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

I 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係わることになる。

更に、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、公衆回線など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」となることに留意しなくてはならない。

II 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。

なお、「I　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」、「II　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」のどちらにおいても、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の外部から接続する場合」を参照されたい。