2.6.10. アプリケーションに対するセキュリティ要求事項
2.6.11. 暗号による管理策
2.6.12. ログの取得及び監査
2.6.13. アクセス制御方針
2.6.14. 作業者アクセス及び作業者ＩＤの管理
2.6.15. 作業者の責任及び周知
2.7. 人的安全対策
2.8. 情報の破棄
2.9. 医療情報システムの改造と保守
2.10. 医療情報処理に関する事業継続計画
2.10.1. 要求事項の識別
2.10.2. 事業継続計画の立案及びレビュー
３．ガイドラインの見直し

１．はじめに

このガイドラインは、個人情報の保護に関する法律（平成15年法律第57号。以下「法」という。）第７条第１項に基づき平成16年４月２日に閣議決定された「個人情報の保護に関する基本方針」（以下、「基本方針」という。）を踏まえ、また、法第６条及び第８条に基づき法に定める事項に関して必要な事項を定め、医療機関等から医療情報を受託する事業者となる立場の情報処理事業者等（以下、「医療情報受託者」という。）が行う個人情報の適正な取扱いの確保に関する活動を支援する具体的な指針として定めるものである。

医療情報については、基本方針及び国会における附帯決議において、個人情報の性質や利用方法等から、特に適正な取扱いの厳格な実施を確保する必要がある分野の一つであると指摘されており、安全管理措置に関して積極的な取組が求められている。

他方、医療情報受託者には、「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」（以下、「経済産業分野ガイドライン」という。）の規定が適用されているが、経済産業分野ガイドラインは、多様な業種の事業者が広汎な種類の個人情報を取り扱うことを想定しているため、機微性の高い医療情報の取扱いに携わる医療情報受託者に対しては、同ガイドラインで規定される安全管理措置よりも十分な安全管理措置が求められる。

本ガイドラインは、法の趣旨を踏まえ医療情報受託者における個人情報の適正な取扱いが確保されるよう、医療情報受託者が講ずべき措置に関連する項目を挙げている。

本ガイドラインのうち、「２．医療情報を受託管理する情報処理事業者における安全管理上の要求事項」に記載されている項目については、それに従わなかった場合、経済産業大臣により法の規定違反と判断され得る。

なお、本ガイドラインに記載されている各項目に取り組むに当たっては、本ガイドラインに関する参考資料「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第２版（経済産業省、平成24年10月）」の内容を十分に理解することが必要である。

1.1. 本ガイドラインで用いる医療情報用語の説明

本ガイドラインで扱う医療情報に関する特有の用語について、法令及びガイドライン類にて定義されている用語のうち、本ガイドラインの理解に必要なものについて以下に示す。なお、本ガイドラインにおいて「医療情報」とは、医療に関する患者情報（個人識別情報）を含む情報という意味で用いている。

【診療録】

医師及び歯科医師が患者を診療した経過を記録したもの。カルテとも呼ばれ、診療終了後所定年限（５年等）の保存が義務づけられている。医師法施行規則第23条及び歯科医師法施行規則第22条により「診療を受けた者の住所、氏名、性別及び年齢、病名及び主要症状、治療方法（処方及び処置）、診療の年月日」が記載事項とされている。

【診療記録】

診療録、処方せん、手術記録、看護記録、検査所見記録、エックス線写真、紹介状、退院した患者に係る入院期間中の診療経過の要約その他の診療の過程で患者の身体状況、病状、治療等について作成、記録又は保存された書類、画像等の記録をいう。本ガイドラインに基づき安全管理策を実施する際には、情報の種類に応じたリスク評価を行い、必要な安全レベルを考慮した安全管理策を選択することが求められる。

【患者情報】

上記の記録類に記載されている情報のうち、患者の既往歴、家族歴、嗜好等のこと。高度なプライバシー情報であり、医療機関等にとっては守秘義務が課せられていることからも、機密性への高い配慮が求められる。なお、要介護者は言葉の定義としては患者には含まれないと考えられるが、その情報は同様に高度なプライバシーに関する情報であることから、要介護者の情報についても患者情報と同等と考え、要介護者情報を扱うシステムは下記の医療情報システムに含まれるものとする。

なお、これらのプライバシーに関する情報は、疾患に伴って医療機関等にかかった患者の情報に限らず、例えば介護保険申請時に主治医が主治医意見書を作成する際に行った問診情報も含まれると解される。従って、患者情報は疾患に係わり収集された既往歴等だけに限らないことに留意しなくてはならない。

【医療情報システム】

医療において発生する患者情報を含む医療情報を、情報処理事業者が受託管理するためのシステムを指す。

【医療機関等】

主に病院、診療所、薬局、助産所等を指す。

1.2. 本ガイドラインで用いる制度及び技術用語の説明

本ガイドラインで扱う制度及び技術用語について、本ガイドラインの理解に必要なものについて以下に示す。

【ＩＳＭＳ（情報セキュリティマネジメントシステム）】

ＩＳＭＳ適合性評価制度では、「ＩＳＭＳとは、個別の問題毎の技術対策の他に、組織のマネジメントとして、自らのリスクアセスメントにより必要なセキュリティレベルを決め、プランを持ち、資源配分して、システムを運用することである。」と定義している。ＩＳＯ（国際標準化機構）のマネジメントモデルに準拠しており、Ｐ（Plan）、Ｄ（Do）、Ｃ（Check）、Ａ（Act）サイクルを継続することで組織的な改善を図ることを特徴とする。

【ＪＩＳ　Ｑ　27001：2006】

ＩＳＭＳの国際標準規格としてＩＳＯ／ＩＥＣ　27001：2005が定められており、これに対応する日本工業規格としてＪＩＳ　Ｑ　27001：2006（情報セキュリティマネジメントシステム要求事項）が定められている（以下、「ＪＩＳ　Ｑ　27001」という。）。

【ＩＳＭＳ適合性評価制度】

ＩＳＭＳ適合性評価制度は、ある組織が構築したＩＳＭＳがＪＩＳ　Ｑ　27001に適合しているかどうかを「認証機関」が審査して、認定された場合には「認定機関」に登録を行う仕組みである（以下、「ＩＳＭＳ評価制度」という。）。ＩＳＭＳ認定を受けて登録されることを「ＩＳＭＳ認証を取得する」とも呼ぶ。

【ＪＩＳ　Ｑ　15001：2006】

通商産業省（現在の経済産業省）が作成した「民間部門における電子計算機処理に係る個人情報の保護に関するガイドライン」を基礎として、1999年に制定された。その後、「個人情報の保護に関する法律」が2003年に制定され、規格の取り巻く環境は大きく変化したことから、2006年改正を行い、個人情報の保護に関する法律に基づく個人情報保護ルール及びマネジメントシステムを併せもった規格となった（以下、「ＪＩＳ　Ｑ　15001」という。）。