資　料　3

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版（案）

削除: 3

平成　　年　　月

削除: 20

削除: 3

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。

削除: 3 月

削除: 3 月

削除: 1 月

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及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　　年　月	

削除: および

削除: および

【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、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）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

削除: １１年４月
削除: １１年４月２２日付け
削除: １４年３月
削除: １４年３月２９日付け
削除: １６年
削除: 第１４９号。
削除: １５年６月
削除: １６年９月
削除: １１
削除: 4
削除: ２２
削除: １４年５月３１日付け
削除: １６年１２月
削除: １７年４月
削除: １５年
削除: 第５７号。

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関わる基本的考え方」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。

削除: 係わる

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) 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。

削除: および

「(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。

削除: など

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。

削除: 係わる

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及び情報の取り扱いに関する基準」を改定している。

削除: および

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。

削除: および

【第４版】

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。

削除: 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必ず実施しなければならない事項を記載している。

削除: かならず

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、いく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。

削除: 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、

削除: がある。後述するように

削除: されたい

削除: が

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」は対象となる文書等が一部限定されている。

削除: ただし以下の 3 つの章

3.1　第 7 章及び第 9 章の対象となる文書について

医療に関する文書は、法令等によって作成や保存が定められている文書と、そうでない文書に大別できる。第 7 章及び第 9 章の対象となる文書は、法令による作成や保存が定められている文書の一部であり、具体的には、e-文書法の対象範囲となる医療関係文書等として、「厚生労働省の所管する法令の規定に基づく民間事業者等が行う書面の保存等における情報通信の技術の利用に関する省令」（平成 17 年厚生労働省令第 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。）で定められた下記の文書等を対象としている。

削除: 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」、…び第 9 章の「診療…

削除: １７年…7 年厚生労働省令第４４号…

削除: 「「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。

第 7 章及び第 9 章…9 章の対象文書等（但…

○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 条の診療録

削除: ２３年…3 年法律第２０１号)第２４…

二　歯科医師法(昭和 23 年法律第 202 号)第 23 条の診療録

削除: ２３年…3 年法律第２０２号)第２３…

三　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

削除: ２３年…3 年法律第２０３号)第４２…

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

削除: ２３年…3 年法律第２０５号）第５１…

五　歯科技工士法(昭和 30 年法律第 168 号)第 19 条の指示書

削除: ３０年…0 年法律第１６８号)第１９…

六　薬剤師法(昭和 35 年法律第 146 号)第 28 条の調剤録

削除: ３５年…5 年法律第１４６号)第２８…

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 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

削除: 第十七条…17 条及び歯科医師法第十…

八　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

削除: ３年…年法律第３６号)第４６条の規…

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 項の帳簿

削除: ２３年…3 年厚生省令第５０号）第３…

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 条の診療録等（作成については、同規則第 22 条）

削除: ３２年…2 年厚生省令第１５号)第９…

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 条の調剤録

削除: ３２年…2 年厚生省令第１６号)第６…

（作成については、同規則第 5 条）

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 の書類（作成については、同規則第 12 条第 14 号及び第 15 号）

十三　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。）、及び同法第 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。）、及び同法第 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。）

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

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、たと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。

3.2　第 8 章の対象となる文書等について

第 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 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 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

削除: ３３年...3 年厚生省令第２４号）第１...

削除: ２３年...3 年法律第２０５号）第２１...

削除: ３５年...5 年法律第１４６号)第２７...

削除: ３２年...2 年厚生省令第１６号)第６...

削除: ２３年...3 年法律第２０５号)第２１...

削除: 第４６号)第１８条の規定による

削除: ２６年...6 年法律第２２６号）第２８...

削除: <#>第８章の対象文書等 .

.

1

削除: ２３年...3 年法律第２０１号)第２４...

削除: ２　…科医師法(昭和２３年...3 年法...

削除: ３　…健師助産師看護師法(昭和２３...

削除: ４　…療法（昭和２３年...3 年法律第...

削除: ５　…療法(昭和２３年...3 年法律第...

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

3.3　取扱いに注意を要する文書等

3.1に示した文書等の他、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、第7章及び第9章に準じて取扱うこと。

なお、9.4章の「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、第8章に準じて取扱うこと。

削除: 6
削除: ３０年
削除: 第１６８号)第１９条
削除: 7
削除: 第十七条
削除: 第十七条
削除: ６２年
削除: 第２９号）第１１条
削除: 8
削除: 3年
削除: 第３６号)第４６条
削除: 9
削除: ２３年
削除: 第５０号）第３０条の２３第１項
削除: 第２項
削除: １０
削除: ３２年
削除: 第１５号)第９条
削除: １１
削除: ３３年
削除: 第２４号）第１２条
削除: 3
削除: １２
削除: 第４６号)第１８条
削除: １３
削除: ２６年
削除: 第２２６号）第２８条
削除: - - - - - - - - - - - - - - - - - -

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、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および指針の他、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。

したがって、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、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有するばかりでなく、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。

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。

削除: .
情報の取扱いについては、情報が適切に
削除: され、必要に応じて遅滞なく利用できるように適切に
削除: され、不要になった場合に適切に廃棄されることで、
削除: 係わる
削除: こと
削除: なりうるから、いずれにしろ
削除: 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、
削除: 求められる。
削除: あり、本ガイドラインは、医療情報 ...
削除: 医療情報を電子的に取り扱う場合と ...
削除: 、
削除: 、
削除: など、固有の特殊性もある。従って
削除: 昨今のブロードバンドに代表される ...
削除: から、空間的境界
削除: 越えてネットワーク上に広がって存 ...
削除: 医療情報の
削除: が
削除: の管理
削除: その際、必要となる新たな概念とし ...
削除: を取り扱う際の責任のあり方として、
削除: および
削除: 提供
削除: の責任分界点について
削除: 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、通常の運用時から払われているべき、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。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計画を明確に文書化すること
・ 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あたる必要がある。

・ 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恐れがあ

削除: 保護
削除: べく
削除: さまざまな局面で注意を払う必要が…
削除: いかなる
削除: かという意味での
削除: に分けて解説する。
削除: に医療機関等の管理者が何をすべき…
削除: 実際には、単に
削除: 行っているばかり
削除: そのような体制が適切にとられてい…
削除: そこで、本ガイドラインにおける医…
削除: 。…
削除: 必要がある。また、
削除: し、その
削除: も
削除: し、また
削除: のはもちろんの
削除: 、その
削除: も
削除: が必要である。
削除: 当該システムの運用管理を医療機関…
削除: 。
削除: 受け、
削除: 必要がある。
削除: 担当
削除: 必要があり、電子情報化
削除: 担当
削除: 決めて、請負事業者との対応にあた…

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。

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

・原因といかなる対処法をとる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。

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

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

削除: し、

削除: 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

削除: 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

削除: <#>説明責任 .

削除: 説明は個々の患者に対するものであると同時に、

削除: 有しているので、…するため、個々

削除: 医療情報について何らかの事故が生じた場合、…た、医療機関等の管理者には

削除: 、

削除: 、…）再発防止策を講ずる責任に分

削除: 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。 .

削除: 分界点について

削除: 2…種類があり、…るため、それぞ

削除: 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

削除: ・…・「管理責任・…・「定期的に見

削除: 事故…都合な事態が生じた場合にも

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為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。

削除: 事故

削除: あり、以下にその

削除: 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。

削除: システム

削除: 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。

削除: 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。

削除: 事故（典型的には漏えいの

削除: ）

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。

とはいえ、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ので、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わざるを得ない。

医療機関等の管理者は、患者に対して、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、の善後策を講ずる責任を免れるものではない。

医療機関等の管理者の、患者等に対するすべ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。

その為には、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。

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、個人情報の保護に関する法律（平

削除: 前項で述べたように、
削除: 。
その
削除: は
削除: 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
削除: ことはできない。ただし
削除: 押し付け合いをするよりも
削除: ため、
削除: おいては
削除: B.

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。

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たからといっ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。したがって、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。

また、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言うべき概念が新たに発生する。

いったん適切・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は、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、情報処理関連事業者および送信側との間で、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、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、いく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章を参照すること。

(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

削除: 第２３条

削除: いったん適切・適法に

削除: された

削除: については提供元の

削除: 責任

削除: ない。

削除: 提供先

削除: 言い換えれば、

削除: 処理

削除: 段階に

削除: 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。

削除: 提供元

削除: 提供先

削除: 提供先

削除: 医療機関等・情報処理関連事業者・提供先の間で

削除: 「4.2

削除: について」

削除: 4.2の

削除: 考えた場合である

削除: A.

削除: I

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。

削除: など

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。

削除: および

ただし、委託の場合は、通常運用における責任、事後責任は、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。

削除: は、委託の場合

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。

削除: 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医療機関等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。

更に、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

削除: II

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。

削除: 4.2で述べた

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

削除: Ⅲ

削除: の

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」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を参照されたい。

削除: および

削除: および

削除: および

(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

削除: B.

削除: Ⅰ

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。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。

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」となる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。

(1) 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。

削除: 係わる

削除: など

削除: Ⅱ

削除: 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。

C.

医療機関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機微な情報の取り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。

削除: など

(2) 法令で定められている場合

削除: D.

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も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。

削除: など

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も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

削除: 【参考】

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（ベンダー）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、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第10章と付表を参考にし、「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。

削除: する

5　情報の相互運用性と標準化について

本ガイドラインの大部分は医療にかかわる情報の様々な程度の電子化を前提としている。医療機関等において電子化された情報を扱うシステムを導入する目的は、当初事務処理の合理化だけであったが、現在は平成 13 年に作成された「保健医療分野の情報化にむけてのグランドデザイン」でも明確に記載されているように、情報共有の推進や、医療安全、医療の質の向上に寄与できるものへと拡張されてきている。これらの目的を達成するためには、統合的な医療情報システムを構成する個々のシステムが相互に情報交換を行えなければならない。情報システムが相互に情報交換を行い、交換された情報がそれぞれの情報システムで利用可能であることを、情報システムに相互運用性があるというが、医療情報の標準に基づく相互運用性が必要となっている。

本ガイドラインは医療に関係する情報システムの安全な管理・運用に関して指針を提供することを目的としている。情報の安全性の重要な要素の一つとして、必要時に情報が利用可能であること（以下、「可用性」という）が挙げられる。可用性は、情報を利用する任意の時点で確保されなければならない。例えば、医療機関等で医療情報を長期間保存する際、システム更新に伴い旧システムで保存された医療情報を確実に利用できる「相互運用性」を確保することは、見読性及び保存性の確保の点からみても電子保存を行う医療情報システムの必須の要件である。

医療に有用な意味のある情報を長期間にわたり利用可能な形で保存するためには、将来にわたりメンテナンスを継続することが期待される標準的な用語集やコードセットを利用するか、それらに容易に変換可能な状態で保存することが望ましい。

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

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。さらに、基本データセットの利用において、医療情報システム開発センター（MEDIS-DC）が整備する標準マスターと組み合わせることによって、容易にデータの互換性を確保できることが相互運用性実証事業で行われた実証実験で示された。

現在基本データセットとして以下に示す情報項目が定義されている。

① 利用者情報
② 患者情報（基本情報）
③ 患者情報（感染症、アレルギー情報、入退院歴、受診歴）
④ オーダ情報（処方、検体検査、放射線）
⑤ 検査結果情報（検体検査）

削除: 利用性
削除: 処理
削除: は
削除: の
削除: であることが求められて
削除: 実現
削除: 適切な標準化が必要であることは論を待たない。
削除: が、
削除: を確保する
削除: を上げること
削除: できる。 .
削除: 保持しなければならない
削除: 伴い新旧のシステム間での情報の互換性を保ち旧
削除: 読み出せるという、「新旧システムで医療情報の
削除: 利用性
削除: 電子保存の
削除: 原則
削除: 読み出し
削除: 出来る限り利用して
削除: を行うことが
削除: 標準的な用語集
削除: すでに公開されている用語集やコードセットのうち、日本での各分野
削除: 実質的な標準的用語コード集と考えられるものについては情報の保存の際にこ
削除: 必要

⑥　病名情報
⑦　注射に関わる指示、実施情報等
⑧　処置・手術

必要なもの全てが整備されたわけではないが、ここに示したような情報項目を利用することにより、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、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。

- 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

なお、基本データセットの詳細については相互運用性実証事業を紹介した以下の Web サイトにあるので参照されたい。

医療情報システムにおける相互運用性の実証事業報告書
http://www.jahis.jp/sougounyou/sougounyou_top.html

削除: ある。以下に

また、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
http://www.jahis.jp/standard/seitei/st07-102/st07-102.htm

標準的な用語集やコードセットは、MEDIS-DC で以下のような対象について整備開発や保守が行われている。

削除: 例

病　　名：ICD10 対応電子カルテ用標準病名マスター
手術・処置：標準手術・処置マスター
臨床検査：標準臨床検査マスター（生理機能検査を含む）
医　薬　品：標準医薬品マスター
医療機器：標準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・所見標準マスター
歯 科 病 名 ：標準歯科病名マスター
歯科手術等：標準歯科手術・処置マスター
画 像 検 査 ：標準画像検査マスター
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 標準マスター類は以下の URL から取得できる。
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。また、医療情報標準化推進協議会（Health Information and Communication Standards Board：HELICS 協議会）がわが国で推奨されるべき標準的用語集やコードセットの登録を進めているので随時参照されたい。

5.2 データ交換のための国際的な標準規格への準拠

一般的に医療情報システムは複数のシステムから構成された統合的なシステムとなっている。相互運用性の確保には、情報の交換を標準化されたデータ交換規約を用いることも含まれる。医療情報では、HL7（Health Level Seven）や DICOM（Digital Imaging and Communications in Medicine）が国際的な標準となっている。標準化されたデータ交換規約をシステム構築に適用することは、可用性が保証されたシステム構築を進めるという意味で重要である。

これらの標準の中で、我が国の医療に適合するものについては、直接採用するか、少なくともこれらの標準に適合した情報形式に容易に変換可能な状態にすることを強く推奨する。我が国において利用可能な標準データ交換規約として、例えば以下の規格を保健医療福祉情報システム工業会（JAHIS）が制定している。

1. JAHIS 臨床検査データ交換規約
2. JAHIS 処方データ交換規約
3. JAHIS 健診データ交換規約
4. JAHIS 放射線データ交換規約
5. 介護メッセージ仕様
6. 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
7. JAHIS 生理検査データ交換規約
8. JAHIS 病名情報データ交換規約
9. 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

削除: あげるが
削除: の用語集
削除: 標準案の
削除: おり、
削除: 病名：ICD10 対応電子カルテ用標準病名マスタ．
医薬品名：標準医薬品マスタ．
臨床検査:JAHIS 臨床検査データ交換規約
．
．
．
．
削除: 、HL7（Health Level Seven）等の規格及びこれらの規格の標準的な運用方法を定めた IHE（Integrating the Healthcare Enterprise）は、
削除: や規格として提唱され、一部はわが国でも利用が進んでいる
削除: 国際的な
削除: や規格
削除: 情報の相互利用性の観点から
削除: これらの規格や標準を
削除: 規格や
削除: しておく
削除: が
削除: される

10. JAHIS 内視鏡データ交換規約

これらの規約は以下の URL で取得できる。

http://www.jahis.jp/standard/index.html

削除: また、

5.3 標準規格の適用に関わるその他の事項

医療情報の標準規格への対応については、HELICS 協議会が我が国で推奨すべき標準規格を医療情報標準化指針として紹介している。また、厚生労働省の保健医療情報標準化会議においても HELICS 協議会が指針として掲げた標準規格の内我が国で必要不可欠と考えられるものについては取り上げる方向で検討を進めている。

最後に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。

削除: JIS 文字コード

削除: ような容易

削除: 移行可能な文字セット以外の文字を

削除: してもちいた

削除: そのような

削除: 標準化の観点から見れば外字を使用する必要がない文字セットが検討されることを期待したい。

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、行政機関の保有する個人情報の保護に関する法律（平成15年法律第58号）、独立行政法人等の保有する個人情報の保護に関する法律（平成15年法律第59号））に規定された安全管理・確保に関する条文によって法的な責務として求められている。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。安全管理をおろそかにすることは上記法律に違反することになるが、医療においてもっとも重要なことは患者等との信頼関係であり、単に違反事象がお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。

削除: １５年

削除: 第５８号

削除: １５年

削除: 第５９号

A.　制度上の要求事項

（安全管理措置）

法第二十条　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）

法第二十一条　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）

法第二十二条　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）

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ドライン」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。

削除: でも

削除: められているが、

削除: 上記の

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 27001:2006（情報セキュリティマネジメントシステム-要求事項）」で、下記のように定めている。

ISMS 基本方針を、事業・組織・所在地・資産・技術の観点から、次を満たすように定義する。
1) 目的を設定するための枠組みを含め、また、情報セキュリティに関係する活動の方向性の全般的認識及び原則を確立する。
2) 事業場及び法令又は規制の要求事項、ならびに契約上のセキュリティ義務を考慮する。
3) それのもとで ISMS の確立及び維持をする、組織の戦略的なリスクマネジメントの状況と調和をとる。
4) リスクを評価するに当たっての基軸を確立する。
5) 経営陣による承認を得る。

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

A. 制度上の要求事項

（安全管理措置）

法第二十条　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）

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 27001:2005）ならびに JIS（JIS Q 27001:2006）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。

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。

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。

削除: など

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おこなわれているかについてJIPDEC（財団法人 日本情報処理開発協会）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医師が処方箋を出し、②処方箋が薬剤部に送られ、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）

削除: など）

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すで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おのずと見え、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言える。

削除: など

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、維持して行く。

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言える。

削除: など

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すべてリストアップし、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。この他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、患者等にきわめて深刻な影響を与える可能性があり、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。

削除: 一般に

削除: が個人識別可能な状態で

削除: もっとも

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を元に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、たとえ起こりえる可能性は低くても、万が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。この分析の結果えられた脅威に対して、6.3～6.11 の対策を行うことになる。

特に安全管理や、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。

削除: 個人情報保護関連各法

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恐れのある個人情報を保護するための方策を考える必要がある。以下にさまざま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 医療情報システム自身
(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

これらの脅威に対し、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になる。

C. 最低限のガイドライン

1. 情報システムで扱う情報をすべ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. この分析の結果得られた脅威に対して、6.3～6.11 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かか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きわめて重要であり、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

削除: 運用管理規程には必ず以下の項目を含めること。

削除: .
<#>理念（基本方針と管理目的の表明）.
<#>医療機関等の内部の体制、外部保存に関わる外部の人及び施設.
<#>契約書・マニュアル等の文書の管理.
<#>機器を用いる場合は機器の管理.
<#>患者等への説明と同意を得る方法.
<#>監査.
<#>苦情の受け付け窓口.
.

削除: および

削除: および

(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・質問の受け付け窓口

削除: リスクに対する予防、発生時

削除: 対応の

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幾つかのセキュリティ区画を定義し、以下の事項を考慮し、適切に管理する必要がある。

① 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）
② 盗難、窃視等の防止
③ 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

削除: および

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。

削除: および

削除: および

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出来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う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. 窃視防止の対策を実施すること。

削除: 権限者

削除: こと

削除: こと

削除: 離席時にも端末等での正当な権限者以外の者による

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。

削除: 1.