第２０回医療情報ネットワーク基盤検討会
議　事　次　第

平成２０年１２月１９日（金）

中央合同庁舎第５号館

共用第７会議室

１０：００ ～ １２：００

１．開　会

２．議　事

(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

(3) その他

３．閉　会

【資　料】

資料１　医療情報ネットワーク基盤検討作業班の開催について

資料２　医療情報システムを安全に管理するために（案）

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）

資料４　ユースケース図

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

資料Ⅱ　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

資料Ⅲ　ＡＳＰ・ＳａａＳにおける情報セキュリティ対策ガイドライン

資　料　1

平成２０年７月３０日

医療情報ネットワーク基盤検討作業班の開催について

1　開催趣旨

医療情報ネットワーク基盤検討会（以下「検討会」という。）における検討事項につき、実務的・技術的な検討や具体的な作業を行うため作業班を開催する。

2　検討事項

(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　等

3　班員

作業班の班員は別紙のとおりとする。

4　運営等

(1)　作業班に班長を１名置き、班長は副班長を指名することができる。
(2)　副班長は班長を補佐し、班長が不在の場合はその職務を行うこととする。
(3)　作業班は非公開とするが、検討過程、検討結果については、検討会において報告・議論を行こととする。
(4)　班長は必要に応じ、検討に必要な有識者等の参集を求めることが出来る。
(5)　その他、作業班の運営に関し必要なことについては、班長が決定することとする。

5　庶務等

作業班は医政局研究開発振興課長が招集し、その庶務は研究開発振興課が行うこととする。

別　紙

「医療情報ネットワーク基盤検討会」
医療情報ネットワーク基盤検討作業班
班　　員
（平成20年7月現在）

班　員	所　属　・　職　名
稲垣　明弘	日本歯科医師会常務理事
岡田　　康	保健医療福祉情報システム工業会 セキュリティ委員会副委員長
喜多　紘一	東京工業大学統合研究院ソリューション研究機構特任教授
河野　行満	日本薬剤師会事務局業務部医薬・保険課　課長補佐
児島　純司	民間病院を中心とした医療情報連携フォーラム事務局長
篠田　英範	保健医療福祉情報システム工業会標準化推進部会副部会長
土屋　文人	日本薬剤師会副会長
西田慎一郎	日本画像医療システム工業会医用画像システム部会 セキュリティ委員会委員長
野津　　勤	日本画像医療システム工業会医用画像システム部会 セキュリティ委員会副委員長
樋口　範雄	東京大学大学院法学政治学研究科教授
茗原　秀幸	保健医療福祉情報システム工業会セキュリティ委員会委員長
矢野　一博	日本医師会総合政策研究機構主任研究員
○山本　隆一	東京大学大学院情報学環准教授
吉村　　仁	日本画像医療システム工業会医用画像システム部会長

（五十音順：敬称略）

※　○は班長

資　料　2

（　案　）

医療情報システムを安全に管理するために

「医療情報システムの安全管理に関するガイドライン」

医療機関等の管理者向け読本

平成※年※月

厚生労働省

改定履歴

版数	日付	内容
第1版	平成21年　月	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版を医療機関等の管理者向けポイント集としてとりまとめた。

【目次】

1　本書の位置付けと活用方法

1.1　本書の位置付け

本書は、厚生労働省が策定した「医療情報システムの安全管理に関するガイドライン」（以下、「ガイドライン」という。）を医療機関等の管理者に理解してもらうために、そのポイントを要約したものである。

まず、ガイドラインは、次のような性格を持ち合わせるものとして編纂されている。

① 各種の法令等で求められるもしくは規定される要件を満たす実行指針としての側面
② 医療情報という「情報資産」を継続的に保護して行くためのプロセスに関する手引書

このことから、ガイドラインで情報技術を利用・活用する場合の留意点等を記載して行くに当たっては、遵守すべき法令等への言及、情報資産の保護のための方策等に対して詳細に渡って解説を加える必要があり、内容や頁数が多くなる傾向は避けられない。

従って、ガイドラインの概要を理解してもらことを期待して、以下の方々を対象として本書の作成をすることとなった。

本書が想定する主な対象読者

> 医療情報システムの導入を検討もしくは決定する立場にある管理者、ならびに既に同システムを導入し運用している管理者、医療機関等にあっては院長や理事長を主たる対象と想定している。
>
> これら管理者の方々が、本書を一読して実際にシステムを導入する情報技術管理者やベンダ等にガイドラインの趣旨に則った検討や指示を出す際の手引きとなることを期待している。

1.2　本書の活用方法

本書は読みやすさに配慮した上で、ポイントを絞ってガイドラインで求められる要件を以下のように整理し解説を加えている。

<u>第２章　電子的な医療情報を扱う際の責任の在り方</u>

医療機関等において電子的な医療情報を扱うに際して、医療機関等の管理者に求められる責任について解説をしている。これには、ガイドラインに違反していた場合に訴求される管理者の責任に対する考え方も含まれる。

<u>第３章　電子的な医療情報を扱う際の考え方</u>

電子的な医療情報を扱う際に必要な、継続的な情報資産の保護と法令等に対する解説を

している。

・ 医療情報システムの機能向上と運用の見直しに関する視点から
継続的に情報資産を保護するために必要な取組み等について解説している。

・ 個人情報保護の視点から
個人情報保護法で求められる安全管理措置について解説している。

・ e-文書法の視点から
主に e-文書法の厚生労働省省令及び外部保存通知で求められる「真正性」、「見読性」、「保存性」について解説している。

第4章 電子的な医療情報を交換もしくは提供する際の考え方

医療機関等で外部とネットワークを通じて個人情報を含む医療情報を交換する場合について解説している。

2 電子的な医療情報を扱う際の責任の在り方

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必要がある。これにより、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。しかし、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る可能性があるため、そのような事態が生じないよう適切な管理（このような善良なる管理者の注意義務のことを「善管注意義務」という）を行う必要がある。

ガイドラインは、この善管注意義務をできるだけ具体的に示したものであり、そこで述べられている管理者の情報保護責任を俯瞰すると下記のようになる。

情報保護責任

○ 自組織内で管理する場合		
	（通常運用時）	①管理方法・体制等に関する説明責任
		②管理を実施する責任
		③定期的に見直して改善する責任
	（事故発生時）	①事故の原因・対策等に関する説明責任
		②善後策を講じる責任
○ 第三者に委託する場合		受託する事業者の過失に対する責任
○ 第三者に提供する場合		第三者提供が適切に実施されたかに対する責任

2.1 医療機関等の管理者の情報保護責任

医療機関等の管理者の情報保護責任は次の２つのケースに分けて考える必要がある。

(1) 通常運用における責任
医療情報保護の体制を構築し、管理する局面での責任。「①説明責任」、「②管理責任」、「③定期的に見直し必要に応じて改善を行う責任」に分けられる。

(2) 事後責任
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

適切な対応を取る責任。「①説明責任」、「②善後策を講じる責任」に分けられる。

(1) 通常運用における責任

① 説明責任とは？

システムの機能や運用計画が、ガイドラインを満たしていることを必要に応じて患者等に説明する責任である。

ポイント

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し、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、その結果も文書化し、監査の結果問題があった場合は、真摯に対応し、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。また、医療機関等の規模に応じて、患者等に説明するため、患者窓口を設置することも必要となる。

② 管理責任とは？

情報システムの運用管理を、医療機関等が適切に行う責任である。

ポイント

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ため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、適切な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とは？

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。

ポイント

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。ただし、このような最新の技術動向を管理者が都度、把握して行くことは、管理者としての本来業務と異なることもある。従って、管理者は、運用管理の状況を監査・確認する際には、技術の進展を意識しつつ、例えば情報システムの技術担当者やシステムベンダに現在の動向を調査させるなどして、必要な改善を実践して行くことが重要な役割となる。

(2) 事後責任

① 説明責任とは？

医療情報について何らかの事故（典型的には漏えい）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、対処法を説明する責任である。

ポイント

個々の患者へ事故の内容ならびにその原因と対策についての説明責任はもちろんのこと、監督機関である行政機関や社会への説明・公表が求められる。

② 善後策を講ずる責任とは？

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である。

ポイント

何らかの不都合な事態が生じた場合には、医療機関等の管理者は善後策を講じなくてはならない。

その責任は、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でも、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、これら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。

2.2 責任分界点について

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、さらには伝送先の機関等にもまたがるようになる。その際、責任範囲の切り分けが必要で、ガイドラインでは責任分界点として説明されている。

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「(1) 委託（第三者委託）」と「(2) 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。

(1) 委託（第三者委託）の場合

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、管理者の支配下にある。

ポイント

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。一方、委託先と締結する委託契約書には、双方の責任を明記し、その責任の所在を明確にしておく必要がある。

(2) 第三者提供の場合

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、もはや提供元の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。

ポイント

提供元の医療機関等の管理者にとっては、原則として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。

ただし、電子化情報は、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、レセプトの代行請求や特定健診結果の代行送信のように、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。そのためには、それらの事実を可能な限り記録管理し、事故が起きた場合に記録の公開要求があれば、それに応じる必要もある。

3 電子的な医療情報を扱う際の考え方

本章では「情報資産」を保護して行くための継続的に取組む枠組みについてとガイドラインで言及されている各種法令等に対して、医療情報システムで必要な要件について解説する。

3.1 情報資産を保護して行くための手引き

情報システムを導入する時、または導入した後に継続的にシステムを活用し、システムに蓄積された情報を資産として保護して行くために必要な取組みについての考え方を解説する。

一般的に、情報システムやそこに蓄積された情報を保護して行く手段や手続き等については、国際的にも確立された構築方法やそれに伴う文書等がある。中心となる概念としては、「①計画を立てる」、「②それを実行する」、「③必要に応じて見直しを行う」、「④改善をする」である。これらの手順を継続して繰り返すことで情報保護のレベルを向上させて行くというものである。しかし、医療機関等の情報資産保護においてはこの概念が新しいものであるかと言えば、そうではない。

特に、医療安全に関してはこの概念が顕著であり、平成18年の「良質な医療を提供する体制の確立を図るための医療法等の一部を改正する法律」（法律第84号）の施行に伴い通知された「良質な医療を提供する体制の確立を図るための医療法の一部を改正する法律の一部の施行について」（平成19年3月30日付け医政発第0330010号厚生労働省医政局長通知）においては、医療の安全に関する事項として、この概念が以下の様に規定されている。

医療の安全を確保するための措置について（第0330010号通知より要約）

(1) 医療に係る安全管理のための指針の作成
- 「安全管理に関する基本的考え方」、「委員会その他医療機関内の組織」、「従業者研修の基本方針」、「事故報告等、安全確保のための基本方針」、「患者からの相談対応に関する基本方針」等を盛り込んだ指針の作成。

(2) 委員会の設置（※但し、無床診療所は適用除外となっている）
- 管理及び運営に関する規定の制定。
- 重要な検討内容の患者への対応状況を含めた管理者への報告。
- 重大問題発生時の原因分析・改善案の立案及び実施並びに従業者への周知。
- 改善策の実施状況の調査、見直し、等。

(3) 医療に係る安全管理のための職員研修の開催
- 医療安全の基本的な考え方や具体的方策について、病院等の従事者に周知徹底

を行うことで、安全に業務を遂行するための意識の向上を図るものとする。

(4) 医療に係る安全の確保を目的とした改善のための方策

- 安全管理委員会（無床診療所においては管理者）への報告。
- 事例の収集、分析。これにより問題点を把握し改善策の企画立案及びその実施状況の評価並びに医療機関内での情報の共有。
- 改善策については、再発防止策等を含んだものであること。

つまり、医療機関等においては医療安全管理の例の様に「①計画を立てる」、委員会や職員研修を実施しながら「②それを実行する」、改善のための方策を講じるために「③必要に応じて見直しを行う」、必要に応じて「④改善をする」というプロセスが既に存在している。従って、医療情報システムやそこに蓄積された情報の継続的な保護、利用・活用のプロセスも特殊な概念と捉えずに通常の業務の枠組みの一環として検討をした上で、確実に実行して行くことが重要であるといえる。

ただし、医療情報システムの場合、現在活用しているシステムが翌年にはセキュリティ上の問題を抱えたシステムになっていることもあり得る。従って、見直しや改善の際には、通常運用における責任でも述べたように、情報技術の進展にも留意する必要がある。その際には、ガイドラインを参考にすることが有益な手段となるので、積極的に活用してもらいたい。

新たに電子カルテなどの医療情報システムを導入する際には、出発点となる「①計画を立てる」ことが必須である。「①計画を立てる」際には医療機関等の管理者・責任者は、保護すべき情報をリストアップし、それを重要度に応じて分類し、業務や組織形態、人事体系等との整合性を図らなければならない。既に情報システムを導入している場合においても、「③必要に応じて見直しを行う」において適切な見直しを行い改善につなげていく必要がある。

医療情報を資産として捉えた場合、医療機関等の管理者・責任者は、資産管理に対して主体的に行う必要があり、これは情報技術を使う、使わない以前の問題として素直な感覚として捉えてもらえると思われる。

3.2 情報システムの安全管理に求められる基準

個人情報保護法では、第 20 条に安全管理措置の定めがある。安全管理措置とは、具体的には「組織的安全管理対策」「物理的安全対策」、「技術的安全対策」、「人的安全対策」で構成されている。本章では、これらについて解説をする。

組織的安全管理対策（体制、運用管理規程）

組織的安全管理対策とは？

安全管理について従業者の責任と権限を明確に定め、安全管理に対する規程や手順書を整備運用し、その実施状況を確認することをいう。

ポイント

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することが重要である。

また、これらのことを実践し、管理責任や説明責任を果たすために運用管理規程を定めることはきわめて重要である。

医療機関等の管理者は上記の事項を踏まえて、情報システムを運営して行かなくてはならない。

物理的安全対策

物理的安全対策とは？

物理的安全管理措置とは、入退館（室）の管理、個人データの盗難の防止等の措置をいう。

ポイント

情報の種別、重要性と利用形態、組織の規模に応じて幾つかのセキュリティ上保護すべき区画を定義し、情報端末、コンピュータ、情報媒体（CD-R や USB メモリ等）を物理的に適切に管理する必要がある。

留意するポイントとしては、入退館（室）の管理、機器等の盗難の防止、紛失防止等があり、それらを十分に考慮してもらいたい。

技術的安全対策

技術的安全対策とは？

個人データ及びそれを取り扱う情報システムへのアクセス制御、不正ソフトウェア対策、情報システムの監視等、個人データに対する技術的な安全管理措置をいう。

ポイント

情報システムへの脅威に対する主な技術的対策としては、下記の項目が挙げられる。

(1) 情報区分と利用者の対応付けを行い、アクセス権限を設定すること
(2) 運用時における利用者の識別と認証、アクセスの記録(アクセスログ)
(3) 不正なソフトウェアの混入やネットワークからの不正アクセス防止

これらの対策は、それぞれに対して有効範囲を適切に認識して実施すれば、強力な手段となり得る。ただし、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、一般的には運用管理による対策との併用は必須である。

人的安全対策

人的安全対策とは？

従業者に対する、業務上秘密と指定された個人データの非開示契約の締結や教育・訓練等を行うことをいう。

ポイント

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はかるため、人による誤りの防止を目的とした対策を施す必要がある。これには、守秘義務と違反時の罰則に関する規定や教育、訓練に関する事項を含む必要がある。

医療分野は様々な資格者と職種が混在しており、医療情報システムに関連する関係者は更に多岐に渡る。法令上の守秘義務を負う者、雇用契約の下で守秘義務を負う者、保守契約に基づいてシステムを保守する者等が例に挙げられる。従って、これらの関係者を適切に管理する規定の策定と教育、訓練を実施する必要がある。

また、求められていることは医療情報システムが対象にしている情報の生成から廃棄に至るまでの情報のライフサイクルに渡る安全管理であるので、廃棄についても上記措置に含めて考えることが必要である。

3.3 電子保存する場合に求められる基準

従来は紙媒体による管理が義務付けられていた診療録等が、平成11年4月の厚生省通知「診療録等の電子媒体による保存について」によって規制緩和され、いわゆる「電子保存」が認められた。この通知では、前述した情報システムの安全管理に加えて、診療に供する情報を扱うが故の医療固有の要求事項が示されている。これがいわゆる「電子保存の三原則」と呼ばれるものであり、「真正性」、「見読性」、「保存性」の3つの要件で構成されている。

ここでは、e-文書法の厚生労働省令である「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」及び「診療録の保存を行う場所（通知）」に則ってガイドライン第3版の7章から9章の中で詳細に記述され、実現を求められる「真正性」、「見読性」、「保存性」について解説する。

真正性の確保について

真正性とは？

正当な人が記録し確認された情報に関し第三者から見て作成の責任の所在が明確であり、かつ、故意または過失による、虚偽入力、書き換え、消去、及び混同が防止されていることである。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。

ポイント

発生する各種のデータに対して、「作成責任の所在と、内容の確定方法の明確化」が必要である。その上で、技術的対策、運用的対策等を組み合わせて責任の所在と完全性の確保（虚偽入力、書き換え、消去、及び混同の防止）を行う必要がある。

また、記名・押印が必要な文書については、電子署名、タイムスタンプを付すことが必要である。

一方、ネットワークを通じて外部に保存を行う場合、第三者が医療機関等になりすまして、不正な診療録等を診療録等の外部保存を受託する事業者へ転送することは、診療録等の改ざんとなる。また、ネットワークの転送途中で診療録等が改ざんされないように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、非対面での情報転送であることや通信経路上でのハッキングの危険性等、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。なお、これらのリスクについては、本書の4章で解説をしているので参照してもらいたい。

見読性の確保について

見読性とは？

電子媒体に保存された内容を、権限保有者からの要求に基づき必要に応じて肉眼で見読可能な状態にできることである。 ただし、見読性とは本来「診療に用いるのに支障が無いこと」と「監査等に差し支えないようにすること」であり、この両方を満たすことが、ガイドラインで求められる実質的な見読性の確保である。

ポイント

必要に応じてとは、「診療」、「患者への説明」、「監査」、「訴訟」等に際して、それぞれの目的に支障のない応答時間やスループットと操作方法でということである。

情報の所在管理と見読化手段の管理も必要である。患者毎の情報全ての所在が日常的に把握されていなければならない。外部保存していたとしても同様である。また、電子媒体に保存された情報は、そのままでは見読できず、その電子媒体から情報を取り出すには何らかのアプリケーションが必要であり、表示のための編集前提となるマスタ、利用者テーブル等が別に存在したりする可能性がある。これらの見読化手段が日常的に正常に動作することが求められる。

また、必要な情報を必要なタイミングで正当な情報利用者に提供できなかったり、記録時と異なる内容で表示されたりすることは、重大な支障となるので、それを防ぐためのバックアップや冗長性の確保などのシステム全般の保護対策が必要である。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無い最低限の見読性を確保するための対策が必要である。

更には、システムを更新する場合も同様であり、新旧のシステム間で記録内容が異なるようなことがないようにしなくてはならない。

保存性の確保について

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渡って真正性を保ち、見読可能にできる状態で保存されることをいう。

ポイント

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、下記のものが考えられる。

(1) データ保存自体が機器やソフトウエアの障害等によりなされていない可能性
(2) 記録媒体、設備の劣化による不完全な読取

(3) コンピュータウイルスや不正なソフトウェアを含む設備・記録媒体の不適切は管理による情報の喪失
(4) システム更新時の不完全なデータ移行

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。

外部保存を行っている場合には、保存施設においてこれらのことが対策されていることを確認することが必要である。

また、マスタ変更の際に、過去の記録が記録時と異なる内容で表示されたりすることが無い様にする事も保存性確保の範囲である。

4　電子的に医療情報を交換もしくは提供する際の考え方

ここでは、ネットワークを通じて組織の外部と情報交換を行う場合に、個人情報保護およ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。これには、双方向だけではなく、一方向の伝送も含まれる。

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、薬局、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（Application Service Provider）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様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場合等が考えられる。

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」、「内容を覗き見されない方法で」送付しなければならない。

本章では、これらについて医療機関等の視点から、「4.1　医療機関等における留意点」、「4.2　選択すべきネットワークセキュリティの考え方」について解説をする。

4.1　医療機関等における留意事項

ここでは、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、適切に送信先の医療機関等に受け渡しされるまでの一連の流れ全般において適用される。

医療機関等において情報を送信しようとする場合には、情報を適切に保護する責任を意識しつつ、次のような点に留意してもらいたい。

盗聴の危険性に対する対応

盗聴とは？

ネットワークに特異な事象ではなく、広く一般的に、意図的に第三者が会話や情報を盗み聞いたり、盗み取る行為。ネットワークでは、一般的には何らかの手段で伝送中の情報（電気信号）を盗み取る行為を指す。

ポイント

ネットワークを通じて情報を伝送する場合には、盗聴に最も留意しなくてはならない。

医療機関等においては、万が一、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。そのひとつの方法として医療情報の暗号化が考えられる。

どの程度の暗号化を施すか、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の高さ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、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必須である。

盗聴防止については、例えばIDとパスワードを用いたリモートログインによる保守を実施するような時も同様である。その場合、医療機関等は保守委託事業者等に対処方法を確認し、監督する責任を負う。

改ざんの危険性への対応

改ざんとは？

情報を不正に書き換える行為のこと。例えば、ホームページを不正に書き換えたり、伝送途中の情報を書き換えたりする行為を指す。

ポイント

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ることも重要な要素である。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、ネットワークの構成によっては、情報を暗号化せずに伝送する可能性も否定できず、その場合には改ざんに対する対処は必ず実施しておく必要がある。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。

なりすましの危険性への対応

なりすましとは？

本人ではない第三者が本人のふりをしてネットワーク上で活動すること。例えば、本来情報を受取る人のふりをして、不正に情報を取得する行為や他人のIDやパスワードを盗み出して、本人しか見ることができない情報を見たりする行為を指す。

ポイント

ネットワークを通じて情報を伝送する場合、ネットワークは非対面による情報伝達手段であることを十分に認識した上で、情報を送ろうとする医療機関等は、送信先の医療機関等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医療機関等は、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、送られて来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。

確認の手段は様々な方法があり、それらを適切に活用もしくは組み合わせて、なりすましに対する危険性へ対応する必要がある。

4.2　選択すべきネットワークのセキュリティの考え方

「4.1　医療機関等における留意事項」では、主に情報の内容に対しての脅威に対応する方法の考え方について解説したが、ここでは、情報を伝達する通信経路上に対しての脅威に対応する方法の考え方について解説する。

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、医療機関等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。

一言でネットワークといっても、その構成は様々なものがあるため、全てを網羅して行くことは難しい。そこで、ガイドラインでは大きく「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されている場合」とに分けて考えており、本書もその体系に合わせて解説をする。

Ⅰ．クローズドなネットワークで接続する場合

クローズドなネットワークとは？

インターネットに接続されていないネットワーク網で、「専用線」、「ISDN」、「閉域 IP 通信網」のことを指す。

ポイント

クローズドなネットワークは安全性は高いものの、例えば、異なる通信事業者の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。この場合、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言えないため、クローズドなネットワークを利用する場合であっても、「4.1　医療機関等における留意事項」を参考に、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、改ざんを検知可能な仕組みを導入するなどの措置を考慮する必要がある。

また、ウイルス対策ソフトのウイルス定義ファイルや 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。

Ⅱ．オープンなネットワークで接続されている場合

オープンなネットワークとは？

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、インターネットを活用して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行くことが考えられる。

ポイント

オープンなネットワークを利用する場合、その通信経路上では、「盗聴」、「侵入」、「改ざん」、「妨害」等の様々な脅威が存在する。従って、十分なセキュリティ対策を実施することは必須である。また、「4.1　医療機関等における留意事項」に従って、医療情報に対して暗号化の措置を講じなければならない。

ただし、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も意味する。

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やサービスが存在し、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。多くの場合、ネットワーク導入時に業者等に委託をするが、その際には、リスクの説明を求め、理解しておくことも必要である。

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

厚生労働省

削除: 20

削除: 3

改定履歴

版数	日付	内容
第1版	平成17年＿	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＿＿	平成18年＿＿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つけ、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1版	平成　年　月	

削除: および

削除: および

【目次】

1　はじめに

平成[illegible]の通知「診療録等の電子媒体による保存について」（平成[illegible]

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[illegible]通知「診療録等の保存を行う場所について」（平成[illegible]

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[illegible]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[illegible]法律[illegible]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[illegible]

平成[illegible]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[illegible]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[illegible]年[illegible]月[illegible]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[illegible]

[illegible]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[illegible]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[illegible]の「個人情報の保護に関する法律」（平成[illegible]法律[illegible]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１月２９日付
削除：１２年３月
削除：１３年３月２９日付
削除：１６年
削除：第１６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。

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。この上さな状況下においては、従来のように医療従事者のみ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こと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)～(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、免許資格ごと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与する以上、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と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章の関連する箇所に追記し、特にネットワークの在り方については「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】

削除: および

削除: なら

削除: 係わる

削除: および

削除: および

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ヒで、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があるため、付表の運用管理表を活用し、適切な具体的対策を採用

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: かもしれ

削除: ること

削除: されたい

削除: か

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、医療に関す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。

は対象となる文書等の一部限定されている

3.1　第７章及び第９章の対象となる文書について

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の１）の要件を充足のこと）

一　医師法(昭和二十三年法律第二百一号)第二十四条　診療録
二　歯科医師法(昭和二十三年法律第二百二号)第二十三条　診療録
三　保健師助産師看護師法(昭和二十三年法律第二百三号)第四十二条　助産録
四　医療法（昭和二十三年法律第二百五号）第五十一条の二第一項及び第二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(昭和三十年法律第百六十八号)第十九条　指示書
六　薬剤師法(昭和三十五年法律第百四十六号)第二十八条　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（昭和六十二年法律第二十九号）第十一条　診療録
八　救急救命士法(平成三年法律第三十六号)第四十六条　救急救命処置録
九　医療法施行規則（昭和二十三年厚生省令第五十号）第三十条の二十三第一項及び第二項の帳簿
十　保険医療機関及び保険医療養担当規則(昭和二十二年厚生省令第百五号)第九条の診療録等（平成十八年厚生労働省令第百十一号）附則第二十二条
十一　保険薬局及び保険薬剤師療養担当規則(昭和二十二年厚生省令第百六号)第九条　調剤録

削除：次ページの３．２の章

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…

削除：２３年…３年法律第２０１号）第２…

削除：２３年…３年法律第２０２号）第２…

削除：２３年…３年法律第２０３号）第１２…

削除：２３年…３年法律第２０５号）第５１…

削除：３０年…０年法律第１６８号）第１９…

削除：３５年…５年法律第１４６号）第２８…

削除：第十七条…17条及び歯科医師法第十…

削除：３年…年法律第３６号）第４６条の規…

削除：２３年…３年厚生省令第５０号）第３…

削除：３２年…２年厚生省令第１５号）第９…

削除：３２年…２年厚生省令第１６号）第６…

十二　臨床検査技師等に関する法律施行規則（昭和…厚生省令…書類

十三　医療法（昭和…法律…記録（同項…に規定する診療に関する諸記録のうち医療法施行規則…に規定する処方せんに限る。）、…の記録（同条…に規定する診療に関する諸記録のうち医療法施行規則…の…に規定する処方せんに限る。）、及び…の記録（同条…に規定する診療に関する諸記録のうち医療法施行規則…の…に処方せんに限る。）※

十四　薬剤師法(昭和…法律…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…厚生省令…処方せん※

十六　医療法(昭和…法律…の記録（医療法施行規則…に規定する処方せんを除く。）、…の記録（医療法施行規則…の…に規定する処方せんを除く。）、及び…の記録（医療法施行規則…の…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…歯科衛生士の業務記録

十八　診療放射線技師法（昭和…法律…の規定による照射録

削除：１３年…３年厚生省令第２４号）第…

削除：２３年…３年法律第２０５号）第…

削除：３５年…５年法律第１１６号）第…

削除：３２年…２年厚生省令第１６号）第…

削除：２３年…３年法律第２０５号）第…

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…

削除：<#>第８章の対象文書等．

1

3.2　第８章の対象となる文書等について

1　医師法(昭和…法律…に規定されている診療録
2　歯科医師法(昭和…法律…に規定されている診療録
3　保健師助産師看護師法(昭和…法律…に規定されている助産録
4　医療法（昭和…法律…及び…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…法律…、第…条及び第…条の…に規定されている診療に関する諸記録及び同法…及び…の…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：２３年…３年法律第２０１号）第２…

削除：２　…科医師法(昭和２３年…３年…

削除：３　…保健師助産師看護師法(昭和２…

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21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、上施行通知には含まれていないものの、この文書法の対象範囲であり、患者の個人情報が含まれている文書等（麻薬帳簿等）、法定保存年限を経過した文書等、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的検査の記録や画像、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。

これらまで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、各種指針及びこのガイドライン 6.9章の安全管理等を参照し、情報管理体制確保の観点から、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章の一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。[redacted]収集、保管、[redacted]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する法令、通知、指針等により定められている要件を満たす[redacted]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。[redacted]管理者に善良な管理者の注意義務（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的に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、[redacted]

- 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。

[redacted]、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[redacted]存在するという状況からネットワークを用いた交換・共有等が考えられる社会では、[redacted]管理責任と医療機関等を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関して、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、[redacted]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: か
削除: の管理
削除: その際、必要となる新たな概念と
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[redacted]する[redacted]善管注意義務を果たすために[redacted]、[redacted]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[redacted]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[redacted]」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、適切な情報管理ということになるが、適切な情報管理を[redacted]で、次に、[redacted]責任を負う必要がある。

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。[redacted]を果たすためには、[redacted]

・システムの仕様や運用計画を明確に文書化する。

・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[redacted]

・監査結果をあいまいさのない形で文書化[redacted]

・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[redacted]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。[redacted]医療機関等[redacted]

・少なくとも管理状況の報告を定期的に[redacted]

・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。[redacted]

[redacted]個人情報保護法上は[redacted]

・個人情報保護の責任者を定める。[redacted]

・[redacted]生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[redacted]

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[redacted]進歩[redacted]、情報保護体制、[redacted]

削除: 保護

削除: 、

削除: さまざまな局面で注意を払う要[redacted]

削除: いろいろな

削除: かういう意味での

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[redacted]

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[redacted]

削除: そこで、本ガイドライン[redacted]における医[redacted]

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[redacted]

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[redacted]

当該情報システムの運用管理の状況を定期的に監査[redacted]

問題点を洗い出し、改善すべき点があれば改善[redacted]

[redacted]保護[redacted]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[redacted]（典型的には漏えい）が生じた場合には、[redacted]責任がある。

[redacted]

特に医療機関等は一定の公共性を[redacted]監督機関である行政機関や社会への説明・公表[redacted]

[redacted]

① 善後策を講ずる責任

[redacted]医療機関等の管理者には善後策を講ずる責任[redacted]発生する。その責任は、[redacted]

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[redacted]種類が[redacted]医療機関等の管理者の[redacted]責任のあり方[redacted]前項[redacted]整理[redacted]

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[redacted]説明責任[redacted]管理責任[redacted]定期的に見直し必要に応じて改善を行う責任[redacted]を果たす義務を[redacted]

万一、何らかの[redacted]事態が生じた場合にも同様に[redacted]受託する事業者と連携しながら[redacted]説明責任[redacted]と[redacted]善後策を講ずる責任[redacted]を果たす必要が[redacted]

削除: 、

削除: 「[redacted]責任である」[redacted]、情報保護に関する技術の進歩[redacted]、関連機器の情報

削除: 仕様[redacted]、一時的[redacted]一つの理由性があり[redacted]。

[redacted]、医療機関等の管理者は、医療情報保護[redacted]

削除: <#>説明責任。[redacted]

削除: 説明は個々の患者に対して[redacted]ると同時に、[redacted]

削除: 有しているので[redacted]すなわち、個々[redacted]

削除: 医療情報について何らかの事故が生じた場合、一方、医療機関等の管理者には[redacted]

削除: 、[redacted]

削除: 、…「再発防止策を講ずる責任に加[redacted]

削除: 事故か、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。[redacted]

削除: 分界点について

削除: 2[redacted]種類があり、一般的に、委託[redacted]

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[redacted]

削除: ・・・・「管理責任・・・・「定期的に見[redacted]

削除: 事故…都合な事態が生じた場合に[redacted]

ある。

ただし、これとは別に、受託する事業者の責任による[illegible]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[illegible]

以上に医療機関等の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。

[illegible]受託する事業者、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[illegible]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[illegible]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。[illegible]事故[illegible]受託する事業者[illegible]責任[illegible]場合[illegible]適切な委託契約の[illegible]事業者の適切・監督[illegible]適切な上[illegible]上[illegible]医療機関等[illegible]管理者[illegible]責任[illegible]

[illegible]医療機関等[illegible]管理者[illegible]受託する事業者[illegible]管理者[illegible]責任[illegible]上[illegible]善後策[illegible]責任[illegible]医療機関等[illegible]管理者[illegible]責任[illegible]範囲[illegible]被害者[illegible]損害賠償[illegible]事故[illegible][illegible]場合[illegible][illegible]事故[illegible]事業者[illegible]医療情報[illegible][illegible]責任[illegible]事故[illegible]発覚[illegible][illegible]医療情報[illegible]保護[illegible][illegible]善後策を講ずる責任は医療機関等の管理者にあるべきことを意味する。

医療機関等の管理者は、患者等に対し、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、[illegible]善後策を講ずる責任を免れる。[illegible]

医療機関等の管理者[illegible]患者等[illegible]

[illegible]、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[illegible]、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。

[illegible]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、受託する事業者の適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) [illegible] 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ダンス」を遵守する必要がある。

[illegible] 提供 [illegible] 医等情報 [illegible]

[illegible] 医療機関等 [illegible] に [illegible] は [illegible]

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。

[illegible]

また、医療情報が電子化され、ネットワーク等を通じて [illegible] 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 [illegible] 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、[illegible] 情報処理関連事業者 [illegible] の責任 [illegible] 範囲 [illegible] 態 [illegible] 整理する。

[illegible] 場合、[illegible] 提供 [illegible] 医療情報 [illegible] 医療機関等 [illegible] 責任 [illegible] [illegible] ある。[illegible] 第三者提供の主体は [illegible] 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 [illegible] に到達するまでは、原則として [illegible] 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 [illegible] 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。適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 [illegible] ため、医療情報システムの安全管理や [illegible] 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: [illegible] 適切・適正に

削除: された

削除: についての提供元の

削除: 責任

削除: 負い

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: 1

(i) 情報処理関連事業者の提供するネットワーク [illegible] 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

[illegible]

提供元医療機関等と提供先 [illegible] 機関 [illegible] はネットワーク経路における責任分界点を定め、平常時や事故発生時の対処も含めて契約 [illegible] 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 [illegible] サービスに何らかの障害が起こった際の対処をどう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、[illegible] 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。

(ii) 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。[illegible]

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 [illegible] 機関 [illegible] 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 [illegible] 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 [illegible] 機関 [illegible] が1対N通信で、提供先 [illegible] 機関 [illegible] 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

(i) 医療情報が発信元／送信先で適切に暗号化 [illegible] 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 [illegible] 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 [illegible] 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

削除: なと

削除: おとり

削除: 但し、委託の場合

削除: について述べる。

削除: II

削除: 4.2で述べた

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。

その様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。

(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: III

削除: の

削除: および

削除: および

削除: および

削除: B.

削除: I

(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繋ぐことになる。

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。

(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、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、上記のような単なる業務委託ではないとき、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。

(2) 法令で定められている場合

法令で定められている場合とは、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。

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。

3.4 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（以下、）」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（以下、）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。

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表の様な「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の説明（　　）の際の参考資料に利用できる。

削除: なお

削除: D.

削除: なお

削除: 【参考】

削除: 中で

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と位置づけられている。これらの目的を達成するためには、総合的な医療情報システムを構成する個々のシステム相互に情報交換を行うことはもちろんのこと、情報システムから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となること、情報システムの相互運用性、いわゆる、医療情報標準に基づく相互運用性が必要となってくる。

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・運用に関する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として、必要時に「速やかに利用可能であること」、すなわち可用性、availabilityが求められる。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された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など、できるだけ容易に互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、「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を利用したシステム間でのデータのインポート・インポートのためのガイドラインを整備している。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）の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: 使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. 処方情報
7. 注射情報
8. 処置情報

必要な項目の整備状況については、これから検討していくこととなっているが、これらの情報が、システム間で交換され、その情報を利用することで、システム間の医療情報について、ある一定レベルの互換性を確保することが可能となる。

・医療機関情報	・傷病名（ICD10対応標準マスター）
・診療医療機関（診療科）情報	・オーダ種別情報
・患者基本情報	・処理（処方・注射）情報
・病名	・内視鏡画像情報
・感染情報	・検体
・患者（来院）履歴	・手術歴

また、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成果報告書、Webページなどで参照できる。

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

また、基本データセットによるデータの互換性を確保するためのガイドラインなども参照できる。

JAHIS 基本データセット適用ガイドライン
http://www.jahis.jp/standard/seitoj/st07-102/st07-102.htm

標準的な用語集やコードセットは、MEDIS-DCなどの団体により、整備、保守が行われている。

- 病名：ICD10対応標準病名マスター
- 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：標準医療機器マスター
- 看護用語：看護実践用語標準マスター

削除: ある。以下に
削除: 例

…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…

…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

…DICOM（Digital Imaging and Communications in Medicine）…国際的な標準…

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…こと…

…JAHIS…

削除: あげる

削除: の用語集

削除: 標準案の

削除: より、

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適用方法を定めたIHE（Integrating the Healthcare Enterprise）ほ、

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: か

削除: される

…

5.3 標準規格の適用に関わるその他の事項

…

…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、…に…独自に定義…表記文字であるか、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: ：

削除: JIS文字コード

削除: ような符号

削除: 移行可能な文字セット以外の文字を

削除: してもらいた

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」では、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は、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。

削除: でも
削除: められているが、
削除: 上記の

a) 事業の内容及び規模を考慮した適切な個人情報の収集、利用及び提供に関すること
b) 個人情報の安全管理（漏えい、滅失又は毀損の防止及び是正）に関すること
c) 法令、国が定める指針その他の規範を遵守すること
d) 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
e) 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）では、下記のように定めている。

ISMS 基本方針 トップマネジメントは、次の事項を確実にするための基本方針を確立する。
a) ISMS を確立するための目的を含むか、又はこれらの設定のための枠組みを与える。
b) 事業及び法令又は規制の要求事項、並びに情報セキュリティの契約上の義務を考慮する。
c) 現在及び将来の組織の情報セキュリティ環境との戦略的な整合を含む。
d) リスクを評価するための基準を確立する。
e) 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として、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、公開すること。
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することにより、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

B 考え方

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。
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、看護など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。

反面、情報セキュリティではIT技術の日覚しい発展により、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などを確立すれば、あとは自然にISMSが構築されていく土壌があると言える。

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。

削除: など
削除: など
削除: など
削除: など

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、説明責任も情報に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、点検等を含めたアクセス管理規程を作成すること。
1. 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. 推奨されるガイドライン

1. 情報システムで利用する機器の管理

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、情報システムで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 情報システム・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、点検等を含めたアクセス管理規程を作成すること。
1. 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: 運用管理規程には次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) [illegible]

(e) 障害を想定した冗長化機器の管理

(f) 個人情報の記録媒体の管理（保管・授受等）の方法

(g) 患者等への説明や同意を得る方法

(h) 監査

(i) 苦情・質問の受付窓口

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策の措置

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。

削除: および

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、[illegible]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。[illegible]
   - 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.

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、技術的対策は強力な脅威対抗手段となりうる。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

なお、情報又は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 情報又は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とパスワードや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、また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[illegible]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[illegible]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。
- 容易に推測できる、あるいは、文字数の少ないパスワードの設定されており、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、また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・パスワードの組合せは、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づける等、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な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[illegible]手段としては、ICカード等のセキュリティ・デバイスとパスワードのように利用者しか持ち得ない2つの独立した要素を用いて行う方式（2要素認証）やバイオメトリクス[illegible]等、より認証強度が高い方式を採用することが望ましい。

また、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。

＜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[illegible]

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な対策を講じる必要がある。また、万一その[illegible]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[illegible]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[illegible]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えない情報との組合せによってのみ有効になるようなメカニズム、運用方法を採用すること。

削除: これら
削除: および
削除: および
削除: 置いて
削除: 用いられる
削除: 以下のような行為により、
削除: 防止策が取られなければ
削除: ＩＤ
削除: 、
削除: 、
削除: 用いられる
削除: なって

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、緊急時の代替え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、本人確認を十分におこなった上で代替手段の使用を許し、さらにログ等を残し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）には十分とは言えず、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合せて利用するべきである。

また、生体情報を基に認証するために以下のような、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)

上記の事を考慮のうえ、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、二要素認証（IC カードやパスワードなどと生体認証の組み合わせ等）を用いること。

(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

削除: （生体計測情報）

削除: より

削除: "なりすまし"や

削除: 等

削除: 、

削除: 用いたり、

削除: 等のセキュリティ・デバイスと

削除: 行う方法や、従来のパスワードを付加する方法も有効である

削除: 規程

削除: が

削除: される

削除: は

削除: される

行う必要があり、組織の規程で定められていなければならない。

(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ため、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、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は、記録する時刻は重要である。精度の高いものを使用し、医療機関の全てのシステムで同期をとらなければならない。

(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とられていなければ、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を引き起こされる。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づくことになる。

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することが必須である。

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。このためには、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手段としてファイアウォ

削除: 組織内

削除: とらなけれ

削除: コード

削除: コード

削除: コード

削除: コード

削除: コード

削除: および

削除: コード

ールの導入がある。

[redacted]

(6) 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への利用には注意が必要である。

最近では、電力線搬送通信（PLC：Power Line Communication）が利用可能になった。しかし、医療機関等において PLC 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」[redacted]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。

削除: また、
削除: 利用して
削除: の保護
削除: 対する
削除: また、基本ソフトやWebに対するセキュリティ商品として、ファイアウォールとアクセス対策ソフトをセットにした製品で提供している商品もある。
削除: の使用環境に合わせて、これらのシステムとの組み合わせを行う必要がある。
削除: 行なったり
削除: 行なう
削除: にて
削除: 行なう
削除: 問題
削除: 問題
削除: 絶えず注意して避ける
削除: 傍受
削除: など
削除: その際、暗号化技術として、容易に解読されない手法を選択する必要がある。
削除: 昨今は無線 LAN を用いてコンピュータをネットワークに接続する構成にて
削除: など
削除: など
削除: など
削除: それとは別に、
削除: など、
削除: また、

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。

[redacted]

1. 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。
5. 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、そのレベルに応じたアクセス管理を行うこと。[redacted]

   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[redacted]、次項の操作記録を[redacted]ことで担保する必要がある。
6. 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[redacted]とも利用者のログイン時刻[redacted]時間、[redacted]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）を必ず行うこと。

   [redacted]
8. 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。
9. システム構築時、適切に管理されていないメディア使用[redacted]、外部からの情報[redacted]にはウイルス等の不正なソフトウェア、混入[redacted]か確認すること。[redacted]

   [redacted]
10. 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([redacted]不可逆変換[redacted])され、適切な手法で管理及び運用が行われること。(利用者識

削除: 現状
削除: などで
削除: 行なう
削除: すべて
削除: および
削除: や
削除: を
削除: もた
削除: で受け取る際
削除: の
削除: かない
削除: 7.

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、盗用されたりする恐れがある場合で、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、本人以外が知りえ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)、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。

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とること。

(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「安心して無線LANを利用するために」を参考にすること。

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有す)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とバイオメトリックスあるいはICカード等のセキュリティ・デバイスとパスワードまたはバイオメトリックスのように利用者しか持ち得ない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。
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行うこと。

削除: IC
削除: される
削除: (
削除:)
削除: 、不注意による
削除: の盗用は、盗用された本人の責任になる
削除: を認識すること
削除: 8
削除: など
削除: 、WPA/TKIP、
削除: <#>アクセスの記録として、誰が、何時、誰の情報にアクセスしたかを記録し、定期的な記録の確認を行うこと。。<#>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(たとえばパターンファイルの更新の確認・維持)を行なうこと。。
削除: が望ましい
削除: が望まれる

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確定する必要がある。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、次の各種類を想定する。

(a) 医師、看護師等の業務で診療に[redacted]情報を取扱い、法令上の守秘義務のある者
(b) 医事課職員、事務委託者等の病院事務の業務に携わり、雇用契約の下に医療情報を取扱い、守秘義務を負う者
(c) システムの保守要員等の雇用契約を結ばずに[redacted]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、万が一、第三者によりシステム内の情報が漏えい等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か、これに関しては詳細を8章に記述する。

(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[redacted]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あたっては、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[redacted]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。

削除: 係わる

削除: 診療を維持するため

削除: 患者、

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. 病院事務、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づ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・作業結果の確認をおこなうこと。
   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、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、やむをえ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づけられた守秘契約等の秘密保持の対策を行うこと。

削除: [redacted]の異常等で、保存データを救済する必要があるとき等、やむをえない事情で

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。破棄に確実、行に要するなど、また、関連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るため、破棄もしくは廃棄など。

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

削除: 運用、保存する場合だけでなく

削除: また

削除: ある

削除: 廃棄

削除: 廃棄プログラム等

削除: したものを作成

削除: 外部保存を委託している診療録等について、その委託の終了により診療録等を破棄する場合には、速やかに破棄を行い、処理が厳正に執り行われたかを監査する義務（または 監督する責任）を果たさなくてはならない。また、受託する機関等も、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、処理を行った旨を明確に示す必要がある。

削除: 行なわれた

削除: 廃棄

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作業時の病院関係者の監督、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あたっては、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、およ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変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

削除: また、安全な情報システムの構築を推進するため、システム全体の構成管理を適切に行い、定期的にシステム評価を実施し、最新のセキュリティ技術や標準を適切に取り入れ、客観的に評価された暗号、製品等を導入することも重要である。

なお、

削除: および

えておくこと。

5. 保守会社から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と同等の義務を課すこと。

削除: 許可制とする

削除: 行われる

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. 保守作業時には病院関係者立会いのもとで行うこと。
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. 保守作業にかか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て表示し、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

削除: および

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、情報機器の持ち出しに伴う個人情報を含む情報の漏えいする事案が発生している。

削除: とその

削除: る

情報の持ち出しについては、ノートパソコンのような情報端末やモバイルデバイス、USBメモリのような情報記録可能媒体が考えられる。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）や情報機器も考えられる。

削除: 適切な、医療機関等における可搬媒体、モバイルデバイスおよびその持ち出しに関する情報、すなわち、情報機器の持ち出しについて考え方と留意点は以下のとおりである。

まず重要なことは、「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」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も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もしくは情報機器に対して対策を立てなければならない。

適切に情報が把握され、リスク分析がなされていれば、それ心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こと、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、情報機器の取り扱いについての把握や規制は難しくなるが、情報の取り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。

削除: 取り扱ったり、医療機関等の情報システムにアクセスしたことで

このようなことから、情報も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、組織として情報も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。

たたし、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、情報も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、人的安全対策を更に施す必要がある。

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も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もしくは情報機器の所在を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を設定すること。設定にあ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。
9. 持ち出した情報を、例えばファイル交換ソフト（Winny 等）がインストールされた情報機器で取り扱わないこと。医療機関等が管理する情報機器の場合は、このようなソフトウェアをインストールしないこと。
10. 個人保有の情報機器（パソコン等）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。

削除: および

削除: および

削除: など

削除: 取り扱ったり、医療機関等のシステムへアクセスするような

6.10 災害等の非常時の対応

B. 考え方

医療機関等は医療情報システムに不具合が発生した場合でも患者安全に配慮した医療サービスの提供が最優先されなければならない。

ここでは、「6.2.3 リスク分析」の「②医療情報システム自身」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出来ない事態に陥った場合における留意事項について述べる。

「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また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(BCP : Business Continuity Plan)

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。

医療施設として定められる BCP においては、医療情報システムについての計画を含め、全体としての整合性が必要である。

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

事前に対応策を知ってもらい、信頼してもらっておくべきである。

- 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

災害や事故の発生（或いは発生の可能性）を検知してから、BCP 実行か通常の障

削除: な

削除: など

削除: など

削除: および

削除: および

害対策の判断を行い、BCP 発動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、システムの切替・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を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ていること。
具体的項目は、「基本方針の確定」、「発生事象の確認」、「安全確保・安否確認」と、「影響度の確認」である。

② 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・手作業への代替手段により業務を再開し、軌道に乗せるまでフェーズで、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・設備の確保」、「再開／復旧活動の両立」と、「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。

③ 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」と、「制限の確認」である。

④ 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」と、「総括」である。

⑤ 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。

削除: および
削除: なら
削除: および
削除: および
削除: および
削除: および

(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上の用意
- 停電、火災、漏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。医療情報システムでは使用可能であること、使用者側の事情で通常時とは著しく違い、正規のアクセス権者による操作が望ましく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、主に用意し、患者データへのアクセス制限や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は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用ユーザアカウントへ変更をすることを基本としている。

② 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、必要に応じて非常時の運用に対応した機能を実装すること。

削除: なし

上記の様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。

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、もし使用された場合には使用されたことが多くの人にわかるようにする等、適切に管理、監査をすること。
   - 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。
4. サイバー攻撃で広範な地域での一部医療行為の停止、医療サービス提供体制に支障が発生する場合は、所管官庁への連絡を行うこと。

削除: および
削除: など
削除: 別途定める

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

B. 考え方

ここでは、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、薬局、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様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」、「内容を覗き見されない方法で」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幾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

ここでは第4章の「電子的な医療情報を扱う際の責任のあり方　4.2 委託と提供における責任分界点について」で述べた責任の内、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しされるまでの一連の流れ全般において適用される。

ただし、誤解のないように整理しておくべきことは、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）のことを指す。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

削除: および

削除: （Application Service Provider）

削除: 場合

削除: および

削除: ネットワークに対する

削除: および

削除: など

削除: 医療

削除: 等

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のことを指す。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ひとつである。このような情報の内容に対するセキュリティのことをオブジェクト・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のことをチャンネル・セキュリティと呼ぶことがある。

このような視点から見れば、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、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、明らかな犯罪行為であり、必ずしも医療機関等の責任といえない事例も想定される。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、万が一、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。そのひと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。

どの様な暗号化を施すか、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度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ような時も同様である。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

削除: チャンネル

削除: て、不適切な

削除: 通りであり、

削除: のことを指している。すなわち

削除: 考え方が必要となる

削除: 程度の

削除: 機密性の高さ

削除: ID とパスワードを用いた

削除: ②

削除: 伝えることも重要な要素である

リティの考え方」のネットワークの構成によっては、[illegible]に[illegible]場合、[illegible]改ざんに対する対処は確実に実施しておく必要がある。[illegible]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

ネットワークを通して情報を伝達する場合、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、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[illegible]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[illegible]・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[illegible]や、業務の必要性[illegible]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、第4章「電子的な医療情報を扱う際の責任のあり方 1.2 責任分界点について」でも触れた通り、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は留意をし、確認をする責務がある。

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、医療機関等としては交換しようとする情報の機密度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、[illegible]機密度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分界点がネットワークを提供する事業者となるか、医療機関等となるか、また、どこまで負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内、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[illegible]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のない者が安易にネットワークを構築し、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、例えば情報の送信元と送信先に設置される機器や医療機関内に設置されている情報端末、端末に導入されている機能、端末の利用者等を確実に確認する手段を確立したり、情報をやり取りする機関同士での情報の取り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[illegible]ネットワーク経路上のセキュリティを[illegible]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を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して交換しようとする場

削除: 情報を暗号化せず
削除: 信頼する可能性も高まります。そ
削除: ため
削除: 医療
削除: 等
削除: 医療
削除: 等
削除: 医療
削除: 等
削除: の医療機関等
削除: ネットワーク
削除: 同じ医療機関等の
削除: や
削除: 「B-1. 医療機関等における留意事項」では情報そのものに対する暗号化について触れているが、同様の観点から、情報の機密度に応じてネットワーク種別も選択しなくてはならない。
削除: された
削除: 発信
削除: や
削除: 担保

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，以降では幾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，これらについては特に「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．

削除: ，および

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．

削除: ウイルス

削除: セキュリティパッチ

以下，それぞれの接続方式について特長を述べる．

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（「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，その導入にあたってはやり取りされる情報の重要性と情報の量等の兼ね合いを見極める必要もある．

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など、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）に接続する接続方法ではなく、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、誤送信のリスクや専用線と同様で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もしくは画像等の容量の大きな情報を送信する場合には適用範囲を適切に見定める必要がある．

削除: など

削除: 接続先

削除: を

削除: する際に

図 B-2-② 公衆網で接続されている場合

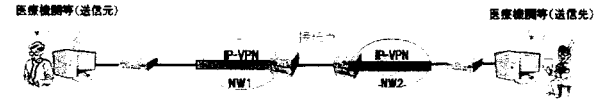
③閉域 IP 通信網で接続されている場合

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言う．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、遠隔地を含めた企業内LANのように利用され、責任主体間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も可能である。

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[illegible]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言えない。電気通信事業法があり、万が一偶発的に漏示してもそれ以上の拡散は考えられないか、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。そのほか、医療機関等から閉域IP通信網に接続する点も、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、改ざんを検知可能な仕組みを導入するなどの措置を取る必要がある。

削除: など

削除: など

Ⅱ．オープンなネットワークで接続されている場合

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など、その利用範囲を拡大して行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要である。また、医療情報システムの安全化の対策を取らなければならないことはもちろん、オブジェクト・セキュリティの考え方に基づいた対策を施す必要がある。

さらに、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切断に関係する層
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、機械の形状・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」と言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。一方、IPSecを用いる

場合は、2階層目もしくは3階層目の「ネットワーク層」と言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。

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。多くの場合、ネットワーク導入時に業者等に委託をするが、その際には、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や可搬型コンピュータ等の、いわゆるモバイル端末を用いて、医療機関の外部から医療機関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、さまざま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。

削除：「6.9　情報および情報機器の持ち出しについて」で述べた

削除：（テレワーク）

削除：など

削除：、および

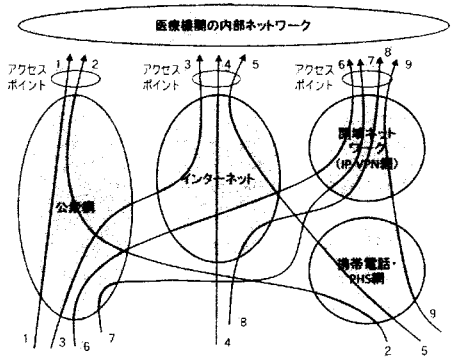


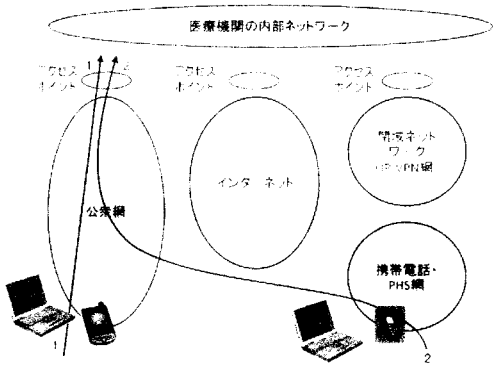
図 B-2-⑤　モバイル環境における接続形態

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。

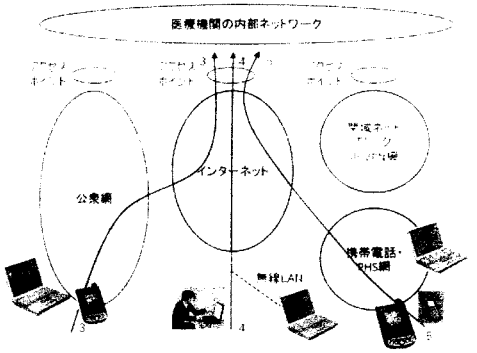
②は①における電話回線の代わりに、携帯電話・PHSやその搬送波を利用する通信用カード等をモバイル端末に装着して携帯電話・PHS網に接続ケースである。①と②は携帯電話・PHS網を経由するかどうかの違いがある。

いずれも「1．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、セキュリティ的な要件は、そこでの記述を適用すること。すべ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。

削除: など

削除: など

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、セキュリティ的な要件は、そこでの記述を適用すること。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。

具体的には、モバイル端末として携帯電話・PHS機や、より高機能な端末装置（いわゆるスマートフォン等）を利用する場合には、その端末でSSL/TLSが利用できるのか、接続経路にIPSecとIKEが適用されているのか、等のサービス内容を確認する必要がある。

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。

削除: など

削除: な

削除: 「8章　情報および情報機器の持ち出しについて」の記述からもわかるように

医療機関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

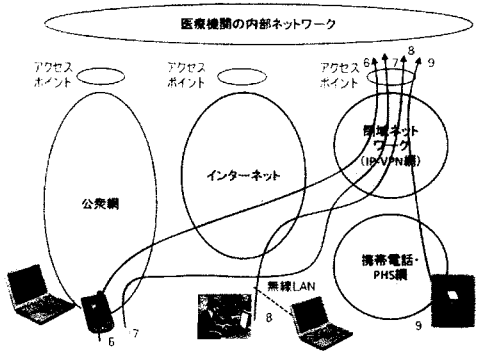


図 B-2-⑧　モバイル環境における接続形態（閉域ネットワーク経由）

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のアクセスポイント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「1．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、セキュリティ的な要件は、そこでの記述を適用すること。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。

削除: など

削除: など

削除: など

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うる。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視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　情報と、情報機器の持ち出しについて」に詳細を記述したので、参照すること。

削除: など

削除: などである

削除: および

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、PCを含めて自宅等から、病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する安全管理の要件は、すでに述べてきたが、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など、非管理端末であること、一定の安全管理が可能な技術的対策を講じられたものでないこと、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、考慮すべきことがいくつかある。

1．PC等、自己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こと。

2．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なこと。

3．医療機関等の管理が及ばない私物のPCなど、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て、不具合があること。

従って、通常は行うべきではないが、医療従事者の過剰な労働や医師の過疎等に対応するためには、それを許す場合、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の普及しており、これらの導入を検討することが重要であると共に、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

診療情報等の開示の進む中、ネットワークを介して患者（または家族等）に診療情報等を提供するケースや医療機関内の診療情報等を閲覧でき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、診療情報のやりとりを想定しているが、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、その際の考え方について触れる。

基本的な考え方の原則は、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を外部保存を受託する事業者から直接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だけで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が行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り、説明が不足している中で万が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。

また、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、一般的にはインターネット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、既に第4章やB-1で述べられているが、インターネットに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 SSL 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 に関す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、ウイルス混入などの改ざんを防止する対策をとること。
   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とること。
   セッション乗っ取り、IP アドレス詐称などのなりすましを防止する対策をとること。
   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あげられる。
   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、機器の出入口・使用機器・使用機器上の機能単位・利用者などの必要な単位で、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とること。これに関しては、医療情報の安全管理に関するガイドライン 4.5 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. ルータなど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も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などのセキュリティ対策を実施すること。たとえば、SSL/TLS の利用、S/MIME の利用、ファイルに対する暗号化など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など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必要な動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また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また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。

削除: および

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 章　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。

削除: および

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 SSL 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の納得できる説明を実施し、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。

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

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」　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、法令で署名または記名・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、「民間事業者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に基づく厚生労働省令」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・押印にか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、署名を信頼性を持って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[illegible] RSA 1024bit [illegible] SHA1 [illegible] 2008 [illegible] 政府機関 [illegible] SHA1及びRSA1024に関する移行指針 [illegible] 2014年度 [illegible] RSA 2048bit 及びSHA2 [illegible] 移行される予定になっている。

[illegible] 電子署名を [illegible] 電子証明書の有効期間 [illegible]

削除: 平成１２年法律第１０２号

削除: 過ぎた場合は検証ができないという特徴がある。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

[illegible]

C. 最低限のガイドライン

法令で署名または記名・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 認証局も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 認証局については、電子証明書内に医師等の保健医療福祉に係る資格が格納された認証基盤として構築されたものである。保健医療福祉分野において国家資格を証明しなくてはならない文書等への署名は、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のが望ましい。
ただし、当該電子署名を検証しなければならない者すべてが、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、[illegible]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. 「電子署名に係る地方公共団体の認証業務に関する法律」（平成[illegible]法律[illegible]）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

削除: [illegible]同様

削除: １４年

削除: 第１５３号

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すべ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、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事.
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に、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共に署名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

[illegible]

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。

（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、第４条第４項第二号、平成17年3月25日）

B. 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。

（1） 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。

（2） 作成の責任の所在を明確にすること

（施行通知 第２ 第３ ２(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)）

削除: 保存義務のある情報の真正性が確保されていること。

削除: （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 第４条第４項第二号）。

削除: 第２

削除: １

B. 考え方

真正性とは、正当な[redacted]されたことに対し、虚偽入力、書き換え、消去、及び混同が防止されて[redacted]ことである。なお、混同とは、患者を取り違えた記録がされたり、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。

[redacted]、ネットワークを通じて外部に保存を行う場合、[redacted]の外部保存[redacted]の転送途中で、診療録等が[redacted]されないように[redacted]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、書き換え、消去及び混同を防止すること

保存義務のある[redacted]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、正当な手続きを経ずに、[redacted]電子的な[redacted]が誤入力、書き換え・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、作成責任者（情報を作成、書き換え、消去しようとする者）は、情報の保存を行う前に情報が正しく入力されており、過失による書き換え・消去及び混同がないことを確認する義務がある。

故意または過失による虚偽入力、書き換え、消去及び混同に関しては、入力者[redacted]の操作者の故意[redacted]過失、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、書き換え、消去及び混同の防止は、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) 故意または過失による虚偽入力、書き換え、消去及び混同の防止

故意による虚偽入力、書き換え、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. 情報の作成責任者が明確で、いつでも確認できること。
2. 作成責任者の識別・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。

削除: 上の記録と確認

削除: 情報に関し責任者の果たすべき作成責任者の所在が明確であり、かつ、故意又は過失

削除: また

削除: いる

削除: 制度上の要求事項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い事が想定され、両者のバランスを取れた総合的な対策が重要と考えられる。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。

一方、

削除: 第三者が診療録等

削除: を受託する事業者になりすまして、不正な診療録等を医療機関等

削除: 転送することは、診療録等の改ざんとなる。また、ネットワーク

削除: 改ざん

削除: 故意または過失による

削除: 情報

削除: その内容

削除: 改ざん、消去されたり、過失による

削除: その

削除: に

削除: 何らかの理由により

3. [redacted]を[redacted]すること
4. [redacted]作業[redacted]こと
5. 作成責任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、どのような操作を行ったのかが記録され、必要に応じて、操作記録に対して適正な利用であることが監査されること
6. 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
7. 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、書き換え、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[redacted]と、[redacted]

[redacted]

(2) 使用する機器、ソフトウェアに起因する虚偽入力、書き換え、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、書き換え、消去及び混同とは、作成責任者が正当に入力したにもかかわらず、利用しているシステム自体に起因する問題により、結果が作成責任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、[redacted]、バージョン下整合等）
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

[redacted]

これらの脅威は[redacted]を[redacted]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、医療機関等自らが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及びDの記述を参照すること。

削除: 作成責任者が行う作業について手順書

削除: 作成

削除: 手順書

削除: 果たす作業の実施する

削除: 、

削除: 点検・規則等で定められた保存期間に基づいて

削除: 従って、

削除: 言える

削除: そのため、入力ミス等はどう発生するとの認識のもと、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、あるいは、ヒヤリ・ハット事例をもとに誤入力の発生しやすい個所を色分け表示する等のシステム的対策を施すことが望ましい。

削除: ソフトウェア

削除: （

削除: ）

削除: 保存された情報

削除: 保護する

削除: 維持

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、記録を作成した（した）責任者が明確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・消去することもごく日常的に行われるものと考えられるが、追記・訂正・消去をした責任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・訂正等の責任者が自明となる場合も考えられるが、その場合、作成責任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適切な記録を残した運用を実施すること。

入力は診療行為の実施者である作成責任者自らが行うことが原則であるが、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、本来の作成責任者である執刀医による入力が物理的に不可能であって、代行者による入力が必要となる場合も想定される。

このような場合は、代行入力に関する規定の確定と、その実施に関して記録が残されなければならない。

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) 作成責任者の識別と認証
(2) 記録の確定
(3) 識別情報の記録
(4) 更新履歴の保存

(1) 作成責任者の識別及び認証

本指針６章の「6.5　技術的安全対策　(1) 利用者の識別及び認証」を参照すること。

<代行入力を行う場合の留意点>

医療機関等の運用上、代行入力を容認する場合には、必ず入力を実施する個人毎に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事は、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

記録の確定とは、作成責任者による入力の完了や、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。これは、この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・誰によって作成されたかを明確にし、その保存情報自体にはいかなる追記、変更及び消去も存在しないことを保証しなければならない。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づ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。

削除: その
削除: の元となった行為等に
削除: 記述
削除: 書き換え
削除: その際に修正記述を行った者（元記録の作成者と同一である場合も含む）も元記録の作成者とは別個の作成責任者として明確に区別されて
削除: 作成責任者と情報の例を以下に示す。
<#>医師が患者の診察時にカルテに所見を記述する。
情報…：所見。
作成責任者。：実際に診察を行った医師。
<#>看護師が医師の指示に基づく処置を行った際に実施状況を看護記録に記述する。
情報…：処置実施記録。
削除: を行った。
情報…：投薬指示。
削除: 記述
削除: 記述
削除: 医療機関等が
削除: ケースを組織のポリシとして容認するのであれば、実施にあたって
削除: 任意の医療
削除: 業務等について誰が誰を代行可能かのルールと、誰が誰を代行したかの関係が
削除: 。
<#>夜間等で当直看護師が主担当医の承認
削除: 行う必要のある

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）により作成される記録では、作成責任者は過失による誤入力や混同の無いことを確認し、それ以降の情報の追記、書き換え及び消去等との区別を明確にするために「確定操作」が行われること。また、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も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、作成責任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こと。

なお、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、取込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、その作業の責任者による確定操作が行われることが必要である。

また、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、管理責任者の元で適正に管理された特定の装置も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を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) 更新履歴の保存

例えば、診療情報を例に取ると、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、確定済で保存してある記録に対して追記や修正を行うことは少なくない。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、更新内容の確定責任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) 作成者の識別及び認証

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. 利用者を正しく識別し、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、権限のある利用者以外による作成、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。

削除: 事
削除: 何時
削除: ここでは電子保存システムにおける「記録の確定」のユースケースとして次の３つを考え、それぞれの要件を定義する。
<#>操作者が情報を、入力画面を見ながら入力して記録する場合。
<#>外部機器等から確定されていない情報を取り込み記録する場合。
<#>外部システムで確定された情報を取り込み記録する場合。
<#>操作者が情報を入力画面を見ながら入力して記録する場合。
入力者の違いによる確定操作の基本的な考え方を以下に示す。
削除: に
削除: 識別
削除: は、
削除: これらを可能とする環境としては例えば次の方法が考えられる。
削除: 。
<#>電子保存システムへの厳格なアクセス
削除: 対策は運用面と技術面の両方で行うことが、より効果的かつ安全であると考え
削除: 、
削除: にID、パスワード等の本人認証、識別に用いる識別情報を発行し、本人しか持
削除: <#>本人認証、識別にICカード等のセキュリティ・デバイスを利用する場合は
削除: <#>情報システムに医療機関等の外部からリモート接続する場合は、暗号化

b. 臨床検査システム、医用画像ファイリングシステム等、特定の装置も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、予め管理規程で定められ、管理責任者、操作者以外の機器の操作が制限、防止されていること
2. 当該装置による記録は、いつ・誰が行ったのかシステム機能と運用の組合せ等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、作成責任者の識別情報の記録

a. 電子カルテシステム等、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、システム上確定された情報として登録できる仕組みを備えること。その際、作成責任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を含まれること
2. 「記録の確定」を行うにあたり、作成責任者による内容の十分な確認が実施できるようにすること
3. 確定された記録が、故意による虚偽入力、書き換え、消去及び混同されること、防止の手の講じられること。（例えば…）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、特定の装置も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、作成責任者の氏名等の識別情報（または装置の識別情報）、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、書き換え、消去及び混同されること、防止対策を講じ…原状回復…手順を施行…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) 代行操作の承認機能

1. 代行操作を運用上認めるケースがあれば、具体的にどう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. 代行操作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、その代行操作の都度記録されること

削除: 運営

削除: 明文化

削除: の

削除: 運営上

削除: また、

削除: 確認

削除: 、

削除: か

削除: 不適用も含めて防止できず、それらが検知された場合は…ックアップ等を用いて原状回復できるようになっている

削除: <#>操作者がスキャナやデジタルカメラ等の外部機器を利用し、電子化した情報を電子保存システムに保存する場合、外部機器から伝送される記録情報等をそのまま電子保存システムに保存するのではなく、受診した情報の内容確認と患者属性の付与（必要に応じて）、確認を行った後、電子保存システムに保存すること。

削除: 時間源

削除: 不適用も含めて

削除: でき、それらが検知された場合は…

削除: できるようになっている

削除: <#>更新履歴の参照（照らし合せ）は…

削除: <#>アクセスログの記録を残す…その…

削除: 医等に関する

削除: プロトコル

削除: 定義する

削除: を認める医療に関する業務等がある…

3. 代行操作により記録された診療録等は、できるだけ速やかに作成責任者による「確定操作（承認）」を行うこと
1. 一定時間後に記録が自動確定するような運用の場合は、作成責任者を特定せず明確なルールを策定し運用管理規程に明記すること

(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…されていること
3. 決め…管理…内容を…に…、従業者等への教育を実施すること
4. …実施…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おこなうこと

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、お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・回復なら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

保守目的等のどうしても必要な場合を…ように…適切に管理されたリモートログインの際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」を参照すること。

削除: この…、代行者が…により記録を…情報共有…管理情報は…要な…明らかにする…ように…一定の時間内に…確定操作の行われるような…機能の組織…として…整備…こと。

削除: .

<#>1つの診療録等を複数の医療従事者が共同して作成する場合の管理.

<#>診療録等を共同して作成する…運用上…は、具体的にどの医療に関する業務等に適用するかを定義すること…それぞれを担当する責任者（ユーザ）を具体的な職種や所属部署等…について定義すること…

<#>それぞれの責任者による記載…について…

削除: 規程

削除: 運用

削除: 規程で決められた

削除: 遵守するため

削除: <#>ルールの遵守.

<#>運用管理規程で決められた内容を遵守…

削除: の内部

削除: 除き、リモートログインが行なえない

削除: B-1. 医療機関等における留意事項

削除: されない…

削除: 場合】.

1)、最低限のガイドラインに記載し…

削除: が望ましい

削除: 高度な対策とは時々の向上が著しい技術的な対策が主であり、ここでは電子…

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。
（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　第４条第１項第一号　平成17年3月25日）

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条　(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

電子媒体に保存された内容を、権限保有者からの「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と操作方法で、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、権限保有者の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、媒体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形で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こと
- 記録が、他のファイルやマスタ等を参照する形で作成されることが多く、これらのデータの作成時点で採用したマスタ等が保存されなければ、正しい記録として見読できないこと
- 複数媒体に分かれて記録された情報の相互関係が、そのままでは一瞬にして判明しないこと

削除: 保存義務のある情報の見読性が確保されていること。。

削除: 第2

削除: 1

削除: 要求に基づき必要に応じて肉眼で見読可能な状態にできること。必要に応じてとは、

削除: 際して

削除: 、

削除: という

削除: 特に監査の場合においては、監査

削除: 求められている

削除: できず、また複数媒体に分かれて記録された情報の相互関係もそのままでは判りにくい。また、その

削除: から情報を取り出すには

削除: あり、表示のための編集前提となるマスタ、利用者テーブル等が別に存在したりする可能性がある。これらの見読化手段が日常的に正常に動作することが求められる。。
また、必要な情報を必要なタイミングで正当な情報利用者に提供できなかったり、記録時と異なる内容で表示されたりすることは、重大な支障となるので、それを防ぐためのシステム全般の保護対策が必要で

削除: 見読性の観点では、

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無い最低限の見読性を確保するための対策を考慮しておく必要がある。

ネットワークを通じて外部に保存する場合は、回線や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し含めた十分な配慮が求められる。その際には、「4.2　責任分界点について」を参考にしつつ、予め責任を明確化しておき、速やかな復旧ができるように配慮しておく必要もある。

これらのように配慮していても、保存している情報が利用出来ない場合等は、可能な限り速やかに復旧に努め、診療、患者への説明、監査、訴訟等の要求に応じた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、患者毎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も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、システムの冗長化や代替え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。

削除: が

削除: である

削除: さらに、「診療」、「患者への説明」時に求められる見読性は、主治医等の医療従事者に対して保障されるべきものであり、緊急時等においても、医療従事者が診療録等を閲覧するために、もず医療従事者以外の許可を求める必要がある等の制約はあってはならない。。
また、

削除: 厳密な意味で見読性の確保を著しく難しく

削除: ように見える。しかし、見読性は本来、「診療に用いるのに支障がないこと。」と「監査等に差し支えないようにすること

削除: 事故や災害に備える

削除: 。

削除: 患者情報の確保を第一優先とし、季

削除: 診療終了後しばらくの間来院が見込

削除: 【医療機関等に保存する場合】

削除: とスループット

削除: 診療

削除: 。

削除: おいては、患者の前回の診療録等の

削除: なお、この場合の"速やかに"とは

削除: 見読手段

削除: 。

削除: <#>緊急に必要になることが予測さ

削除: <#>。

削除: 最低限のガイドラインに加え、障害

(2) 見読性確保のための外部出力

システムの停止した場合でも、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

大規模災害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、自施設に準じた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の情報について、[illegible] 情報を受託する機関等に対して、[illegible]

(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。

削除: を

削除: した

削除: 保存機能

削除: 検索

削除: の内部

削除: が望ましい

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。

（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（第1条第1項第[illegible]号）

[illegible]

「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 [illegible] 1 (4)）

削除: 保存義務のある情報の保存に関する

削除: 第2

削除: 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渡って真正性を保ち、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、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、設備の劣化による読み取り不能または不完全な読み取り
(4) 媒体・機器・ソフトウェアの整合性不備による復元不能
(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

ウイルスまたはクラッカー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恐れがある。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、及び仕様通りに動

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を置いてあ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に、許可された者以外が行えないような対策を施す必要がある。

また、万が一、滅失であるか改ざんまた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、設備の劣化による読み取り不能また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また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・ソフトウェアの整合性不備による復元不能

媒体・機器・ソフトウェアの整合性不備により、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、システムの移行時のマスタデータベース、インデックスデータベースの不整合、機器・媒体の互換性不備による情報復元の不完全・読み取り不能等である。このようなことが起こらないように、システム更新・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お託先

削除: 滅失

削除: また、電子的な情報を保存している媒体又は機器が置かれているサーバ室等への入室は、許可された者以外が行えないような対策を施す必要がある

削除: 紛失

削除: が起こった

削除: 元の情報が改ざんまたは破壊された場合には、そのバックアップから診療録等の情報を

削除: 滅失

削除: 記憶

削除: 記憶

削除: 記憶

削除: 記憶

削除: マスタDB、インデックスDB

削除: 継続

削除: きちんと

削除: あって

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でてくる。

その為、委託する医療機関等は、医療機関等から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、正しく保存されたことを確認してから行う必要がある。

削除: における

削除: 改ざんされることのないデータベース

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。

削除: 保存性を脅かす原因を除去するために真正性、見読性の最低限のガイドラインで述べた対策を施すことに加えて以下に述べる対策が実施することが必要である。

(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用量（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破損した時に、バックアップされたデータを用いて破損前の状態に戻せること。もし、破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わかるようにすること。

削除: 破損

削除: 破損前

削除: 破損前

削除: 失われた

削除: わかる

削除: の

(3) 記録媒体、設備の劣化による読み取り不能また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または記録機器に複写すること。記録する媒体及び機器毎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、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または記録機器については、そのデータを新しい記録媒体また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・ソフトウェアの整合性不備による復元不能の防止

1. システム更新の際の移行を迅速に行えるよう、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. [redacted]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おこなうこと

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または変更されることが考えられる。その場合、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おこなうこと

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おこなうこと。

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、設備の劣化による読み取り不能または不完全な読み取りの防止

1. 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もしくはRAID-1相当以上のディスク障害に対する対策を取ること。

【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】

(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

削除: ・システムの変更の際に際しても以前のシステムで蓄積した情報の継続的利用を図るための対策を実施すること。システム導入時に、契約等で、システム導入業者にデータ移行に関する情報開示条件を明確にし、システムの更新、データ移行を行う場合に、システム内のデータ構造が変わらないことに起因するデータ移行の手間を低減すること。開示条件には画像・解析・取扱い...

削除: マスタDB

削除: の内部

削除: .

<#>外部保存を受託する機関において保存したことを確認すること.

削除: 、外部保存を受託する機関はその区別を行い、、混同による障害を避けるとともに

削除: <#>情報の破壊に対する保護機能や復旧の機能を備えること.

故意または過失による情報の破壊がおこ...

削除: 保存性を脅かす原因を除去するために、上記の最低限のガイドラインに追加して真正性、見読性の推奨されるガイドライ...

削除: なお、改ざん等による情報の破壊が行われていないことが証明された場合は、元の情報が破壊された場合にその複製をお...

削除: は記録媒体に関しては、おもしくは以上の品質が保証された媒体に保存すること。.

削除: 5

削除: 医療機関等の内部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。.

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の入手困難となり、記録された情報を読み出すことに支障を生じる恐れがある。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。

削除: ・

8　診療録及び診療諸記録を外部に保存する際の基準

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。ひとつは電子媒体により外部保存を行う場合で、もうひと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 [illegible] 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

なお、第2版までの記載を以下のように修正しているのでご留意願いたい。

【第2版】8.1.1　電子保存の3基準の遵守
それぞれ真正性、見読性、保存性に分離して「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」に記載を統合。

【第2版】8.1.4　責任の明確化
「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、そちらを参照されたい。

更に、(2) 可搬媒体で外部保存を行う場合、(3) 紙やフィルム等の媒体で外部保存を行う場合に関連して規定されていた「【第2版】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」及び「【第2版】8.3　紙媒体のままで外部保存を行う場合」については、本ガイドラインで解説する電子的な医療情報の取り扱いとは異なるものであることから、それぞれ付則1及び2へと移動したので、そちらを参照されたい。

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、診療録等々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、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、情報の漏えいや診療に重しえる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。

削除: 電気通信回線を経由して、診療録等を外部機関に保存する場合には安全管理に関して、技術的にも情報学的にも十分な知識を持つことが求められる。。
一方、(2) 可搬媒体で外部保存を行う場合、(3) 紙やフィルム等の媒体で外部保存を行う場合については、保存場所を医療機関等に限るものではなく、保存を専門に扱う業者や倉庫等においても、個人情報の保護等に十分留意して、実施することが可能である。。
削除: 3版改定に伴い、第
削除: および
削除: および「
削除: 第3版からは
削除: および
削除: 電気通信回線
削除: 、先進的で
削除: 医療上の問題等
削除: 、
削除: 、
削除: なりかねず、

従って、[illegible] 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、[illegible] 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。

削除: 電気通信回線
削除: 、
削除: 、
削除: 、技術的にも情報学的
削除: も充分な知識を備えて
削除: して行くことが

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

A. 制度上の要求事項

電気通信回線を通じて外部保存を行う場合において、保存に係るコンピュータ、ネットワーク等の情報処理機器が医療法施行令の一部を改正する政令に規定する病院又は同条第一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、[redacted]震災対策等の危機管理上の目的[redacted]場所、[redacted]

（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。[redacted]

さらには、情報の保存を受託する機関等もしくは従業者[redacted]利益を目的とした不当利用の危惧が[redacted]。その一方で金融情報、信用情報、通信情報は[redacted]として、保存・管理を当該事業者以外の外部事業者に委託[redacted]おり、合理的に運用されている。金融・信用・通信に関する情報と医療に関す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となること[redacted]、医療機関等の開設者[redacted]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。[redacted]

[redacted]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「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」に該当する機関を選定する場合には、「C. 最低限のガイドライン」で定める事項を厳守し、また、データセンター等の情報処理関連事業者[redacted]

削除: および
削除: に
削除: 第1章
削除: 5章1項
削除: 2
削除: に置かれるものであること。）、
削除: ついては、ネットワークによる外部保
削除: のために、医療機関等が、医療機関
削除: でのネットワークによる外部保存を行
削除: また、安全に情報が保存された場所
削除: 蓄積された
削除: か、自らの営利や
削除: のために
削除: に
削除: することへの国民等
削除: 存在する
削除: 事案
削除: されて
削除: かかわる
削除: 係わる
削除: 医療機関等の本来の責務は情報を活
削除: の困難さ
削除: 大きい
削除: から、
削除: に対しては、個人情報保護法及び同
削除: による安全管理措置のみならず、厳
削除: 従って、診療録等のネットワーク
削除: に対して厳格な契約を含めた規定を

[redacted]「1. 保存場所に係る規定」、「2. 情報の取り扱い」、「3. 情報の提供」[redacted]考え方を整理する。

[redacted]「4. 電子的な医療情報を扱う際の責任のあり方」、「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、実施にあたっては、これらの指針も遵守する必要がある。

1.　保存場所に係る規定

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。

[redacted]、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[redacted]C 項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

①又は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場所が該当する。

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を目的としている必要がある。

また、情報を保管する機関が、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[redacted]C 項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。

2.　情報の取り扱い

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

削除: [redacted]
削除: [redacted]
削除: [redacted]
削除: [redacted]
削除: 地域医療連携等の情報連携に関
削除: ASP
削除: この場合、救急医療の確保を担う機関同士や民間医療機関との有機的な連携を推進すること等が必要な地域等で、診療録等の電子保存を支援することで質の高い医療提供体制を構築することを目的とし
削除: および
削除: および
削除: 、安全に情報が保存される場所を前提として医療機関等相互の有機的な情報連携や適切な患者への情報提供の実現に資する医療情報の提供体制と構築すること等
削除: および

る場合は、委託した病院、診療所など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、実施にあ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、取り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など、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、情報の取り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の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、も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

冒頭でも触れた通り、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。

現段階では、これらの行為を規制するための民間等の外部保存を受託する事業者に対する指針は存在しないが、その適合の遵守状況を踏まえながら十分検討が必要とされるべきである。

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

削除: および

削除: など

削除: 目的として取り扱う

削除: 明確な規制として

削除: 個人情報の保護に関する法律しか

削除: せず、身体情報の保護に関する特段

削除: 措置

削除: 講じられていないため、委託する医療機関等において、医療情報が機微

削除: ことを踏まえた契約や技術的担保等の特段の

削除: 情報の取り扱いを十分検討した上で実施する必要がある。

い適切に管理するなど、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、次のような方法が考えられる。

(a) 暗号化を行う

(b) 情報を分散保管する

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、すべ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などが考えられる。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。

暗号鍵の使用に当たっては、非常時に限定することとし、使用における運用管理規程の策定、使用したときにその痕跡が残る封印等の利用、情報システムにおける証跡管理等を適切に実施し、外部保存を受託する事業者による不正な利用を防止する措置をとらなければならない。

削除: したり

削除: など

削除: など

削除: など

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、情報の漏えい、異なる患者の情報を見せたり、患者に見せてはいけない情報が見えたり等の誤った閲覧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、医療法人等が患者に対し何らの同意も得ずに実施してはならない。

削除: 規程

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。その場合、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場合は、医療機関等も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ことし、情報の漏えい、異なる患者の情報を見せたり、患者に見せてはいけない情報が見えたり等の誤った閲覧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

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、個人情報の保護に関する法律に則り、患者の同意も得た上で実施する必要がある。

その場合、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場合は、医療機関等も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し、情報の漏えい、異なる患者の情報を見せたり、患者に見せてはいけない情報が見えたり等の誤った閲覧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おうとする場合は、委託した病院、診療所は、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[削除:]、取り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[削除:]、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、情報の漏えい、異なる患者の情報を見せたり、患者に見せてはいけない情報が見えたり等の誤った閲覧が起こらないように配慮すること

(カ) 情報の提供は、原則、患者の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および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、情報の漏えい、異なる患者の情報を見せたり、患者に見せてはいけない情報が見えたり等の誤った閲覧が起こらないようにさせること。

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[削除:]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、保存した情報の取り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) [削除:]

(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。

(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、医療機関等において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、情報の漏えい、異

削除: 、

削除: 外部保存を受託する事

削除: 耐震構造を有すること、免震設備

削除: 自家発電装置を装備している

削除: 、災害発生時

削除: 保存された情報の消失リス

削除: 対して適切な対処がなされていること。
安全な場所

削除: 提供または管理

削除: 外部保存を受託する事業者の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、ベンダ、コーザ制度や不当な運用範囲を定めた適用宣言書に基づくISMS認定制度等による正当な第三者の認定を受けていること。
外部保存を受託する事業者に対して、医療情報等の保存性確保のための情報セキュリティを設定している

削除: いかなる形態であれ、

なる患者の情報を見せたり、患者に見せてはいけない情報が見えたり等の誤った閲覧が起こらないようにさせること。

(キ) 医療機関等において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、の内、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、個人情報保護もしくは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の取得等が推奨される。

(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、上記のような第三者による認定制度も検討されたい。

(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」では、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、「(a)暗号化を行う」、「(b)情報を分散管理する」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。

削除: ①

削除: および

削除: したり

8.1.3 個人情報の保護

A. 制度上の要求事項

「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 (6)-[illegible])

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される必要がある。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り、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 章 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なうこと

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「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」において考え方が示されている。

「Ⅲ 医療・介護関係事業者の義務等」の「4. 安全管理措置、従業者の監督及び委託先の監督（法第20条～第22条）」及び本指針6章を参照し、適切な管理を行なうこと。

(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

削除: 第2 1 (3)

削除: 個人情報保護法が成立し、医療分野においても「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」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、上記ガイドラインを参照し、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）の責任によって個人情報が保護されており、その場合、個人情報の保護について遵守すべき基準は「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」であり、情報システムの安全管理に関しては本ガイドラインがその指針となる。

しかし、

削除: **<#>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。**
<#>秘匿性の確保のための適切な暗号化をおこなうこと。
秘匿性確保のために電気通信回線上は適切な暗号化を行い転送すること。
<#>通信の起点・終点識別のための認証をおこなうこと。
外部保存を委託する医療機関等と受託する事業者間の起点・終点の正当性を識別するために相互に認証を行うこと。
通信手段によって、起点・終点の識別方法は異なる。例えば、インターネットを用いる場合は起点・終点の識別は IP パケットを見る

削除: 3

…きである。

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

…

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…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…。

…、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しい。

削除: 患者自身の個人情報が外部保存されることに同意しない場合、その旨を申し出る必要がある。なお、外部保存に同意した後においてもその取り消しは可能である。ただし、診療録等が外部保存されることに同意が得られない場合でも、医師法等で定められている診療の応召義務には何ら影響を与えるものではなく、それを理由として診療を拒否することはできない。

(4)外部保存終了時の説明

外部保存された診療録等が、一定の期間を経過した後に廃棄等により外部保存の対象から除かれる場合には、診療前の外部保存の了解をとる際に合わせて患者の了解を得ることで十分であるが、医療機関や外部保存先の都合で外部保存が終了する場合や保存先の変更がある場合には、改めて患者の了解を得る必要がある。

削除: .

(5)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もちろん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し、理解を得ればよい。

削除: の同意を得る

削除: の同意

削除: 必要がある。

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 …)

本項の記載は、「1 電子的な医療情報を扱う際の責任のあり方」の「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」に基づきを規定したため、それらを参照されたい。

削除: 第5.1.1

削除: 章の

8.1.5 留意事項

…を通して外部保存を行い、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

削除: 電気通信回線

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。なお、すで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。」
（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、「1　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、すで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、終了しなければならない診療録等は速やかに処理を行い、処理が厳正に執り行われたかを監査する義務を果たさなくてはならない。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。

これらの厳正な取り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うるためであり、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。

削除: 高度

削除: なお、注意すべき点は、診療録等を外部に保存していること自体が院内掲示等を通じて説明され、患者の同意のもとに行われていることである。
これまで、医療機関等の内部に保存されて来た診療録等の保存に関しては、法令に基づいて行われるものであり、保存の期間や保存期間終了後の処理について患者の同意をとってきたわけではない。しかし、医療機関等の判断で実施される診療録等の外部保存においては、個人情報の存在場所の変更は個人情報保護の観点からは重要な事項である。このガイドラインでも、オンライン外部保存には原則として事前の説明と患者の同意を前提としている。
事前の説明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えるし、一連の診療の終了後○○年といった一定の条件が示されていることもありえる。
いずれにしても

削除: 当然のことであるが、

削除: もの

削除: なこと

削除: 電気通信回線

8.4.3 保存義務のない診療録等の外部保存について

[illegible]

削除: 本章は、法的に保存義務のある診療録及び診療に関する諸記録の外部保存について述べたものであり、保存義務のない記録については対象外である。保存義務のない記録とは、例えば、医師法の定めに従って作成・保存していた診療録で、診療終了後、法定保存年限である５年を経過した診療録や、診療の都度、診療録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等がこれにあたる。

削除: しかし、対象外となっている記録等を外部保存する場合であっても、個人情報の保護については、法的な保存義務の有無に関わらず留意しなければならないことは明白である。情報管理体制確保の観点から、バックアップ情報等も含め、記録等を破棄せず保存している限りは本章ガイドラインの取扱いに準じた形で保存がなされること。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て管理に万全を期す必要がある。

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

本章は法令等で作成または保存を義務付けられている診療録等をいったん紙等の媒体で［illegible］、スキャナ等で電子化し、保存または運用する場合の取扱いについて記載している。電子カルテ等システムを入力する際に、紙に描画しスキャナやタブレット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すること。

A. 制度上の要求事項

［illegible］

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で、診療の大部分が電子化された状態で行われている場合で、他院からの診療情報提供書等の、紙やフィルムが［illegible］事情で生じる場合。

(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。

削除: <注意>．

削除: 保存・運用

削除: の注意

削除: ．

削除: 　A. 制度上の要求事項．

<#>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、保存義務のある書類としての必要な情報量を確保するため、光学解像度、セピア等の一定の規格・基準を満たすスキャナを用いること。

<#>改ざんを防止すること。

<#>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、停電時の補助電源の確保、システムトラブルに備えたミラーサーバーの確保等の必要な体制を構築すること

<#>スキャナにより読み取った情報が、点検等で定められた期間は、適切かつ安全に保存されるよう、ソフトウェア・機器及び媒体の適切な管理を確保すること。

<#>個人情報の保護のため個人情報保護関連各法を踏まえた所要の取扱いを講じること　医療機関等の外部での電子保存については本ガイドラインの8章を参照すること（施行通知　第二　２(2)②、(3)）

削除: による媒体

削除: やむを得ない

削除: の媒体

削除: 媒体の

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りえない。従って、もともと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きわめて有効であり、可能であれば院外部への保存も含めて検討されるべきである。［illegible］これらの場合の対策に関しては、「9.4（補足）　運用の利便性のためにスキャナ等で電子化をおこなう、紙等の媒体もその上保存をおこなう場合」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、セピア等の一定の規格・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な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、［illegible］でスキャンを行なうこと。
   - 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 2.0 版（平成 18 年 1 月）」を公表しており、参考にされたい。なお、このガイドラインではマンモグラフィーは対象とされていないが、同委員会で検討される予定である。
   - 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、さまざま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［illegible］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、非可逆圧縮をおこな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おこなう必要がある。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

削除: ［illegible］

削除: 300dpi，RGB 各色８ビット（24ビット）以上

削除: 一般的に使めて精細な精度

削除: 必要なもの以外は 300dpi，24 ビットのカラー スキャンで行なうことおよび、あくまでも

削除: TIFF 形式または PDF

削除: が望ましい

- スキャナにより読み取った電子情報ともと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(実施者または管理者)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、電子署名及び認証業務に関する法律（平成12年法律第102号）第2条第1項に規定する電子署名については、6.9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

削除: の同一性

削除: 署名法に適合した電子署名とは、これを行うための私有鍵の発行や運用方法を適正に管理することにより、本人だけが行うことができる電子署名を指す。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い場合は、少なくとも同様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

削除: <#>スキャナで読み取る際は、読み取った後、遅滞なくタイムスタンプを電子署名を含めたスキャン文書全体に付与すること。。
なお、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、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、スキャン後の電子化文書を利用する第三者がタイムスタンプを検証することが可能である事。。
また、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。。

削除: <#>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、停電時の補助電源の確保、システムトラブルに備えたミラーサーバーの確保等の必要な体制を構築すること。
。
<#>個人情報の保護のため個人情報保護法を踏まえた所要の取扱いを講じること。特に電子化後のもとの紙媒体やフィルムを破

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で、診療の大部分が電子化された状態で行われている場合で、他院からの診療情報提供書等の紙やフィルムによる媒体が混在している場合で、媒体が混在することで、医療安全上の問題が生じるおそれがある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

9.1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、また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程度に早い時点の通常運用における期間で、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止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。

削除: A. 制度上の要求事項。
<#>改ざんを防止するため情報が作成されてから、または情報を入手してから一定期間以内にスキャナによる読み取り作業を行うこと。
（施行通知 第二 2（2）ロ、（3）

削除: やむを得ない

削除: おこなわれる

削除: 機会

削除: 通常の

削除: 行なわなければ

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とることが求められる。「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、厳格な監査を実施すること、である。

C. 最低限のガイドライン

9.1の対策に加えて、以下の対策を実施すること

1. 電子化をにあ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ことを掲示等で周知し、異議の申し立てがあった場合はスキャナ等で電子化をこと。

2. かならず実施前に実施計画書を作成すること。実施計画書に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し立てに対する対応。
   - 相互監視を含む実施の体制。
   - 実施記録の作成と記録項目。（次項の監査に耐えう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から紙やフィルム破棄までの期間、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こと。

4. 外部事業者に委託する場合は、9.1の要件を満たすことができる適切な事業者を選定する。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ことを具体的に明記すること。

削除: A. 制度上の要求事項 .

<#>個人情報を保護する観点から、スキャナによる読み取りを実施する前に[illegible]の対象となる患者又はその看護に当たる者等（以下「患者等」という。）に院内掲示等による情報提供を行うこと。患者等から異議の申し出があった場合は、スキャナによる読み取りを行わない等の必要な配慮を行うこと。

<#>作業における個人情報の適切な保護を図るため、所要の実施計画及び上記運用管理規程の事前作成、スキャナによる読み取り作業終了後の監査等を確保すること。

<#>外部事業者に委託する場合には、安全管理上、スキャナによる読み取りを医療機関等が自ら実施する際に必要な9.1の技術的な基準及び個人情報保護に係る要件を満たす事業者を選定し、契約上も安全管理等に必要なこれらの要件を明記すること。

（施行通知 第二 2（2）②、（3）...

削除: 要点は

削除: おこなう

削除: おこなう

削除: おこなわない

削除: おこなう

削除: おこなって

削除: を

削除: する

削除: 3.

削除: をおこなう

削除: おこなう

削除: おこなう

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

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必要であり、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、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知れない。従って運用の利便性のためとは言え、電子化情報はもと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、もともと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さげることもできる。
   - 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 2.0版（平成18年4月）」を公表しており、参考にされたい。なお、このガイドラインではマンモグラフィーは対象とされていないが、同委員会で検討される予定である。
   - 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、さまざまな対象が考えられる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、非可逆圧縮をおこな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おこなう必要がある。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

削除: おこなう

削除: おこなう

削除: [illegible]

削除: 原則として300dpi、RGB各色8ビット（24ビット）以上

削除: 一般的に極めて精細な精度が必要なもの以外は300dpi、24ビットのカラースキャンで十分と考えられるが、[illegible]。

削除: TIFF形式またはPDF

削除: が望ましい

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。

削除: 個人情報の保護のため個人情報保護関連各法を踏まえた所要の取扱いを講じること。特に

削除: もと

削除: もおろそかにならないように注意しなければならない。

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。

削除: きわめて

A. 制度上の要求事項

1) 平成16年の「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」

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 第三）

○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

医療機関等では規模、診療内容等に応じて様々な形態があり、運用管理規程も当然に様々な様式・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ある。(1)に電子保存する・しないに拘わらず必要な一般管理事項を、(2)に電子保存の為の運用管理事項を、(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、そして(5)に運用管理規程の作成にあ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「推奨」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

- 情報の範囲
- 利用者の職種
- 組織内の情報システムの範囲
- 情報システムで扱う情報の一覧

② 管理体制

a) システム管理者、機器管理者、運用責任者(システムの理解と説明、情報漏洩責任者など)

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) 患者からの苦情・質問の受け付け体制

e) 事故対策(緊急時及び災害時の連絡、復旧体制)

f) 利用者への教育と訓練(定期または不定期)

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」へあなたの病院の個人情報を守るために(財)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

b) 情報保存装置、アクセス機器の設置区画の管理・監視

- 情報

d) [illegible]の記録媒体の管理(保管・授受等)

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

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

h) 技術的安全対策

- 利用者識別と認証
- アクセス権限管理
- アクセスログ取得と監査
- 時刻同期
- 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

i) 無線LANに関する事項

- 無線LAN設定(アクセス制限、暗号化など)
- 電波障害の恐れがある機器の使用制限

j) 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[illegible]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[illegible]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[illegible]

- 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[illegible]
- [illegible]の採取と確認

削除: 運用管理規程に、[illegible]考え方に書いてある通り保存義務の期間を定め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基準、すなわち診療録等の外部保存に関する基準、を満足するために技術的に対応するよう、運用において対応するよう規定、その内容が期間満了後も破棄せず保存する旨を盛り込まなければならない。

削除: の任命

削除: <#>作業担当者の限定。

削除: の任命

削除: 窓口の設置

削除: 周知法

削除: <#>委託契約における個人情報保護の徹底。

削除: 事項

削除: 、

削除: 、

削除: 、

削除: 、

削除: 、

削除: に関する規程

削除: 、

削除: 取り扱い

削除: データ整合

削除: 病院関係者

削除: 監督

削除: <#>保守契約における個人情報保護の徹底。

⑥ 情報およ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および情報機器の規程
b) 持ち出した情報および情報機器の運用管理規程
c) 持ち出した情報およ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と、

削除: 従業員

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) 情報処理事業者等との通常運用時、事故対処時における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

削除: モバイル端末等を使って

e) 事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

削除: 接続

・ アクセスに用いる機器の安全管理

削除: を許容する状態

⑧ 災害等の非常時の対応

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

削除: <#>ログ取得方法。
<#>許容したアクセス状態の保持確認規程。

⑨ 教育と訓練

a) マニュアルの整備
b) 定期また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

運用管理規程の定期的見直し手順

(2) 電子保存の為の運用管理事項

① 真正性確保

a) 作成者の識別及び認証
b) 情報の確定手順と、作成責任者の識別情報の記録
c) 更新履歴の保存
d) 代行操作の承認記録
e) 機器・ソフトウェアの品質管理

削除: <#>一つの診療経等で複数の医療従事者が共同して作成する場合の管理。

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

削除: <#>診療目的。
<#>患者説明。
<#>監査。
<#>訴訟。

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
・ 記録媒体の劣化による読み取り不能または不完全な読み取りの防止策
c) 記録媒体、設備の劣化による読み取り不能または不完全な読み取りの防止策
d) 媒体・機器・ソフトウェアの整合性不備による復元不能の防止策
・ システムの移行時にデータの互換性、機器・媒体の互換性の確保と
システムの更新・移行時の業務計画の策定

削除: <#>万が一に備えての考慮対策。
<#>情報の継続性の確保策（例えば、媒体の劣化対策等）。
<#>情報保護機能策（例えば、バックアップ等）。

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

削除: 利用性

(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、可搬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[redacted]と判断した根拠記載」など

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」に記された要件を参照のこと。

[redacted]

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) [redacted]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」に記された要件を参照のこと。

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

受託事業者に診療録等が残ることがない[redacted]

a) 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) [redacted]

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[redacted]

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[redacted]

削除: 適切な事業者

削除: の

削除:

削除: 事故等

削除:

削除: 、

削除: 様な処理法

削除: <#>リモートログイン制限機能。

削除: 上記事項は推奨

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

[redacted]

b) 標準的なデータ形式及び転送プロトコルの採用[redacted]

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」に記された要件を参照のこと。

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[redacted]

b) 患者本人の[redacted]を得ることが困難であるか診療上の緊急性がある場合[redacted]

c) 患者本人の[redacted]を得ることが困難であるか診療上の緊急性が特にない場合[redacted]

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[redacted]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、実施者または管理者への電子署名及び認証業務に関する法律、電子署名法」に適合した電子署名[redacted]

[redacted]

④ 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

削除: <#>上記事項は推奨。

削除: <#>電気通信回線で外部保存を受託する事業者の選定基準。

<#>電気通信回線で外部保存を受託する事業者の真正性確保。

<#>上記事項は推奨。

<#>情報保護機能。

削除: と同意

削除: 同意

削除: 同意

削除: 、

削除: 同意

削除: 、

削除: の同一性

削除: 1

削除: 1

削除: 1

削除: 1

削除: 、

<#>スキャナ読み取り電子情報への正確な読み取り時刻の付加。

＜運用管理規程の作成にあたって＞

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。即ち、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。勿論、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ける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。

運用管理規程は、かつ1冊の独立した文書である必要性は無い。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、各々ガイドラインで記載された事柄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、業務単位に到り易くまとまっていることが望ましい。

運用管理規程書を作成する場合の進め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言うものではなく、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。

削除: 電子保存及び外部保存の

削除: 具体的な

削除: から選択

削除: 一部変更

削除: から選択し、医療機関等ごとの独自性を一部変更する方法で

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、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おおむ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り、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となる。

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は保存義務のある文書と同等に扱うべきである。

削除: 、電気通信回線上の脅威に基づく

削除: 次第

削除: 今後とも

削除: していく

削除: した場合に

削除: したり

削除: と考えられる

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)）

削除: 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おおむ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把握し、事故・紛失等の発生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、継続して診療をおこなっている場合で、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か、外部に保存しても、保存情報の複製また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、搬送に若しくは時間を要する遠方に外部保存しない限りは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ともなう相互利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、新たな媒体また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

「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

個人情報保護法が成立し、医療分野においても「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」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、上記ガイドラインを参照し、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に、より一層の個人情報保護に配慮が必要である。

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される必要がある。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。

- **診療録等を記録した可搬媒体の遺失防止**
  運搬用車両を施錠したり、搬送用ケースを封印する等の処置を取ることによって、遺失の危険性を軽減すること。
- **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

削除: 、なりすましや盗聴、改ざん等の脅威下にある情報の大量漏えいや大幅な書換え等、市販の電気通信網上の脅威に基づく危険性は少ないが、一方

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。

・ **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、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、やむをえ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の最低限のガイドラインに加えて以下の対策をおこなうこと

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、診療を開始するべきである。

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し、理解を得ればよい。

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 責任分界点について」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。

削除: 患者自身の個人情報が外部保存されることに同意しない場合は、その旨を申し出なければならない。ただし、診療録等を外部に保存することに同意を得られなかった場合でも、医師法等で定められている診療の応召義務には何ら影響を与えるものではなく、それを理由として診療を拒否することはできない。

<u>外部保存終了時の説明</u>

外部保存された診療録等が、予定の期間を経過した後に廃棄等により外部保存の対象から除かれる場合には、診療前の外部保存の了解をとる際に合わせて患者の了解を得ることで十分であるが、医療機関等や外部保存を受託する機関の都合で外部保存が終了する場合や受託機関の変更がある場合には、改めて患者の了解を得る必要がある。

削除: の同意

また、万が一事故が起きた場合に、患者に対する責任は、4.1 における事後責任と表中、説明責任は委託する医療機関等が負うものである、適切に善後策を講ずる責任を単なる 4.2 の責任分界点を明確にしただけで委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、患者に違反した場合はその責任を負うことになる。

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・再検討を常に心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 責任分界点について」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えるし、一連の診療の終了後○○年といった一定の条件が示されていることもありえる。

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、終了しなければならない診療録等は速やかに処理を行い、処理が厳正に執り行われたかを監査する義務を果たさなくてはならない。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うるためであり、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。

更に、委託する医療機関等及び受託する機関が負う責任は、先に述べた通りであり、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ものではないことには十分留意する必要がある。

削除: なお、注意すべき点は、診療録等を外部に保存していること自体が院内掲示等を通じて説明され、患者の同意のもとに行われていることである。

これまで、医療機関等の内部に保存されてきた診療録等の保存に関しては、患者に基づいて行われるものであり、保存の期間や保存期間終了後の処理について患者の同意をとってきたわけではない。しかし、医療機関等の責任で実施される診療録等の外部保存においては、個人情報の存在場所の変更は個人情報保護の観点からは重要な事項である。

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

継続して診療をおこなっている場合等で、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

「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

個人情報保護法が成立し、医療分野においても「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」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、上記ガイドラインを参照し、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、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に、より一層の個人情報保護に配慮が必要である。

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でも、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される必要がある。また、ハードウェア・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、運搬用車両を施錠したり、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[redacted]、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。

削除: の混同が予測される場合には、他の搬送物と

削除: 分け　たり

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、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委託し、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も、個人情報保護法による安全管理義務が画されており、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、万一事故が発生した時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、しっかりした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

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べきである。。

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

[redacted]

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

削除: 患者が自らの個人情報の外部保存を拒否することに同意しない場合は、その旨を申し出なければならない。

削除: なお、診療録等（体制、保存中）ことに同意を得られなかった場合でも、医師法等で定められている診療の応召義務の規定等により、何も診療できないとするものではなく、その理由として診療を拒否することはできない。

#外部保存終了時の説明。

外部保存された診療録等が、千定の期間を経過した後に廃棄等により外部保存の対象から除外される場合には、診療前の外部保存の了解をとる際に合わせて患者の了解を得ることで十分である。医療機関等や外部保存を受託する機関の都合で外部保存が終了する場合や、受託機関の変更がある場合には、改めて患者の了解を得る必要がある。

削除: .

#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そのことが困難な場合で、診療上の緊急性がある場合もそうした事情の説明をして要しない。意識が回復した場合には事後に説明して、理解を得ればよい。。

削除: の同意

乳幼児の場合も含めて本人へ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。

削除: の同意

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　責任分界点について」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、万が一事故が起きた場合に、患者に対する責任は、4.1 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が、適切に善後策を講ずる責任を果たし、予め 4.2 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・再検討を常に心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　責任分界点について」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

削除: なお、注意すべき点は、診療録等を外部に保存していること自体が院内掲示等を通じて説明され、患者の同意のもとに行われていることである。
これまで、医療機関等の内部に保存されて来た診療録等の保存に関しては、法令に基づいて行われるものであり、保存の期間や保存期間終了後の処理について患者の同意をとってきたわけではない。しかし、医療機関等の責任で実施される診療録等の外部保存においては、個人情報の存在場所の変更は個人情報保護の観点からは重要な事項である。

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えるし、一連の診療の終了後5年といった一定の条件が示されていることもありえる。

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査し、必要な改善がなされない診療録等は速やかに処理を行い、処理が厳正に執り行われたかを監査する義務を果たさなければならない。また、受託する機関と、委託する医療機関等の責任分界点で、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手渡す必要がある。

当然のことであるが、これらの廃棄に関する規定は、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、事前に廃棄プロセス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ため、同意した期間を超えて個人情報を保持することを目指し、個人情報の保護上問題となりうるためであり、そのことに十分なご留意をお願いしたい。

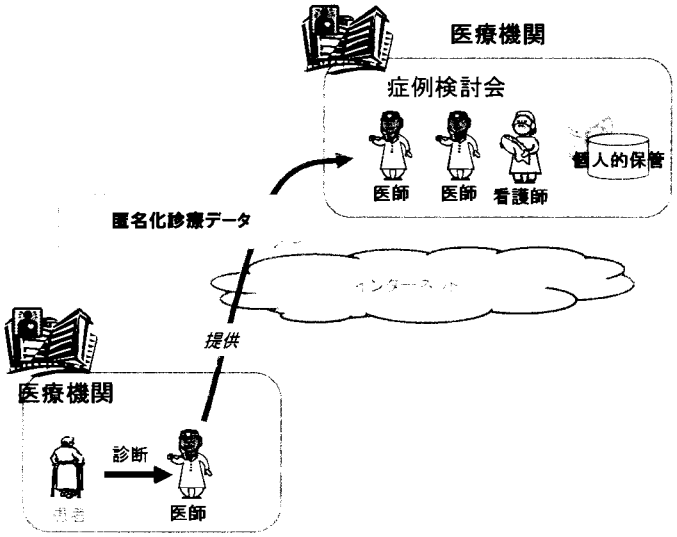
また、患者の個人情報に関する検索サービスを実施している場合は、検索のための台帳やそれに代わるもの、及び検索記録も機密保持できる状態で廃棄しなければならない。

更に、委託する医療機関等及び受託する機関が負う責任は、先に述べた通りであり、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ものではないことには十分留意する必要がある。

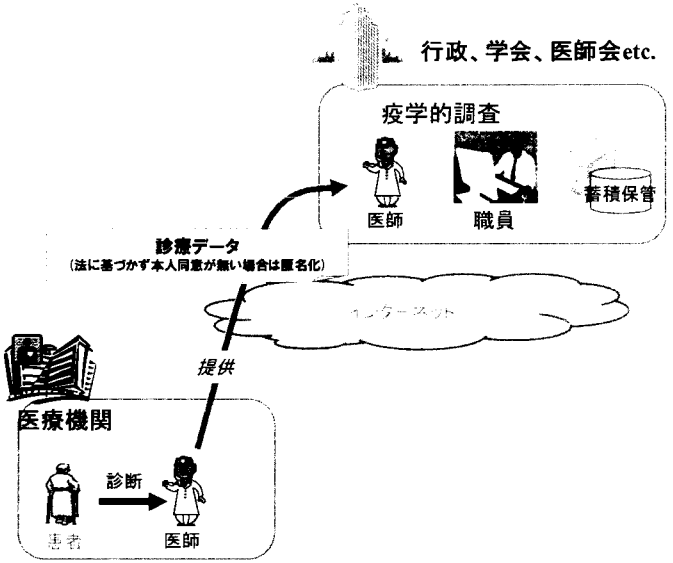
資　料　4

ユースケース図

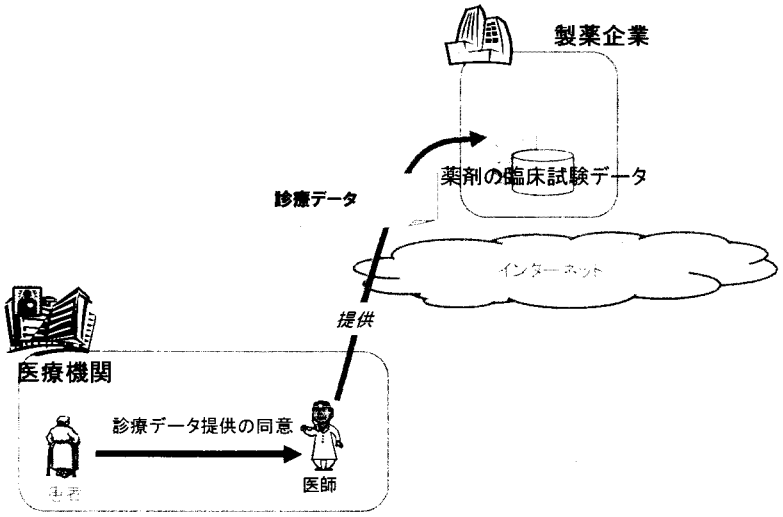
ケース1
（症例検討会）



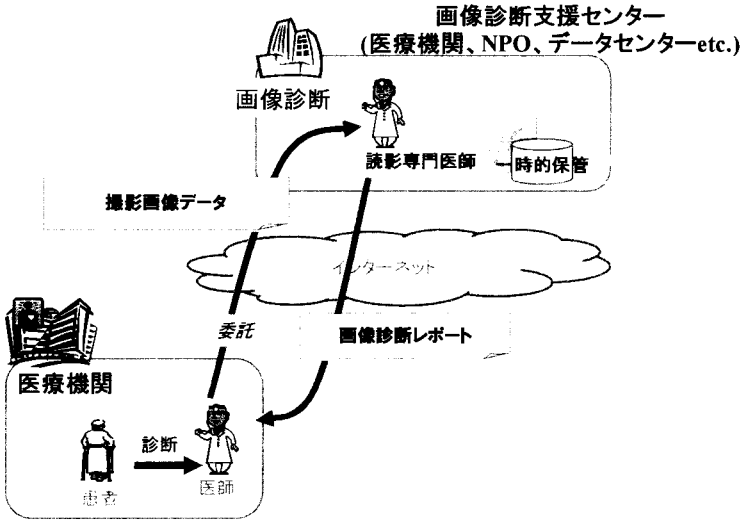
ケース2
（疫学的調査）



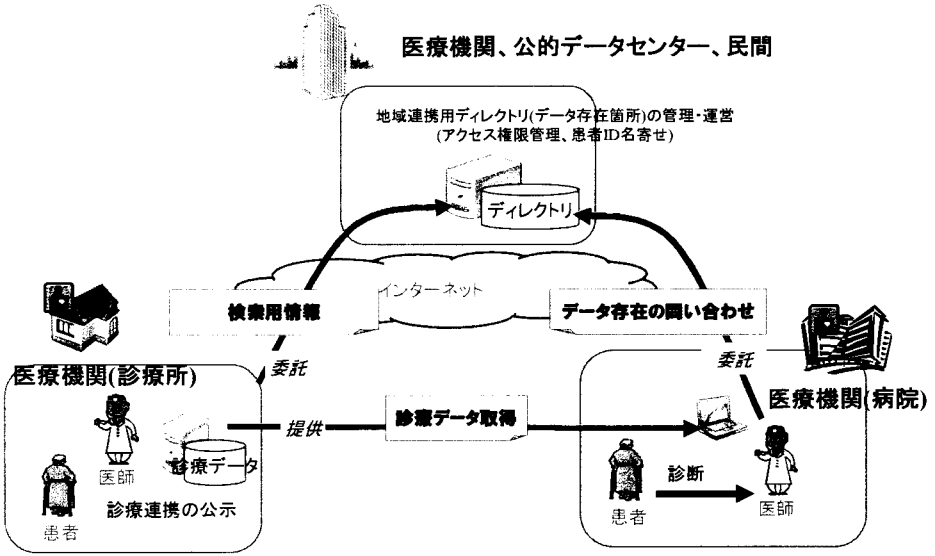
ケース3
（臨床治験）



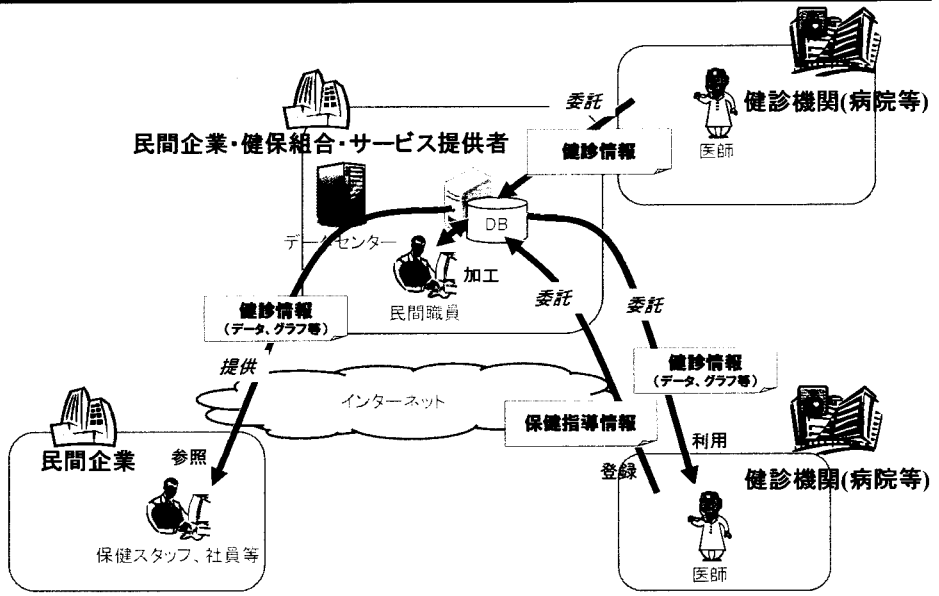
ケース4
（遠隔画像診断）



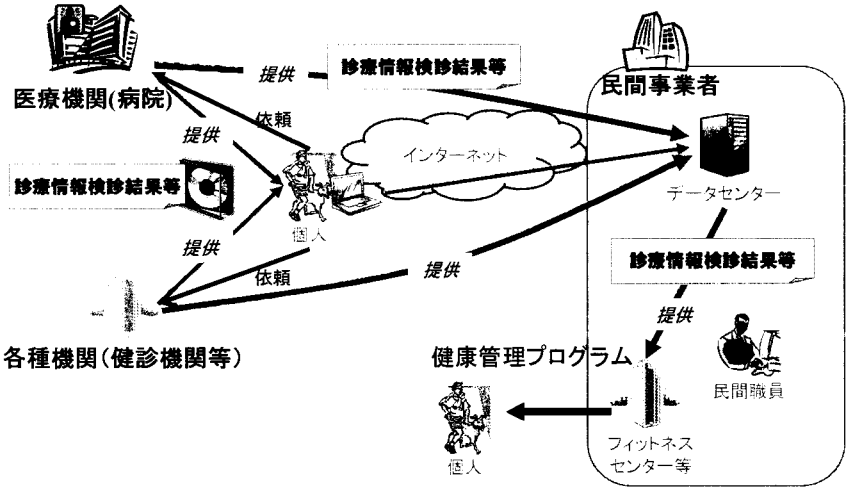
ケース5
（地域連携用ディレクトリ運営）



ケース6
(保健事業支援サービス)



ケース7
（健康増進サービス）



ケース8
（健康・医療情報個人管理サービス）