ても複製または同等の内容を医療機関等の内部に保持すること。

D. 推奨されるガイドライン

【医療機関等に保存する場合】

最低限のガイドラインに加え、障害対策として下記の対策が講じられることが望ましい。

(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。

(2) 見読性を確保した外部保存機能

システムが停止した場合でも、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ができるように、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検索機能

大規模火災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、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。

【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。

(1) 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

保存義務のある情報の保存性が確保されていること。
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4条第4項第三号)

「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

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

ウイルスまたはバグ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。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。

また、万が一、紛失又は破壊が起こった場合に備えて、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、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、記憶媒体や記憶機器の劣化特性を考慮して、劣化が起こる前に新たな記憶媒体や記憶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DB、インデックスDB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、業務継続計画をきちんと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、障害があって正しいデータが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における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、改ざんされることのないデータベースへ保存されたことを確認してから行う必要がある。

C. 最低限のガイドライン

【医療機関等に保存する場合】

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及び以下に述べる対策を実施することが必要である。

(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。

(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. サーバの設置場所には、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、失われた範囲が容易にわかること。

(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. 記録媒体の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. システムの変更に際して、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、旧システムから新システムに移行する

場合に、システム内のデータ構造が分からないことに起因するデータ移行の不能を防止すること。開示条件には倒産・解散・取扱い停止などの事態にも対応できることを含める必要がある。

2. システム更新の際の移行を迅速に行えるように、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。
3. マスタ DB 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】

医療機関等の内部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) 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

外部保存を受託する機関におけるデータベースへの保存を確認した情報を受け取ったのち、委託する医療機関等における処理を適切に行うこと。

(2) 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、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、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。

(3) 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。

(4) 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らないよう、情報保護機能を備えること。また、万一破壊がおこった場合に備えて、必要に応じて回復できる機能を備えること。

D. 推奨されるガイドライン

【医療機関等に保存する場合】

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ンで述べた対策及び以下に述べる対策を実施することが必要である。

(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の防止

1. 電子的に保存された診療録等の情報にアクセスするシステムでは、ウイルス対策ソフト等を導入し、定期的にウイルスの検出を行い、ウイルスが発見された場合には直ちに駆除すること。また、ウイルス定義ファイルは常に最新の状態に保つように、端末の運用管理を徹底すること。
2. アンチウイルスゲートウェイ等を導入し、院内のシステムにウイルスが侵入することを防止すること。また、ウイルス定義ファイル更新用のサーバを導入する等の方策により、各端末に導入したウイルス対策ソフトの定義ファイル及びバージョンが、常に最新の状態に保たれるようにシステム的な対策を施すこと。

(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、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。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診療に用い、保存義務を満たす情報として扱うこととする。

(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. 記録媒体に関しては、あるレベル以上の品質が保証された媒体に保存すること。
2. 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-5 相当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】

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。

(1) 標準的なデータ形式及び転送プロトコルを採用すること

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) 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

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が入手困難となり、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、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が望ましい。

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

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。

なお、第3版改定に伴い、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。

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。

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」および「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「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」および「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、第3版からはそれぞれ付則1および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、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。

電気通信回線を通じて外部保存を行う方法は、先進的で利点が多いが、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、情報の漏えいや医療上の問題等が発生し、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ず、慎重かつ着実に進めるべきである。

従って、電気通信回線を経由して、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、技術的にも情報学的にも充分な知識を結集して推進して行くことが求められる。

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。

8.1.2 外部保存を受託する機関の選定基準および情報の取り扱いに関する基準

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あっては、保存に係るホストコンピュータ、サーバ等の情報処理機器が医療法第１条の５第１項に規定する病院又は同条第２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に置かれるものであること。」

○「官民の地域医療機関間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する場合は、情報管理体制の確保のための一定の安全基準を満たす場合に限り、行政機関等が開設したデータセンター等ついては、オンラインによる外部保存を受託可能とする。」

○「震災対策等の危機管理上の目的のために、医療機関等が、医療機関等以外の場所でのオンラインによる外部保存を行うことが特に必要な場合は、情報管理体制の確保のための一定の安全基準を満たす場合に限り、外部保存を容認する。」

（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。

また、安全に情報が保存された場所を通じて医療機関等が相互に有機的な情報連携や適切な患者への情報提供を実施できれば、より一層の地域医療連携の促進や患者の利便性向上も期待できる。

一方、保存機関の不適切な情報の取り扱いにより患者等の情報が瞬時に大量に漏えいする危険性も存在し、その場合、漏えいした場所や責任者の特定の困難性が増大する。そのため、常にリスク分析を行いつつ万全の対策を講じなければならない。また、一層の情報改ざん防止等の措置の必要性が高まり（責任の所在明確化、経路のセキュリティ確保、真正性保証等）、医療機関等の責任が相対的に大きくなる。

さらには、蓄積された情報の保存を受託する機関等もしくは従業者が、自らの営利や利益のために不当に利用することへの国民等の危惧が存在する。その一方で金融情報、信用情報、通信情報は事実として保存・管理を当該事業者以外の外部事業者に委託されており、合理的に運用されている。金融・信用・通信にかかわる情報と医療に係わる情報を一概に同様に扱うことはできないが、医療機関等の本来の責務は情報を活用し健康の維持・回復を図ることで、情報の管理はそのための責務に過ぎない。

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の困難さが大きいことから、医療機関等に対しては、個人情報保護法及び同法に基づく各種ガイドラインによる安全管理措置のみならず、刑法及び保健師助産師看護師法等の資格法において医療関係資格者について、また、不妊手術、精神保健、感染症等の各関係法律に、資格者でない職員についても、罰則付きの守秘義務が規定されている。さらには、医療法や薬事法において、管理者に対し従業者に対する監督義務を規定しており、個人情報保護法とあいまって、管理者を通じた個人データを取り扱う従業者への監督がなされることになる等、格別の安全管理措置を講じることが求められている。

従って、診療録等のネットワークを通じた医療機関等以外の場所での外部保存については、こうした医療機関等に求められる安全管理上の体制と同等以上の体制を確保した上で、法令上の保存義務を有する保存主体の医療機関等が電子保存された医療情報等を必要時に直ちに利用できるように適切かつ安全に管理し、患者に対する保健医療サービス等の提供に当該情報を利活用するための責任を果たせることが原則である。

冒頭述べたように医療機関等の利便性向上、また、IT 化の進展に伴い、IT を活用することで地域医療連携の促進、患者の利便性向上を図ることが可能となってきている。その場合、医療に関連した情報がネットワーク上やサイバー（仮想）空間上に存在し、それらの情報に触れる事業者等が多岐に渡ってくる。

その際には、不適切な情報の取り扱いによる情報漏えいや不当な営利、利益を目的とした活用がなされることに対する国民等の危惧に十分に配慮する必要がある。

特に以下の「C. 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」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」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に対して厳格な契約を含めた規定を外部保存を委託する医療機関等が厳守させなくてはならない。

そのため、さらに「1. 保存場所に係る規定」、「2. 情報の取り扱い」、「3. 情報の提供」で考え方を整理する。

なお、本章は「4. 電子的な医療情報を扱う際の責任のあり方」および「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」と不可分であるため、実施にあたっては当該規定も併せて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、診療所が地域医療連携等の情報集約機能を果たす、もしくは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 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。

この場合、政策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、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、保存性および 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および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、安全に情報が保存された場所を通じ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が途切れない医療情報の提供体制を構築すること等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、保存性および 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る場合は、委託した病院、診療所および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分析、解析等を行うことは許されない。

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、情報を閲覧、分析等を目的として取り扱うことはあってはならず、許されない。

現段階では民間等の外部保存を受託する事業者に対する明確な規制としては個人情報の保護に関する法律しか存在せず、身体情報の保護に関する特段の措置が講じられていないため、委託する医療機関等において、医療情報が機微であることを踏まえた契約や技術的担保等の特段の保存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。

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い適切に管理したり、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などの利用、情報システムにおける証跡管理などを適切に実施し、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。

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、診療所は適切なアクセス権限を規程し、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、診療所が何らの同意も得ずに実施してはならない。

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などし、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などし、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、診療所および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程し、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もしくは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

(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) 外部保存を受託する事業者が耐震構造を有すること、電源設備等に自家発電装置を装備している等、災害発生時に保存された情報の消失リスクに対して適切な対処がなされていること。

(エ) 安全な場所を提供または管理する外部保存を受託する事業者が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、プライバシーマーク制度や不足なく適用範囲を定めた適用宣言書に基づく ISMS 認定制度等による公正な第三者の認定を受けていること。

(オ) 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厳格なルールを設定していること。

(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。

(キ) いかなる形態であれ、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。

(ク) 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。

(ケ) 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」および「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」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。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。

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 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、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

① 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

② 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 パケットを見るだけでは確実にはできない。起点・

終点の識別が確実でない場合は、公開鍵方式や共有鍵方式等の確立された認証機構を用いてネットワークに入る前と出た後で外部保存を委託する医療機関等と受託する事業者を確実に相互に認証しなければならない。例えば、認証付きのVPN、SSL/TLSやISCLを適切に利用することにより実現できる。当然のことではあるが、用いる公開鍵暗号や共有鍵暗号の強度には十分配慮しなければならない。

なお、情報の暗号化、電気通信回線における留意事項等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」の「B-1. 医療機関等における留意事項」および「B-2. 選択すべきネットワークのセキュリティの考え方」を参照されたい。

(2) 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。

(3) 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べきである。

患者は自分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。なお、外部保存に同意した後においてもそれを取り消すことは可能である。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。

② 外部保存終了時の説明

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。

③ 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。

④ 患者本人の同意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。

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　第２　１（４））

本項の記載は、「4　電子的な医療情報を扱う際の責任のあり方」および「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、それらを参照されたい。

8.1.5 留意事項

電気通信回線を通じて外部保存を行い、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。