

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)

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

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減失してしまうか、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。

C. 最低限のガイドライン

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。

D. 推奨されるガイドライン

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を取得し、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。

7.4 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」（平成12年法律第102号。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・押印とことなり、A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。

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) 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. 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、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。

2. 「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14年法律第153号）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。

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等の可搬型媒体で行う場合
- (3) 紙やフィルム等の媒体で外部保存を行う場合

医療機関等であれば、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ことが可能とされ、また、「医療情報ネットワーク基盤検討会」の最終報告でそれ以外にも外部保存に係る業務を受託可能な場合が提言されている。しかし、実際に運用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)可搬型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。

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機関において、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、情報の漏洩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十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

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))

B. 考え方

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概ね対応が可能と考えられるが、これに加え、伝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の対応について注意する必要がある。

真正性については、第三者が診療録等の外部保存の受託先の機関になりすまして、不正な診療録等を、外部保存の委託元の医療機関等へ転送することは、診療録等の改ざんとなる。また、電気通信回線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。

見読性については、外部機関に保存を行うことは、厳密な意味で見読性の確保を著しく難しくするよう見える。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。」の2つの意味があり、これを両方とも満たすことが実質的な見読性の確保と考えてよい。この際、診療上緊急に必要なことが予測される診療録等の見読性の確保については、外部保存先の機関が事故や災害に陥ることを含めた十分な配慮が求められる。

診療に用いる場合、緊急に保存情報が必要になる場合を想定しておく必要がある。電気通信回線を経由して外部に保存するということは、極限すれば必ず直ちにアクセスできることを否定することになる。これは地震やテロ等を考えれば容易に想定できるであろう。

従って、万が一の場合でも診療に支障がないようにするためには、代替経路の設定による見読性を確保しておくだけでは不十分である。

継続して診療を行う場合等、直ちにアクセスすることが必要となるような診療録等を外部に保存する場合には、保存する情報の複製またはそれと実質的に同等の内容をもつ情報を、内部に備えておく必要がある。

また、保存していた情報が毀損した場合等は、保存を受託した機関は速やかに情報の復旧を図らなくてはならない。その際には、「8.1.4 責任の明確化」を参考にしつつ予め責任を明確化しておき、患者情報の確保を第一優先とし、委託機関と受託機関の間で責任の所在、金銭面でのトラブル等が生じないように配慮しておく必要もある。

診療終了後しばらくの間来院が見込まれない患者に係る診療録等、緊急に診療上の必要が生じるとまではいえない情報についても、監査等において提示を求められるケースも想定されることから、できる限りバックアップや可搬型媒体による搬送経路の確保等、ネットワーク障害や外部保存の受託先の機関の事故等による障害に対する措置を行っておくこ

とが望ましい。

保存性については診療録等を転送している途中にシステムが停止したり、障害があつて正しいデータが保存されない場合は、再度、外部保存の委託元の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、外部保存の委託元の医療機関等におけるデータを消去する等の場合には、外部保存の受託先の機関において、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

(1) 電気通信回線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 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の受託先の機関と外部保存の委託元の医療機関等が、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 電気通信回線上で「改ざん」されていないことを保証すること

電気通信回線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除き、リモートログインが行なえないように適切に管理されたリモートログインのみ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、「6.10 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. 医療機関等における留意事項」を参照されたい。

(2) 電気通信回線や外部保存を受託する機関の障害等による見読性の確保

① 緊急に必要なことが予測される診療録等の見読性の確保

緊急に必要なことが予測される診療録等は、内部に保存するか、外部に保存し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。

(3) 電気通信回線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

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

外部保存の受託先の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、委託元の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、外部保存の受託先の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に対応を維持しなくてはならない。
- ③ **電気通信回線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**

電気通信回線や受託先の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

- (1) **電気通信回線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 **診療録等を転送する際にメッセージ認証機能を用いること**

通信時の改ざんをより確実に防止するために、一連の業務手続内容を電子的に保証、証明することが望ましい。メッセージ認証機能によりメッセージ内容が確かに本人の送ったものであること、その真正性について公証能力、証憑能力を有するものであることを保証する。

なお、メッセージ認証機能の採用に当たっては保存する情報の同一性、真正性、正当性を厳密に証明するためにハッシュ関数や電子透かし技術等を用いることが望ましい。
- (2) **電気通信回線や外部保存を受託する機関の障害等による見読性の確保**
 - ① **緊急に必要なになるとまではいえない診療録等の見読性の確保**

緊急に必要なになるとまではいえない情報についても、ネットワークや受託先の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。
- (3) **電気通信回線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**
 - 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 電気通信回線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、受託先の機関は、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證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。

8.1.2 外部保存を受託する機関の限定

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つては、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については、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

オンラインによる医療機関等以外の場所での外部保存については、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、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。

一方、患者等の情報が瞬時に大量に漏洩する危険性がある一方で、漏洩した場所や責任者の特定の困難性が増し、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こと、また、一層の情報改ざん防止等の措置の必要性の高まり（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）により、医療機関等の責任が相対的に大きくなる。さらには、蓄積された情報の外部保存を受託する機関等が、不当に利用することへの国民等の危惧が存在する。

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は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るとともに、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員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ところである。

従って、診療録等のオンラインによる医療機関等以外の場所での外部保存については、

法令上の保存義務を有する保存主体の医療機関等が、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、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な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を前提とするべきことから、下記のとおり外部保存を受託できる機関を限定しているところである。また、国民等の危惧に配慮し、特に以下の「C. 最低限のガイドライン」で定める、「③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「④医療機関等が震災対策等の危機管理上の目的で確保した安全な場所」に該当し、外部保存を受託する機関は、保存と利活用を明確に分離した上で、電子化された医療情報等を預かる形態での保存のみ実施可能としている。

一方、診療録等は、患者への診療の用に供したり、公衆衛生の目的において利活用されたりするべきものであるため、法令上の保存義務を有する医療機関等自らが、保存した情報を個人情報保護に十分留意しながら利活用することを妨げるものではない。

C. 最低限のガイドライン

① 病院、診療所に保存する場合

外部保存を受託する機関は、病院や診療所の内部で診療録等を保存する必要があるが、病院や診療所の敷地外に保存することはできない。

② 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の管理者が共同責任で管理する場所等がある。当該場所については、医療法に基づき医療機関としての届け出がなされていたり、医師会立の病院に併置されていたりする等の場合は、本項の①に位置づけてよい。一方、個別の医療法人ないしは医療機関等が、危機管理上の目的等で外部保存を行おうとする場合は、保存主体である医療機関等の責任を明確化し安全管理措置を具体的に示した本項の④に従うこと。

③ 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

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だけでなく、下記の情報管理体制の確保のための全ての要件を満たしつつ、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。

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) 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、原則として保存主体の医療機関等のみがデータ内容を閲覧できることを技術的に担保できること。例えば、外部保存受託機関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、あるいは受託機関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。
- ウ) イ) を含め、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。

④ 医療機関等が震災対策等の危機管理上の目的で確保した安全な場所

法令上の保存義務を有する保存主体の医療機関等が、震災対策等の危機管理上の目的で、本章の他の項の要求事項だけでなく、下記の全ての要件を満たしながらネットワーク経由の外部保存を行う場合の医療機関等以外の場所が該当する。

- (ア) 医療機関等が、保存に係る情報処理機器を自らの所有物として保持し、電気通信回線の確保や管理を保存主体である医療機関等の責任で行えること。また、診療録等の保存された情報に係る責任を自ら担保でき、電子保存のための医療機関等以外の場所を電源設備等を含めて自ら確保するか、または、適切な利用形態で借り受けて行う保存形態であること
- (イ) 保存主体の医療機関等のみが保存情報にアクセス（保存情報の変更・修正・参照等）できることを診療録等の保存された情報の暗号化等の措置により技術的に担保できること。
- (ウ) 安全な場所を提供または管理する外部保存受託機関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、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定期的に受ける等により確認されていること。ただし、民間企業が外部保存受託機関である場合はプライバシーマーク制度等の公正な第三者の認定を受けていること。
- (エ) 外部保存受託機関に対して、医療情報等の守秘に関連した事項及び保存性確保のための電源管理等の厳格なルールを委託契約書等で管理者や電子保存作業従事者等のペナルティを含めて設定していること。

D. 推奨されるガイドライン

「②医療法人等が適切に管理する場所に保存する場合」の場合、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も推奨される。

なお、「③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。

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いる。しかし、電気通信回線を通じて外部に保存する場合、委託元の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、外部保存の受託先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。

電気通信回線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る。秘匿性に関しては「6.10 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・3. 選択すべきネットワークのセキュリティの考え方」でも触れた通り、専用線等であっても十分な注意を払う必要がある。従って、電気通信回線を通過する際の個人情報の保護を担保するためには、適切な暗号化は不可欠である。

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機関間の起点・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委託元の医療機関等と受託先の機関を確実

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、ネットワーク回線における留意事項等の具体的な要件については、「6.10 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-2. 医療機関等における留意事項」および「B-3. 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を受託する機関内での個人情報保護

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機関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受託先の施設に送られ、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。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。