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。

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などの管理面のリスク、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窃視等による機密漏洩のリスクなどである。

これについては「6.9　情報および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。

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

診療情報等の開示が進む中、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、もしくは医療機関内の診療情報等を閲覧す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情報のやり取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。そのため、ここでその際の考え方について触れる。

ただし、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に保存し、受託する事業者が独自に情報提供を行うことはあってはならない。

削除: その委託

削除: 先

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ではなく、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、一般的にはオープンネットワーク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、オープンネットワーク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 に係わ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。
   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、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、拠点の出入り口・使用機器・使用機器上の機能単位・利用者の必要な単位で、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など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「6.5 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係わる操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結果責任の明確化。
     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。

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 および 4 を満たしていることを確認すること。
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。

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」（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. 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）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、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。

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. タイプスタンプは、「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。

7　電子保存の要求事項について

7.1　真正性の確保について

A. 制度上の要求事項

保存義務のある情報の真正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）

「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

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。

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、技術面の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、両者のバランスが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、ネットワークを通じて外部に保存を行う場合、第三者が診療録等の外部保存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、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。

削除: の受託先の

削除: 機関

削除: 外部保存の委託元の

B-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

保存義務のある情報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、その内容が改ざん、消去されたり、過失による誤入力、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、消去しようとするもの）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、入力者に起因するものと、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、入力者が何らかの理由により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、成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
3. 作成責任者が行う作業については作業手順書を作成すること
4. 作業手順書に基づき作業が実施されること
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、どん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、保存された情報は法律・規則等で定められた保存期間に基づいて運用規定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。従って、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と言える。

そのため、入力ミス等は必ず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。

(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、ソフトバグ、バージョン不整合等）
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

これらの脅威は保存された情報を保護するとともに、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維持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。

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、その記録の元となった行為毎に作成責任者が明確になっている必要がある。また、一旦記述された情報を追記・書き換え・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、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記録を残した運用を実施すること。

作成責任者と情報の例を以下に示す。

例1)　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

例2） 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
作成責任者 ：実際に処置を行った看護師

例3） 読影担当医が放射線画像の読影レポートを作成する。
情報 ：読影レポート
作成責任者 ：読影を行った放射線科医師

例4） 検査技師が検査ラインから出力された検査結果のバリデーションを実施し、システムに取り込む。
情報 ：検査結果
作成責任者 ：バリデーションと取り込み操作を行った検査技師

例5） 夜間等で当直医が主担当医の電話での指示により、指定された薬剤のオーダ入力を行った。
情報 ：投薬指示
作成責任者 ：実際にオーダを実施した当直医

これらの記述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記述が物理的に不可能であって、代行者による記述が必要となる場合も想定される。

医療機関等がこのようなケースを組織のポリシとして容認するのであれば、実施にあたっては、任意の医療に関する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明確になっていなければならない。

例6） 夜間等で当直看護師が主担当医の電話での指示により、指定された薬剤のオーダ入力を行った。
情報 ：投薬指示
作成責任者 ：電話で投薬を指示した主担当医
代行者 ：当直看護師

以上のような状況を勘案し、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、必ず入力を行う必要のある個人毎に 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。

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」が行われる事。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・何時・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。

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。

（2－1） 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
（2－2） デジタルカメラ等の外部機器から患者を識別する情報を含まない画像情報（患部の写真等）を取り込み記録する場合
（2－3） 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

（2－1） 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。

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確定として扱う運用においても、本手順に準拠することが必要である。

① 作成責任者自身が入力する場合の確定操作

1 回の入力操作が終了したところで確定操作を行う必要がある。ここであえて 1 回と称しているのは、複数の患者の診療を連続して行った場合でも、確定操作は入力した内容が確実に確認できる 1 患者単位で行うことが必要であることを示している。

② 入力者と作成責任者が異なる場合の確定操作

情報入力は作成責任者が行うことが原則であるが、先に述べたように運用上、代行者による入力が必要になる場合がある。代行者が入力を行った際には、代行者の氏名等の識別情報が記録されることが望ましい。

また、作成責任者はできるだけ速やかに記録内容を確認し確定操作を行うこと。代行者による確定操作は行ってはならない。

③ 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確定操作

複数の作成者が関与する記録については、責任を持つ記録及び記録の範囲を明確にしなければならない。

④ 記録の作成責任者や代行入力者自身が紙に記載したシェーマ図等をスキャナやデジタルカメラ等で電子化して作成する場合の確定操作

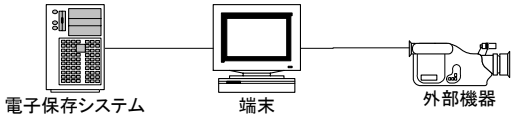
外部機器から送信される記録情報等を一旦電子保存システムの端末に格納し、受信情報の内容の確認と患者属性の付与（必要に応じて）、確認を行い、電子保存システムへ送信し格納する。

この際の記録の確定は、端末での内容確認時点であり、作成責任者が端末で内容を確認する必要がある。

（2－2） デジタルカメラ等の外部機器から患者を識別する情報を含まない画像情報（患部の写真等）を取り込み記録する場合

デジカメ等を電子保存システムの認証機能が動作する端末に接続し、患部の写真、手書きのシェーマ等（取り込む画像情報は医師の直接診断のもととなり、かつ画像情報自体に患者を識別する情報が付属していない）を診療録等の一部として保存する場合は、記録の作成者自身が外部機器から取り込んだ画像情報等を確認し、診療録等として確定する必要がある。

これをユースケースとして示すと次のようになる。



【ケース概要】

外部機器を電子保存システムの認証機能が動作する端末を経由して電子保存システムへ患部の写真等を医療情報の一部として格納するケース。

【入力手順】

外部機器から送信される医療情報等を一旦電子保存システムの端末に格納し、受信情報の内容の確認と患者属性の付与（必要に応じて）、確認を行い、電子保存システムへ送信し格納する。

【記録の確定】

この際の記録の確定は、端末での内容確認時点であり、作成責任者が端末で内容を確認する必要がある。

【基本要件】

- 端末での操作者認証は、電子保存システムの操作者認証機能を用いること。
- 電子保存システムでの確定操作後は､外部機器からの操作で保存データが変更されないこと。

【外部機器例】

具体的な外部機器としては、デジカメ、眼底カメラ、緊急検査装置等が想定される。

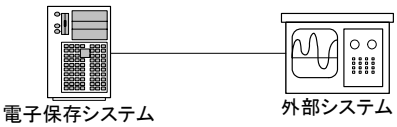
（2－3） 外部システムで確定された情報を取り込み記録する場合

看護支援システム、臨床検査部門、放射線部門等、どの記録が・いつ・誰によって作成されたかが明確に記載され、記録の確定がなされている部門のシステムから別の電子保存システムへ医療情報等を引用登録する場合は、受取る側の電子保存システム側では特に記録の確定を行う必要はない。

この際の記録の作成責任者は外部システムで情報の確定操作を行った者となる。外部システムに電子保存システムと同等な操作者認証が必要とされるが、技術と運用の組み合わせにより実現すること。

なお、外部システム側で記録を再作成・再送信する運用あるいは、電子保存システム側でデータ修正する運用が存在する場合は、確定のタイミングについて運用管理規程に明記する必要がある。

これをユースケースとして示すと次のようになる。



【ケース概要】

確定機能を持つ外部システムから電子保存システムへ医療情報等を引用登録するケース。

【入力手順】

1. 外部システム側から電子保存システムにデータが送られ、そのまま確定する。
2. 外部システム側で再検査が行われ、再送信され、確定版とされる。
3. 電子保存システム側でデータ修正が行われ、確定版とされる。

【記録の確定】

上記、1、2、3 等の運用を外部システムごとに分析し、確定タイミングを決定すること。（たとえば、1 のみであるとか、2、3 は初期送信後の一定時間以内に限定する等）

【基本要件】

- 外部システムは、電子保存システムと同等な操作者認証機能を技術、運用の組み合わせで実現できていること。
- 外部システムが電子保存システムと同等の操作者認証機能を技術的には有してない場合、データの確定時に確定操作者情報を入力する。この際の確定者は、確定操作時に入力した確定操作者となる。なお、外部システム側で責任者がデータの点検を行う等、真正性を確保する運用を行う必要がある。

・外部システムで作成した医療情報等に確定後に訂正（追記、変更、削除）が発生したときは、訂正情報を電子保存システムへ送信し、電子保存システム側では更新履歴（追記、変更、削除）を保持できること。
・電子保存システムでの確定後は、外部システムからの操作で保存データが変更されないこと。

【外部システム例】

具体的な外部システムとしては、看護支援システム、臨床検査機器、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)等が想定される。

(3) 識別情報の記録

確定された記録は、第三者から見て、いつ・誰が作成したものかが、明確になっている必要がある。作成責任者の識別情報には、氏名、及び作成された時刻を含む事が必要であり、また、作成責任者の識別情報が記録情報に関連付けられ、通常の手段では誤った関連付けができないことやその関連付けの分離・変更・改ざんができないことが保証されている必要がある。

識別情報は、作成者が責任を持つ個別の行為毎に個々の患者の診療録等に対して記録または記載されることを原則とする。初回の診療録等の作成時に作成責任者の識別情報が必要であるが、確定され保存された後の追記、修正、削除等を行う場合も、該当する診療録等に対してその作成責任者の識別情報が必要である。

また、グループ診療、及びグループ看護においても、作成責任者は個人とし、複数責任者が存在する場合は複数の個人を責任者として記録する。

(4) 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。このように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識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は、それが検証可能な環境で保存しなければならない。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。

1. 電子保存システムへの厳格なアクセスコントロールを実施すると共に、システム上、確定操作後の修正には、必ず変更履歴を残し、履歴が残らない記録の修正がシステム上防止されていること。また、不正な改ざん等を防止するため、セキュリティに充分注意をはらってシステム運用がなされ、技術と運用両面で対策を実

施する方法。

2. 診療録等の確定部分に対してハッシュ値等の数学的手法で内容変更が検出できる方法を用い、記録そのものとその方法により得た値、そしてそれらへ信頼できる時間源を用いたタイムスタンプ署名を行う方法。
3. 記録の確定時に作成責任者の電子署名及び、信頼できる時刻源を用いたタイムスタンプを付す方法。

また、一旦確定操作が行われた診療録等に対し更新を行った場合には、更新履歴（更新前の情報と更新後の情報が明確に識別できるもの）が保存され、必要に応じて、更新後の情報と更新前の情報が対応付けて参照できる必要がある。例えば次のような方法が考えられる。

1. 診療録等の確定範囲が明示的であり、その範囲に対して確定操作後に更新があった場合には、発見しやすい場所にその旨の表示を行う。変更内容を確認したい場合には、更新（確定）前の診療録等を画面に呼び出し、目視的に変更場所を確認する。
2. 個々の診療録等に対し更新を行う際には、更新前の記録を単純に消すのではなく、取消線等で明示的に削除部分を示し、あわせて追加部分も明示的に表示できるようにする。
3. 上記の想定のような文章上の変更以外にも、検査機器データ（放射線画像、病理画像、波形等）のように複雑な表現を持つものの変更も発生する。この場合は、変更履歴がたどれる機能を持つこと。

C. 最低限のガイドライン

【医療機関等に保存する場合】

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られる。システムの運用は、組織の責任者によって定められた運用管理規程に従って行われるものとし、本要件については下記の内容が記載され、遵守されることが必要である。また、システムが最低限備えているべき機能についても合わせて記述する。

（1） 作成者の識別及び認証

（1） 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. 利用者に 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、本人しか持ち得ない、または知り得ないように運用を定めること。システムは発行された ID、パスワード等による本人認証、識別機能を有すること。ただし、運用

により確実に担保される場合は除く。

2. 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、そのデバイス単独で有効にならないようにし、必ずユーザ ID やパスワードと組み合わせた識別、認証を行うこと。
3. 本人認証、識別に指紋、虹彩等のバイオメトリクスを利用する場合は、1 対 1 の照合となるよう、必ずユーザ ID やパスワードと組み合わせた識別、認証を行うこと。
4. 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。
5. 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。
6. 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、ネットワーク接続端末のアクセス制限等のセキュリティ対策を実施すること。

（2） 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

装置の管理責任者や操作者が運営管理規程で明文化され、管理責任者、操作者以外の機器の操作が運営上防止されていること。また、当該装置による記録は、いつ・誰が行ったかがシステム機能と運営の組み合わせ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

（1） 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、システムは確定された情報が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が含まれること。
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を運用も含めて防止でき、それらが検知された場合はバ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こと。
4. 外部から入力された情報を「参照」する場合、その情報は本ガイドラインに従って正しく保存された確定記録でなければならない。参照元の情報が「保存された記録」でない場合は、コピー等の移動手段を経て取り込み操作を行った後に、その情報も含めた「記録の確定」が行われなければならない。

(2)　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

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)、信頼できる時間源を用いた作成日時が記録に含まれること。

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を運用も含めて防止でき、それらが検知された場合はバ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. 更新履歴の参照（照らし合せ）は、更新前後の情報が各々物理的に独立して保存されているものの様に更新の順序に沿って参照する方法か、更新時の変更点を明示するような方法（消し込み線を表示するように）で参照できること。
3. 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. アクセスログの記録を残し、そのログが改ざんされない対策を講じ、万が一、記録情報の改ざん・削除が起こった場合にはその事実を検証可能とすること。

(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、具体的にどの医療に関する業務等（プロシジャ）に適用するか、また誰が誰を代行してよいかを定義すること。
2. 代行操作を認める医療に関する業務等がある場合は、その代行操作者自身も予め電子保存システムの運用操作に携わる者として当該システムに識別管理情報を登録すること。
3. 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。
4. 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)」が行われること。このため、代行入力により記録された情報及びその管理情報は必要な都度参照ができるとともに、一定の期間内に確定操作が行われるように督促機能が組織のルールとして整備されていること。
5. 一定時間後に記録が自動確定するような運用の場合は、作成責任者を特定する明確なルールを策定し運用規程に明記すること。

(5) 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

1. 診療録等を共同して作成するケースが運用上あれば、具体的にどの医療に関する業務等に適用するか定義すること。また、それぞれを分担する役割者（ロール）を具体的な職種や所属部署等を用いて定義すること。
2. それぞれの役割者による記述を（4）で定義された方法で代行するケースがあれば、それを分担する役割者を医療に関する業務等ごとに定義すること。
3. 記述の分担単位に確定操作が行えるようになっており、それぞれの記述者の識別管理情報が記録されること。

（6）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規定されていること。
3. 運用管理規程で決められた内容を遵守するために、従業者等への教育を実施すること。
4. 内部監査を定期的に実施すること。

（7）ルールの遵守

1. 運用管理規程で決められた内容を遵守するためには、従業者等の教育とルールの徹底が重要である。教育とルールの遵守状況について常に状況を把握すること。
2. ルールの改訂や新たな従業者等の登用の際には、教育を実施すること。
3. ルールの遵守状況に関する内部監査を、定期的に（少なくとも半年に 1 度）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）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。

削除: の

削除: 受託

削除: 委託先の機関

削除: 事業者

削除: 外部保存の委託元の

（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、「6.11　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　B-2．医療機関等における留意事項」を参照されたい。

削除: 0

D．推奨されるガイドライン

【医療機関等に保存する場合】

「C．最低限のガイドライン」に記述した内容は文字通り最低限の方策であり、電子保存システムにおける一般的かつ典型的な脅威に対抗したものであるに過ぎない。患者の安全確保や個人情報保護に重大な責任を持つ医療機関等にとっては、さらなるセキュリティ面の強化や、電子化された情報の証拠性をより担保できる高度な対策を施すことが望ましい。

高度な対策とは昨今の向上が著しい技術的な対策が主であり、ここでは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や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にかかわらず、下記の機能をシステム自体が備えていることを推奨する。

なお、セキュリティやセキュリティ管理の技術は日進月歩であり、ここで推奨したものも数年のうちには（場合によっては数ヶ月で）陳腐化する可能性を考慮しなければならない。もちろんその場合には本ガイドラインの改定が必要であろうことは言うまでもないが、もとよりシステムを運用管理する医療機関等にも、それらへの対応の責務があることを認識されたい。

（1） 作成・記録責任者の識別及び認証

1. 記録の作成入力に関与する利用者識別・認証用に電子証明書を発行し、本人しか持ち得ないよう私有鍵を IC カード等のセキュリティ・デバイスに格納する。
2. 本人が私有鍵を活性化する際にはパスワードや生体認証等の認証情報を用い、その認証情報が暗号化されずにネットワークへ流れることのないような手段を用いること。また、電子証明書をシステムへの認証用に用いる際は少なくとも端末へのログオン毎に、電子署名用に用いる際には署名毎に私有鍵の活性化を求めること。
3. 利用者の権限範囲に応じた適切なアクセスコントロール機能を有すること。
4. 情報システムにリモートアクセスする場合には、VPN 等、通信経路の暗号化を実施するとともに IC カード、電子証明書とパスワード等、2 つ以上の要素から

なる認証方式により利用者の識別、認証を求めること。

(2) 情報の確定手順の確立と、作成・記録責任の識別情報の記録

1. 「記録の確定」に際し、作成者責任者の電子署名を行うこと。また、確定操作がいつ行われたかを担保するために、確定操作後速やかに信頼できる時刻源を用いたタイムスタンプ署名を行うこと。
2. 「記録の確定」に際し、その作成責任者の識別情報が電子署名により記録情報に関連付けられること。この際、署名は IC カード等のセキュアなトークン内で行われるか、利用者の端末内で行われる場合は署名後に私有鍵の情報が一切残らない方式を用いること。
3. 電子署名は保存が義務づけられた期間より長期にわたり署名時点での証明書及び署名の有効性が確認できること。
4. 「確定操作」を行うにあたり、責任者による内容の十分な確認が行われたことを確認する手続きを義務づけること。

(3) 更新履歴の保存

1. 一旦確定された情報は、後からの追記・書き換え・消去等の事実を正しく確認できるよう、当該事項の履歴が保存され、その内容を容易に確認できること。追記・書き換え・消去等の確定操作を行う際には当該部分の変更履歴を含んだ電子署名をおこなうこと。

(4) 代行操作の承認機能（代行操作が運用上に必要な場合のみ）

1. 代行操作を認めるかどうかを医療に関する業務等（プロシジャ）ごとに定義しうること。
2. 操作者の役割（ロール）を定義し、上記で定義したプロシジャに対して適用可否を判断できること。
3. 代行操作が行われたプロシジャに対し、その承認者（作成責任者）による承認操作が行えること。また、その承認操作が督促されること。

(5) 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

1. 1 つの診療録等に対し、複数の入力者による署名をサポートすること。この場合、1 つの情報単位に対して複数の署名を付与する実装でもよいし、情報を分担ごとの複数のセクションに分けて、それぞれを独立した情報として別々に署名を付与してもよい。しかし、後者の場合には情報間の関連性が失われないように配慮すること。
2. 共同作業における情報入力のワークフローが管理でき、そのワークフローに沿っ

た制御が可能であること。

3. ワークフローに沿ったログが記録されること。

(6) システムの改造や保守等で診療録等に触れる場合の管理

1. 運用管理規程を整備し、定期的に監査すること。
2. アクセスログを定期的に監査すること。

(7) 機器・ソフトウェアの品質管理

1. システムを構成するソフトウェアの構成管理を行い、不正な変更が検知できること。また検知された場合は、バックアップ等を用いて原状回復できること。

(8) 誤入力の防止

1. 過失は起こるものとの発想で、ヒヤリ・ハット事例等をもとに、誤入力防止のシステム的対策を施すこと。
2. 誤入力の発生状況を監察し、誤入力防止の対策が有効かどうか定期的に評価し、不十分な場合は、誤入力防止の仕組み及び方法を是正すること。(オーダ画面の薬剤配置、色分け、限度量・限度回数チェック､禁忌チェック、リストバンドによる本人チェック等)

(9) ルールの遵守

1. 運用管理規程に書かれたルールは確実に遂行されることが必要であり、確実を期すための内部監査を効果的に実施することは必須である。これを医療機関等の内部で適切かつ効果的に遂行することが期待できない場合は、第三者に委託することを考慮すべきである。
2. 組織内での運用プロセスが標準に準拠されたもの（ISO9000、ISMS 等）に沿って構築されていることを、必須ではないが強く推奨する。

【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) 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。

7.2　見読性の確保について

A. 制度上の要求事項

保存義務のある情報の見読性が確保されていること。
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 4 項第一号）

「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

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。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。特に監査の場合においては、監査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ている。

電子媒体に保存された情報は、そのままでは見読できず、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、それを防ぐためのシステム全般の保護対策が必要であるが、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が必要である。

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、必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、ネットワークを通じて外部に保存する場合は、厳密な意味で見読性の確保を著しく難しくするように見える。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。」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、診療上緊急に必要になる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。ネットワーク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、保存を受託する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、「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、患者情報の確保を第一優先とし、委託する医療機関等と受託する機関との間で責任の所在、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を受託する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。

削除: 受託
削除: 委託
削除: した
削除: は
削除: に
削除: せ
削除: 委託先の機関
削除: 機関
削除: 事業者
削除: 型
削除: の
削除: 受託
削除: 委託先の機関
削除: 事業者

C. 最低限のガイドライン

【医療機関等に保存する場合】

電子媒体に保存された全ての医療情報等が、見読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見読可能であることと、システム障害においてもバックアップシステム等により診療に致命的な支障が起きない水準で見読出来ることが必要である。

(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とスループット

1. **診療目的**
   ① 外来診療部門においては、患者の前回の診療録等が当日の診療に支障のない時間内に検索表示もしくは書面に表示できること。
   ② 入院診療部門においては、入院中の患者の診療録等が当日の診療に支障のない時間内に検索表示もしくは書面に表示できること。

2. **患者への説明**
   ① 患者への説明が生じた時点で速やかに検索表示もしくは書面に表示できること。なお、この場合の“速やかに”とは、数分以内である。

3. **監査**
   ① 監査当日に指定された患者の診療録等を監査に支障のない時間内に検索表示もしくは書面に表示できること。

4. **訴訟等**
   ① 所定の機関より指定された日までに、患者の診療録等を書面に表示できること。
   ② 保存場所が複数ある場合、各保存場所毎に見読手段を用意し、その操作方法を明示すること。

(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手段を用意すること。

(5) システム障害対策としてのバックアップデータの保存

システムの永久ないし長時間障害対策として、日々バックアップデータを採取すること。

【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) 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。

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。

削除: 受託

削除: 委託先の

削除: 事業者

削除: 機関

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。

削除: 外部保存の委託元の

削除: 外部保存の委託元の

削除: の

削除: 受託

削除: 委託先の機関

削除: 事業者

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。

削除: の
削除: 委託する先機関
削除: 事業者
削除: の
削除: 受託先の
削除: 委託先の機関
削除: 事業者
削除: 委託元の
削除: の
削除: 受託
削除: 委託先の
削除: 先の
削除: 機関
削除: 事業者
削除: の
削除: 委託先する機関
削除: 事業者
削除: わせる
削除: 事業者
削除: 受託
削除: 委託先の機関
削除: わせる

（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。

削除: の
削除: する委託先機関
削除: 事業者
削除: させる
削除: 事業者
削除: 受託
削除: 委託先の機関
削除: に
削除: させる
削除: させる