6.7　情報の破棄

B. 考え方

医療に係る電子情報は運用、保存する場合だけでなく破棄に関しても安全性を確保する必要がある。またデータベースのように情報がお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。

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。

外部の委託機関等に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、受託先の機関等も、委託元の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。

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. 破棄を外部事業者に委託した場合は、「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、さらに委託元の医療機関等が確実に情報の破棄が行な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廃棄を定める規程の作成の方法

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。

また、保守作業によっては保守会社からさらに外部委託業者に修理等を依頼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、再委託先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えておくこと。

5. 保守会社が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. リモート保守によるシステムの改造や保守が行なわれる場合には、必ずメッセージログを採取し、当該作業の終了後速やかにメッセージログの内容を医療機関等の責任者が確認すること。
9. 再委託が行なわれる場合は再委託先にも保守会社と同等の義務を課すこと。

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で表示し、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 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、個人情報保護に関して特に留意すべき項目について述べる。外部と医療情報を交換するケースとしては、検査を外部機関に委託していて、オンラインでデータをやり取りする場合等が考えられる。

医療機関等が法令による義務の有無に係らず、外部と個人情報を含む医療情報を交換し、外部に保存を委託する場合は、情報の不適切な二次利用を防止する等、特段の個人情報保護に関する配慮が必要なため、8 章に別途まとめて記載を行う。

個人情報を電気通信回線により伝送する場合は以下による。

① 秘匿性の確保のための適切な暗号化

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。秘匿性に関しては専用線であっても施設の出入り口等で回線を物理的にモニタすることで破られる可能性があり配慮が必要である。したが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。

② 通信の起点・終点識別のための認証

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機関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。たとえば、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。なお、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。

③ リモートログイン制限機能

個人情報を含む医療情報の保存業務を受託先の機関や委託元の機関のサーバへのリモートログイン機能に制限を設けないで容認すると、ログインのためのパスワードが平文で LAN 回線上を流れたり、ファイル転送プログラム中にパスワードがそのままの形でとりこまれたりすることにより、これが漏洩する可能性がある。

また、認証や改ざん検知の機能をソフトウェアで行っている場合には、関連する暗号鍵が盗まれたり、認証や改ざん検知の機構そのものが破壊されたりするおそれもある。また、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、システムメンテナンスを目的とした遠隔保守のためのアクセスも考えられる。

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。適切に管理されたリモートログイン機能のみに制限しなければならない。

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。

○　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。

○　作成の責任の所在を明確にすること。

（施行通知　第二　２（３）②）

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。

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箇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、ソフトウェアが第三者により（悪意ある）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後に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 5 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

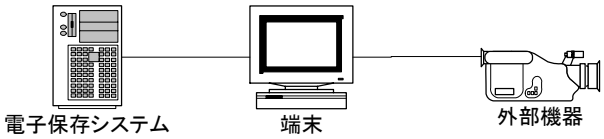
外部機器から送信される記録情報等を一旦電子保存システムの端末に格納し、受信情報の内容の確認と患者属性の付与（必要に応じて)、確認を行い、電子保存システムへ送信し格納する。

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。

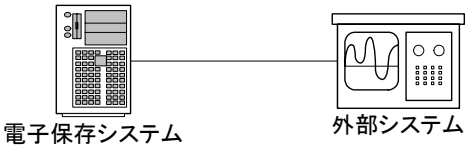
(2－3)　外部システムで確定された情報を取り込み記録する場合

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

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

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. 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外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。

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

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

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。

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

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。

D. 推奨されるガイドライン

「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訂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。

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。

○　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。

○　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　第二　２（３）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。

C. 最低限のガイドライン

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プ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。

D. 推奨されるガイドライン

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) バップアップサーバ

システムが停止した場合でも、バップ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。

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。

○　法令に定める保存期間内、復元可能な状態で保存すること。

（施行通知　第二　２（３）③）

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。

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。

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充分な知識を結集して推進して行くことが求められる。