

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

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。

削除: 型

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「6.10 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。

削除: 型

削除: 型

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十分な知識を結集して推進して行くことが求められる。

削除: の委託先

削除: を受託する

削除: 機関

削除: において

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

削除: 受託

A. 制度上の要求事項

削除: 委託

- 「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

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增大する。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へ委託されており、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。

削除: 委託した

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

削除: の委託を受ける

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

削除: 情報保存機関

削除: 委託元である

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、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ってはならないことは当然である。

仮に保存された情報の分析等をしようとする場合、目的は公衆衛生の向上等、公益に資するものを対象にし、委託した病院、診療所、患者の同意を得て実施しなくてはならないものである。

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

削除: された

削除: の

削除: を委託元の

削除: を依頼

削除: 元の

削除: を依頼

削除: 元の

削除: を依頼

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揭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。

削除: 受託

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。

削除: 受託

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は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。

削除: 受託

削除: 受託

削除: 機関

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つてはならず、許されない。

削除: 受託

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。

削除: 受託

削除: の委託元

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は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。

削除: 受託

削除: 外部保存

削除: 受託

削除: 機関

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。

削除: 委託元である

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。

削除: 受託

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は、暗号鍵の使用について厳重な管理が必要である。

削除: 受託

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定の策定、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。

削除: 受託

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ている病院、診療所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らないように配慮しなくてはならない。

削除: の委託を受けている

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ている病院、診療所が何らの同意も得ずに実施してはならない。

削除: の委託を受けている

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

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。

削除: 受託

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と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らないようにしなくてはならない。

削除: 受託

削除: 受託

削除: も委託されて

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

削除: 委託先機関

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。

削除: 受託

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土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。

削除: 受託

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らないようにしなくてはならない。

削除: 受託

削除: も委託されて

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。

削除: 受託

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) 保存された診療録等を委託元の病院、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) 保存された情報の分析等をしようとする場合、目的は公衆衛生の向上等、公益に資するものを対象にし、委託元の病院、診療所、患者の同意を得て実施すること。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実施すること。
- (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ている病院、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。

削除: 委託されている

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

- (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。

削除: 受託

削除: 受託

削除: 受託

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。

削除: 受託

削除: 外部保存

削除: 受託

削除: 事業者

削除: 受託

削除: 受託

削除: 受託

削除: 受託

削除: 受託

削除: 受託

(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らないようにさせること。

削除: 受託

削除: 受託

(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。

削除: 受託

- (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。

削除: 保存主体の

(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。

削除: 受託

削除: 外部保存事業者

削除: 受託機関

書式変更: 左揃え、なし、改ページ時1行残して段落を区切らない

8.1.3 個人情報の保護

削除:

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。

削除: 委託元の

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。

削除: の

削除: 委託先機関

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「6.1 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。

削除: 0

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。

削除: 受託する機関

削除: 外部保存事業者

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。

削除: 委託元の

削除: 外部保存事業者

削除: 受託先の機関

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、「6.1.1 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。

削除: 0

(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

削除: 機関

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。

削除: 委託する先の機関

「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。

削除: 受託先

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でない場合

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「6.10 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型媒体に保存する場合には、「付則 1 電子媒体による外部保存を可搬型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: 受託先の機関

削除: 外部保存事業者

8.2 電子媒体による外部保存を可搬型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、「4 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、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ければならない。

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、医療機関等の自己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。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〇〇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ければならない。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。

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契約書等にも明記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。

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、そのことに十分なこと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、電気通信回線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ければならない。

- 削除: 委託側の
- 削除: 受託側の機関
- 削除: 外部保存事業者

- 削除: 受託先の機関
- 削除: 外部保存事業者
- 削除: 受託先の機関
- 削除: 外部保存事業者
- 削除: 委託先の
- 削除: 委託先の
- 削除: 委託側と受託側で取り交わす
- 削除: 委託先、受託先
- 削除: 厳正な取扱いを

- 削除: 外部保存事業者
- 削除: 委託側、受託側

8.4.3 保存義務のない診療録等の外部保存について

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。

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

<注意>

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保存・運用されたのちに、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。電子カルテ等へシエーマを入力する際に、紙に描画し、スキャナやデジタルカメラ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。

9.1 共通の要件

A. 制度上の要求事項

- (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
- (2) 改ざんを防止すること
- (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、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
- (4) スキャナにより読み取った情報が、法令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
- (5) 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))

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、紙やフィルムによる媒体がやむを得ない事情で生じる場合。
- (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の媒体で残り、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での運用であって、紙等の媒体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。

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らない。従って、いったん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、可能であれば外部への保存も含めて検討されるべきであろう。このような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が、紙等の媒体もそのまま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。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、300dpi、RGB 各色 8 ビット (24 ビット) 以上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 1.1 版 (平成 14 年 6 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。一般的に極めて精細な精度が必要なもの以外は 300dpi、24 ビットのカラーで十分と考えられるが、あくまでも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 TIFF 形式または PDF 形式で保存することが望ましい。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
- ・ 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の同一性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等を遅滞なく行い、責任を明確にすること。

なお、電子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。

- ・ 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。

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. 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。
4. 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
5. 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棄する場合、シュレッダー等で個人識別不可能な状態にしたうえで破棄しなければならない（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、及び本指針第 6 章参照）。

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

A. 制度上の要求事項

- (1) 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) ②、(3))

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やむを得ない事情で生じる場合で、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おこな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機会が生じない程度の期間で、通常は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。

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

A. 制度上の要求事項

- (1) 個人情報保護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あらかじめ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。
- (2) 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。
- (3) 外部事業者へ委託する場合には、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))

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。要点は「9.1 共通の要件」の要求をすべて満たした上で、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. 電子化をおこなう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おこなう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おこなわないこと。
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おこなうこと（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おこなってから紙やフィルムを破棄するまでの期間、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をおこなう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おこなうこと。
 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おこなうことを具体的に明記すること。

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が、紙等の媒体もそのまま保存をおこなう場合

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おこなう必要があり、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、原則として 300dpi、RGB 各色 8 ビット（24 ビット）以上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 1.1 版（平成 14 年 6 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。一般的に極めて精細な精度が必要なもの以外は 300dpi、24 ビットのカラーで十分と考えられるが、あくまでも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 TIFF 形式または PDF 形式で保存することが望ましい。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. 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。特に電子化後のもとの紙媒体やフィルムの安全管理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きわめて重要であり、運用管理規程は必ず定めなければならない。

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

運用管理規程には、システムの導入に際して、「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基準」や「診療録等の外部保存を行う際の基準」を満足するために技術的に対応するか、運用によって対応するかを判定し、その内容を公開可能な状態で保存する旨を盛り込まなければならない。

医療機関等には規模、業務内容等に応じて様々な形態があり、運用管理規程もそれに伴い様々な様式・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、そして終わり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」に記載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
- b) 対象情報

② 管理体制

- a) システム管理者、機器管理者、運用責任者の任命
- b) 作業担当者の限定
- c) マニュアル・契約書等の文書の管理
- d) 監査体制と監査責任者の任命
- e) 苦情の受け付け窓口の設置
- f) 事故対策
- g) 利用者への周知法

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」～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
- c) 委託契約における安全管理に関する条項
- d) 個人情報の記録媒体の管理（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) 技術的安全対策事項
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に関する規程
- 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取り扱い規程、日常的運用規程

⑤ 業務委託の安全管理措置

- a) 業務委託契約における守秘条項
- 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データ参照
 - ・ 保守要員専用のアカウントの作成及び運用管理
 - ・ 作業時の病院関係者の監督
 - ・ 保守契約における個人情報保護の徹底
 - ・ メッセージログの採取と確認

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) 従業員への周知徹底

- 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) 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
 - e) 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の運用管理規定
 - ・ アクセスを許容する状態
 - ・ ログ取得方法
 - ・ 許容したアクセス状態の保持確認規程
- 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規程
 - c) 非常時の機能と運用規程
 - d) 報告先と内容一覧
- 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) 一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
- f) 機器・ソフトウェアの品質管理

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
 - ・ 診療目的
 - ・ 患者説明
 - ・ 監査
 - ・ 訴訟
- d) システム障害対策
 - ・ 冗長性
 - ・ バックアップ
 - ・ 緊急対応

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

④ 相互利用性確保

- 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

(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」

可搬型媒体による外部保存、紙媒体による外部保存にあたっては、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) 委託に値する事業者と判断した根拠の記載

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。

削除: 機関

削除: 「

- b) 医療機関等における管理責任者

削除: 委託元

- c) 受託事業者への監査体制

削除: での

- d) 受託事業者、回線事業者等との責任分界点

削除: 機関

- 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

削除: 保存業務

- f) 事故等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。

削除: 機関

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。

削除: 機関

削除: 機関

- g) 外部に保存を委託する文書の選定基準

削除: 「

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様な処理法

削除: 先

- 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

削除: 先

削除: 受託先との

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

- c) リモートログイン制限機能

④ 見読性確保

- a) 緊急に必要なことが予測される医療情報の見読性の確保手段

- b) 緊急に必要なこととまではいえない医療情報の見読性の確保手段

* 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

削除: 外部保存事業者

- b) 標準的なデータ形式及び転送プロトコルの採用

削除: を受託する機関

* 上記事項は推奨

- 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

- d) 電気通信回線や外部保存を受託する事業者の設備の劣化対策
- e) 電気通信回線や外部保存を受託する事業者の設備の互換性確保
 - * 上記事項は推奨
- f) 情報保護機能

削除: 機関

削除: 機関

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

削除: 機関

削除: 「

⑧ 患者への説明と同意

- a) 診療開始前の同意
- b) 患者本人の同意を得ることが困難であるが、診療上の緊急性がある場合
- c) 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

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

削除: 機関

削除: への

削除: 機関側

削除: での

(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の同一性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)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
- ④ 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

⑤ 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

<運用管理規程の作成にあたって>

運用管理規程は、電子保存及び外部保存の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。

具体的な作成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、付表の「運用管理項目」、「実施項目」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」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）していかなければならない。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。