医療情報システムの安全管理に関するガイドライン

第２版

平成１９年３月

厚生労働省

改定履歴

版数	日付	内容
第 1 版	平成 17 年 3 月	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」及び、平成 14 年 3 月通知「診療録等の保存を行う場所について」に基づき作成された各ガイドラインを統合。 新規に、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ガイドライン（紙等の媒体による外部保存を含む）、及び医療・介護関連機関における個人情報保護のための情報システム運用管理ガイドラインを含んだガイドラインとして作成。
第 2 版	平成 19 年 3 月	平成 18 年 1 月の高度情報通信技術戦略本部（IT 戦略本部）から発表された「IT 新改革戦略」（平成 18 年 1 月）において、「安全なネットワーク基盤の確立」が掲げられたこと、及び、平成 17 年 9 月に情報セキュリティ政策会議により決定された「重要インフラの情報セキュリティ対策に係わる基本的考え方」において、医療を IT 基盤の重大な障害によりサービスの低下、停止を招いた場合、国民の生活に深刻な影響を及ぼす「重要インフラ」と位置付け、医療における IT 基盤の災害、サイバー攻撃等への対応を体系づけ、明確化することが求められたことを踏まえ、 (1) 医療機関等で用いるのに適したネットワークに関するセキュリティ要件定義について、想定される用途、ネットワーク上に存在する脅威、その脅威への対抗策、普及方策とその課題等、様々な観点から医療に関わる諸機関間を結ぶ際に適したネットワークの要件を定義し、「6.10 章　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」として取りまとめる等の改定を実施。 (2) 自然災害・サイバー攻撃による IT 障害対策等について、医療の IT への依存度等も適切に評価しながら、医療における災害、サイバー攻撃対策に対する指針として「6.9 章　災害等の非常時の対応」を新設して取りまとめる等の改定を実施。

【目次】

1　はじめに 1
2　本指針の読み方 3
3　本ガイドラインの対象システム及び対象情報 5
4　電子情報を扱う医療機関等における責任のあり方 8
5　情報の相互利用性と標準化について 11
5.1　標準的な用語集やコードセットの利用 11
5.2　国際的な標準規格への準拠 12
6　情報システムの基本的な安全管理 13
6.1　方針の制定と公表 13
6.2　医療機関における情報セキュリティマネジメント（ISMS）の実践 14
6.2.1　ISMS 構築の手順 14
6.2.2　取扱い情報の把握 15
6.2.3　リスク分析 16
6.3　組織的安全管理対策（体制、運用管理規程） 19
6.4　物理的安全対策 21
6.5　技術的安全対策 22
6.6　人的安全対策 29
6.7　情報の破棄 31
6.8　情報システムの改造と保守 32
6.9　災害等の非常時の対応 34
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 38
7　電子保存の要求事項について 51
7.1　真正性の確保について 51
7.2　見読性の確保について 66
7.3　保存性の確保について 69
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 73
8　診療録及び診療諸記録を外部に保存する際の基準 75

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 75
8.1.1　電子保存の 3 基準の遵守 76
8.1.2　外部保存を受託する機関の限定 80
8.1.3　個人情報の保護 84
8.1.4　責任の明確化 87
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 90
8.2.1　電子保存の 3 基準の遵守 90
8.2.2　個人情報の保護 93
8.2.3　責任の明確化 96
8.3　紙媒体のままで外部保存を行う場合 98
8.3.1　利用性の確保 98
8.3.2　個人情報の保護 100
8.3.3　責任の明確化 103
8.4　外部保存全般の留意事項について 105
8.4.1　運用管理規程 105
8.4.2　外部保存契約終了時の処理について 106
8.4.3　保存義務のない診療録等の外部保存について 108
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 109
9.1　共通の要件 109
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 112
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 113
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 115
10　運用管理について 117
付表 1　一般管理における運用管理の実施項目例
付表 2　電子保存における運用管理の実施項目例
付表 3　外部保存における運用管理の例

1　はじめに

平成１１年４月の通知「診療録等の電子媒体による保存について」（平成１１年４月２２日付け健政発第 517 号・医薬発第 587 号・保発第 82 号厚生省健康政策局長・医薬安全局長・保険局長連名通知）、平成１４年３月通知「診療録等の保存を行う場所について」（平成１４年３月２９日付け医政発 0329003 号・保発第 0329001 号厚生労働省医政局長・保険局長連名通知）により、診療録等の電子保存及び保存場所に関する要件等が明確化された。その後、情報技術の進歩は目覚しく、社会的にも e-Japan 戦略・計画を始めとする情報化の要請はさらに高まりつつある。平成 16 年 11 月に成立した「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法律」（平成１６年法律第１４９号。以下「e-文書法」という。）によって原則として法令等で作成または保存が義務付けられている書面は電子的に取り扱うことが可能となった。

平成１５年６月より厚生労働省医政局に設置された「医療情報ネットワーク基盤検討会」においては、医療情報の電子化についてその技術的側面及び運用管理上の課題解決や推進のための制度基盤について検討を行い、平成１６年９月最終報告が取りまとめられた。

上記のような情勢に対応するために、これまでの「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ガイドライン」（平成１１年４月２２日付け健政発第 517 号・医薬発第 587 号・保発第 82 号厚生省健康政策局長・医薬安全局長・保険局長連名通知に添付。）、「診療録等の外部保存に関するガイドライン」（平成１４年５月３１日付け医政発第 0531005 号厚生労働省医政局長通知）を見直し、さらに、個人情報保護に資する情報システムの運用管理にかかわる指針と e-文書法への適切な対応を行うための指針を統合的に作成することとした。なお、平成１６年１２月には「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」が公表され、平成１７年４月の「個人情報の保護に関する法律」（平成１５年法律第５７号。以下「個人情報保護法」という。）の全面実施に際しての指針が示されたが、この指針では情報システムの導入及びそれに伴う外部保存を行う場合の取扱いに関しては本ガイドラインで示すとされている。

今回のガイドラインは、病院、診療所、薬局、助産所等（以下「医療機関等」という。）における診療録等の電子保存に係る責任者を対象とし、理解のしやすさを考慮して、現状で選択可能な技術にも具体的に言及した。したがって本ガイドラインは技術的な記載の陳腐化を避けるために定期的に内容を見直す予定である。本ガイドラインを利用する場合は最新の版であることに十分留意されたい。

また、本ガイドラインは「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」と対になるものであるが、個人情報保護は決して情報システムにかかわる対策だけで達成されるものではない。したがって、本ガイドラインを使用する場合、情報システムだけの担当者であっても、「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」を十分理解し、情報システムにかかわらない部分でも個人情報保護に関する対策が達成されていることを確認することが必要である。

改定概要

【第 2 版】

本ガイドライン初版公開（平成 17 年 3 月）後の平成 18 年 1 月、高度情報通信技術戦略本部（IT 戦略本部）から、「IT 新改革戦略」が発表された。IT 新改革戦略では、「e-Japan 戦略」に比べて医療情報の活用が重視されている。様々な医療情報による連携がメリットをもたらすものと謳い、連携の手法、またその要素技術について種々の提言がなされており、そのひとつに「安全なネットワーク基盤の確立」が掲げられている。

他方、平成 17 年 9 月に情報セキュリティ政策会議により決定された「重要インフラの情報セキュリティ対策に係わる基本的考え方」において、医療を IT 基盤の重大な障害によりサービスの低下、停止を招いた場合、国民の生活に深刻な影響を及ぼす「重要インフラ」と位置付け、医療における IT 基盤の災害、サイバー攻撃等への対応を体系づけ、明確化することが求められた。

これらの状況を踏まえ、医療情報ネットワーク基盤検討会では、「(1) 医療機関等で用いるのに適したネットワークに関するセキュリティ要件定義」、「(2) 自然災害・サイバー攻撃による IT 障害対策等」の検討を行い、本ガイドラインの改定を実施した。

「(1) 医療機関等で用いるのに適したネットワークに関するセキュリティ要件定義」では、想定される用途、ネットワーク上に存在する脅威、その脅威への対抗策、普及方策とその課題等、様々な観点から医療に関わる諸機関間を結ぶ際に適したネットワークの要件を定義し、「6.10 章　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」として取りまとめている。さらには、関連個所として「8 章　診療録及び診療諸記録を外部に保存する際の基準」の中のネットワーク関連の要件について 6.10 章を参照すること、医療機関等における当該ネットワークの運用の指針となる「10 章　運用管理について」の一部改定を実施している。

また、「(2) 自然災害・サイバー攻撃による IT 障害対策等」では、医療の IT への依存度等も適切に評価しながら、医療における災害、サイバー攻撃対策に対する指針として「6.9 章　災害等の非常時の対応」を新設して取りまとめ、情報セキュリティを実践的に運用して行くための考え方として「6.2 章　医療機関における情報セキュリティマネージメント（ISMS）の実践」の概念を取り入れ、「10 章　運用管理について」も該当個所の一部追記を行った。

なお、本ガイドライン公開後に発出、改正等がなされた省令・通知等についても制度上の要求事項として置き換えを実施している。基本的要件について変更はないが、制度上要求される法令等が変更されている点に注意されたい。

2　本指針の読み方

本指針は次のような構成になっている。医療機関等の責任者、情報システム管理者、またシステム導入業者が、それぞれ関連する個所を理解した上で、個々の対策を実施することを期待する。

なお、本指針では医療情報、医療情報システムという用語を用いているが、これは患者を対象とする医療に関して、患者情報（個人識別情報）を含む情報及びその情報を扱うシステムという意味で用いている。

【1 章～6 章】

個人情報を含むデータを扱うすべての医療機関等で参照されるべき内容を含んでいる。

【7 章】

保存義務のある診療録等を電子的に保存する場合の指針を含んでいる。

【8 章】

保存義務のある診療録等を医療機関等の外部に保存する場合の指針を含んでいる。

【9 章】

e-文書法に基づいてスキャナ等により電子化して保存する場合の指針を含んでいる。

【10 章】

運用管理規程に関する事項について記載されている。主に電子保存や外部保存を行う場合の運用管理規程の作成に関する指針であるが、電子保存や外部保存を行わない場合でも参考にされたい。

なお、本指針の大部分は法律、厚生労働省通知、他の指針等の要求事項に対して対策を示すことを目的としており、そのような部分ではおおむね、以下の項目にわけて説明をしている。

A.　制度上の要求事項

法律、通知、他の指針等を踏まえた要求事項を記載している。

B.　考え方

要求事項の解説及び原則的な対策について記載している。

C. 最低限のガイドライン

A の要求事項を満たすためにかならず実施しなければならない事項を記載している。

この項にはいくつかの対策の中の一つを選択する場合もあるが、選択を明記している場合以外はすべて実施しなければならない対策である。なお、この項の対策にあっては医療機関等の規模により実際の対策が異なる可能性がある。後述するように付表の運用管理表を活用し、適切な具体的対策を採用されたい。

D. 推奨されるガイドライン

実施しなくても要求事項を満たすことは可能であるが、説明責任の観点から実施したほうが理解が得やすい対策を記載している。

また、最低限のシステムでは使用されていない技術で、その技術を使用する上で一定の留意が必要となる場合についての記載も含んでいる。

なお、巻末の 3 つの付表は安全管理上の要求事項を満たすための技術的対策と運用的対策の関係を要約したもので、運用管理規程の作成に活用されることを期待して作成した。安全管理対策は技術的対策と運用的対策の両面でなされてはじめて有効なものとなるが、技術的対策には複数の選択肢があることが多く、採用した技術的対策に対して、相応した運用的な対策を行う必要がある。付表は以下の項目からなる。

1. **運用管理項目**：安全管理上の要求事項で多少とも運用的対策が必要な項目
2. **実施項目**：上記管理項目を実施レベルに細分化したもの
3. **対象**：医療機関等の規模の目安
4. **技術的対策**：技術的に可能な対策、ひとつの実施項目に対して選択可能な対策を列挙した
5. **運用的対策**：4. の技術的対策をおこなった場合に必要な運用的対策の要約
6. **運用管理規程文例**：運用的対策を規程に記載する場合の文例

各機関等は実施項目に対して採用した技術的対策に応じた運用的対策を運用管理規程に含め、実際に規程が遵守されて運用されていることを確認することで、実施項目が達成されることになる。また技術的対策を選択する前に、それぞれの運用的対策を検討することで、自機関等で運用可能な範囲の技術的対策を選択することが可能である。一般に運用的対策の比重を大きくすれば情報システムの導入コストは下がるが、技術的対策の比重を大きくすれば利用者の運用的な負担は軽くなる。したがって適切なバランスを求めることは非常に重要なので、これらの付表を活用されることを期待する。

3　本ガイドラインの対象システム及び対象情報

本ガイドラインは保存システムだけではなく、医療に関わる情報を扱うすべての情報システムと、それらのシステムの導入、運用、利用、保守及び廃棄にかかわる人または組織を対象としている。ただし以下の 3 つの章は対象となる文書等が一部限定されている。

第 7 章の「電子保存の要求事項について」、第 8 章の「診療録及び診療諸記録を外部に保存する際の基準」、及び第 9 章の「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」は、e-文書法の対象範囲となる医療関係文書等として、「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」（平成１７年厚生労働省令第４４号)、「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法律等の施行等について」（平成１７年３月３１日付け医政発第 0331009 号・薬食発第 0331020 号・保発第 0331005 号厚生労働省医政局長・医薬食品局長・保険局長連名通知。以下「施行通知」という。）及び「「診療録等の保存を行う場所について」の一部改正について」（平成１７年３月３１日付け医政発第 0331010 号・保発第 0331006 号厚生労働省医政局長・保険局長連名通知。以下「外部保存改正通知」という。）で定められた文書等を対象としている。

１．第７章及び第９章の対象文書等（但し、※処方せんについては施行通知第二２（４）の要件を充足のこと。）

○施行通知　第二　２（１）

一　医師法(昭和２３年法律第２０１号)第２４条の規定による診療録

二　歯科医師法(昭和２３年法律第２０２号)第２３条の規定による診療録

三　保健師助産師看護師法(昭和２３年法律第２０３号)第４２条の規定による助産録

四　医療法（昭和２３年法律第２０５号）第５２条の規定による財産目録及び貸借対照表並びに損益計算書

五　歯科技工士法(昭和３０年法律第１６８号)第１９条の規定による指示書

六　薬剤師法(昭和３５年法律第１４６号)第２８条の規定による調剤録

七　外国医師又は外国歯科医師が行う臨床修練に係る医師法第十七条及び歯科医師法第十七条の特例等に関する法律（昭和６２年法律第２９号）第１１条の規定による診療録

八　救急救命士法(平成３年法律第３６号)第４６条の規定による救急救命処置録

九　医療法施行規則（昭和２３年厚生省令第５０号）第３０条の２３第１項及び第２項の規定による帳簿

十　保険医療機関及び保険医療養担当規則(昭和３２年厚生省令第１５号)第９条の規定による診療録等

十一　保険薬局及び保険薬剤師療養担当規則(昭和３２年厚生省令第１６号)第６条の規定

による調剤録

十二　臨床検査技師、衛生検査技師等に関する法律施行規則（昭和３３年厚生省令第２４号）第１２条の３の規定による書類

十三　医療法（昭和２３年法律第２０５号）第２１条第１項の規定による記録（同項第９号に規定する診療に関する諸記録のうち医療法施行規則第２０条第１０号に規定する処方せんに限る。）、第２２条の規定による記録（同条第２号に規定する診療に関する諸記録のうち医療法施行規則第２１条の５第２号に規定する処方せんに限る。）、及び第２２条の２の規定による記録（同条第３号に規定する診療に関する諸記録のうち医療法施行規則第２２条の３第２号に処方せんに限る。）※

十四　薬剤師法(昭和３５年法律第１４６号)第２７条の規定による処方せん※

十五　保険薬局及び保険薬剤師療養担当規則(昭和３２年厚生省令第１６号)第６条の規定による処方せん※

十六　医療法(昭和２３年法律第２０５号)第２１条第１項の規定による記録（医療法施行規則第２０条第１０号に規定する処方せんを除く。）、第２２条の規定による記録（医療法施行規則第２１条の５第２号に規定する処方せんを除く。）、及び第２２条の２の規定による記録（医療法施行規則第２２条の３第２号に規定する処方せんを除く。）

十七　歯科衛生士法施行規則(平成元年厚生省令第４６号)第１８条の規定による歯科衛生士の業務記録

○施行通知　第二　３

診療放射線技師法（昭和２６年法律第２２６号）第２８条第１項の規定による照射録

２．第８章の対象文書等

○外部保存改正通知　第１

１　医師法(昭和２３年法律第２０１号)第２４条に規定されている診療録

２　歯科医師法(昭和２３年法律第２０２号)第２３条に規定されている診療録

３　保健師助産師看護師法(昭和２３年法律２０３号)第４２条に規定されている助産録

４　医療法（昭和２３年法律第２０５号）第５２条に規定されている財産目録及び貸借対照表並びに損益計算書

５　医療法(昭和２３年法律第２０５号)第２１条、第２２条及び第２２条の２に規定されている診療に関する諸記録及び同法第２２条及び第２２条の２に規定されている病院の管理及び運営に関する諸記録

６　歯科技工士法(昭和３０年法律第１６８号)第１９条に規定されている指示書

７　外国医師又は外国歯科医師が行う臨床修練に係る医師法第十七条及び歯科医師法第十七条の特例等に関する法律（昭和６２年法律第２９号）第１１条に規定されている診

療録

8　救急救命士法(平成３年法律第３６号)第４６条に規定されている救急救命処置録

9　医療法施行規則（昭和２３年厚生省令第５０号）第３０条の２３第１項及び第２項に規定されている帳簿

１０　保険医療機関及び保険医療養担当規則(昭和３２年厚生省令第１５号)第９条に規定されている診療録等

１１　臨床検査技師、衛生検査技師等に関する法律施行規則（昭和３３年厚生省令第２４号）第１２条の３に規定されている書類

１２　歯科衛生士法施行規則(平成元年厚生省令第４６号)第１８条に規定されている歯科衛生士の業務記録

１３　診療放射線技師法（昭和２６年法律第２２６号）第２８条に規定されている照射録

4　電子情報を扱う医療機関等における責任のあり方

医療に関わるすべての行為は医療法等で医療機関等の管理責任者の責任で行うことが求められており、情報の取扱いも同等である。媒体に関わらず情報の取扱いは本章の最後に参考１として添付した「証拠能力、証明力について」や、参考２「技術的対策と運用による対策」を留意して医療機関等の自己責任で行う必要がある。

診療録等の電子保存や外部保存に係る自己責任は、電子化を行う場合に新たに付け加えられた要件ではなく、本来、そもそも紙やフィルムによる記録を院内に保存する場合も、医療法等で、医療機関等の管理責任者の責任、すなわち自己責任で行われてきており、それと同等な要件である。

ただ、紙の媒体やフィルムはその動きが一般の人にとってわかりやすく、特段の配慮が求められてこなかったが、電子化情報は一般の人にとってわかりにくく、情報の電子化はその実施が強制されるものではなく、それぞれの医療機関等がその事情によりメリット・デメリットを勘案して外部保存を含めた電子化の実施範囲及びその方法、すなわち導入システムの機能や運用計画を選択して求められる基準等への対応を決める必要があることから、自己責任で行っていることをあらためて明示し、管理責任者等の意識を喚起するために、あえて明記されたものと考えることができる。

自己責任は、「説明責任」、「管理責任」、「結果責任」を果たすことと考えられている。説明責任とは、電子保存や外部保存に関するシステムの機能や運用計画が電子保存や外部保存の基準を満たしていることを第三者に説明する責任である。管理責任とは、当該システムの運用管理を医療機関等が行う責任である。結果責任とは当該システムにより発生した問題点や損失に対する責任である。

この中で特段の配慮が必要なものは説明責任と管理責任で、説明責任を果たすためには、システムの仕様や運用計画を明確に文書化する必要がある。また仕様や計画が当初の方針の通りに機能しているかどうかを定期的に監査し、その結果もあいまいさのない形で文書化し、また監査の結果問題があった場合は、真摯に対応するのはもちろんのこと、その対応の記録も文書化し、第三者が検証可能な状況にすることが必要である。管理責任も、例えば電子保存や外部保存に関するシステムの管理を納入業者にまかせていては果たせない。すくなくとも管理状況の報告を定期的に受け、管理に関する最終的な責任の所在を明確にする等の監督を行う必要がある。

【参考 1】証拠能力・証明力について

訴訟における証拠能力・証明力については「高度情報通信社会推進本部制度見直し作業部会報告書　平成８年６月」に以下のように述べられている。

① 刑事訴訟

電子データの存在自体を立証する場合は、非供述証拠であり、刑事訴訟法上の伝聞法則の適用はなく、したがって、要証事実との関連性が立証できれば証拠能力が認められる。通常、プリントアウトした書面を証拠として提出することになるため、電子データの内容が正確に出力されていることの立証が必要とされている。

また、電子データの内容の真実性を立証する場合は、供述証拠であり、文書に準ずるものと考えられることから、証拠能力が認められるためには、要証事実との関連性に加え、刑事訴訟法上の伝聞法則の例外が認められるための要件の具備が必要とされている。この場合、商業帳簿等業務の通常の過程において作成された書面については、一般に業務の遂行に際して規則的、機械的かつ継続的に作成されるもので、作為の入り込む余地が少なく、正確に記載されるものと一般に期待されていることから、証拠能力が認められている。これ以外の書面についても特に信用すべき状況の下に作成されていることが認められれば、証拠能力が認められるが、商業帳簿等と同様に信用性の高い書面であることが必要とされている。

さらに、証明力については裁判官の自由な判断に委ねられているが、その判断は電子データの正確性等の評価に依存するものとされている。

以上から、電子データの証拠能力及び証明力の確保については、データの入力及び出力の正確性を確保するとともに、データの改変の可能性を減殺すること等により電子データの信頼性を高め、かつこれに対する責任の所在を明かにする必要がある。
そのためには、書類の内容、性格に応じた電子データの真正性、見読性及び保存性の確保措置を講ずる必要がある。

なお、紙で作成又は受領した証票類の電子化については、紙に記録される紙質、筆跡等の情報が電子データには記録されないため、犯罪捜査・立証上問題が多いと指摘されており、電子データによる保存を認めるに当たっては、その点に十分配意する必要がある。

② 民事訴訟

民事訴訟においては、証拠能力についての制限はなく、また、証明力については裁判官の自由な判断に委ねられている。

電子データによって保存された書類を証拠とする場合、その証明力の判断においては、データの入力及び出力の正確性、データの改変の可能性が問題となり、電子データの信頼性を高め、かつこれに対する責任の所在を明らかにすることが必要であるが、この点については、書類の内容、性格に応じた電子データの真正性、見読性及び保存性の確保措置を講ずる必要がある。

なお、書類の電子データによる保存の認容をどの程度とするかは、そのデータにより証明しようとする事柄についての挙証責任を官と民のいずれが負担するかについても関係するので、その点も踏まえ、検討することが必要である。

さらに、上記の補足として、医療分野における各種の法令にも留意する必要がある。

例えば、医師等の資格保有者が作成した文書は、医師法、歯科医師法、薬剤師法、医療法等の各種法令により、2 年から 5 年の保存期間が設けられている。保存期間が設けられている文書は財務関係書類等にも見られるが、財務関係書類等と大きく違う点が存在し、医師法を例に挙げれば、第 33 条の 2 の条項がそれにあたる。

この条項は、医師が診療行為を行って診療録を作成しなかった、もしくは 5 年間保存していなかった場合、50 万円以下の罰金刑を科するという条項である。つまり、医師は、診療録そのものを作成・保存していない行為そのものが刑事罰の対象となる。このような厳しい規定は、健康情報を扱う医療分野の特異性といえる。

裁判等で、電子データの証拠能力、証明力を争う場合は、「高度情報通信社会推進本部制度見直し作業部会報告書　平成 8 年 6 月」の見解に加え、このような医療分野に特異な法令も踏まえた上で検討をすることが必要である。

【参考 2】技術的対策と運用による対策

情報システムの安全を担保するためには、「技術的な対応」と「組織的な対応（運用による対策)」の総合的な組み合わせによって達成する必要がある。

技術的な対応は医療機関等の総合的な判断の下、主にシステム提供側（ベンダー）に求められるものであり、組織的な対応（運用による対策）は利用者側（医療機関等）の責任で実施される。

総合的な判断とは、リスク分析に基づき、経済性も加味して装置仕様あるいはシステム要件と運用管理規程により基準に適合させることである。この選択は安全性に対する脅威やその対策に対する技術的変化や医療機関等の組織の変化を含めた社会的環境変化により異なってくるので、その動向に注意を払う必要がある。

運用管理規程は、医療機関等として総合的に作成する場合と医用画像の電子保存のように部門別や装置別に作成される場合がある。基準を満たしているか否かを判断する目安として「基準適合チェックリスト」等を作成して整理しておく必要がある。このようなチェックリストは第三者へ説明する際の参考資料に利用できる。

5　情報の相互利用性と標準化について

本ガイドラインの大部分は医療にかかわる情報の様々な程度の電子化を前提としている。医療機関等において情報処理システムを導入する目的は当初は事務処理の合理化だけであったが、現在は平成 13 年に作成された「保健医療分野の情報化にむけてのグランドデザイン」でも明確に記載されているように、情報の共有の推進や、医療安全、医療の質の向上に寄与できるものであることが求められている。

これらの目的を実現するためには情報の適切な標準化が必要であることは論を待たない。本ガイドラインは医療に関係する情報システムの安全な管理・運用を目的としているが、情報の安全性の重要な要素として、必要時に利用可能であることを確保する可用性を上げることができる。

可用性は情報を保持しなければならない任意の時点で確保されなければならない。例えば、医療機関等で医療情報を長期間保存する際、システム更新に伴い新旧のシステム間での情報の互換性を保ち旧システムで保存された医療情報を確実に読み出せるという、「新旧システムで医療情報の相互利用性」を確保することは、電子保存の見読性及び保存性原則確保の点からみても医療情報システムの必須の要件である。

医療に有用な意味のある情報を長期間に渡り読み出し可能な形で保存するためには、将来に渡りメンテナンスが継続することが期待される標準的な用語集やコードセットを出来る限り利用して保存を行うことが望ましい。

5.1　標準的な用語集やコードセットの利用

すでに公開されている用語集やコードセットのうち、日本での各分野における実質的な標準的用語コード集と考えられるものについては情報の保存の際にこれらを利用することが強く推奨される。使用しない場合でもこれらの用語集やコードセットに容易に変換できることが必要である。以下に標準的な用語集やコードセットの例をあげるが、医療情報標準化推進協議会（ Health Information and Communication Standards　Board：HELICS 協議会）がわが国での用語集やコードセットの標準案の登録を進めており、随時参照されたい。

病名：ICD10 対応電子カルテ用標準病名マスタ
医薬品名：標準医薬品マスタ
臨床検査：JAHIS 臨床検査データ交換規約

5.2　国際的な標準規格への準拠

DICOM（Digital Imaging and Communications in Medicine）、HL7（Health Level Seven）等の規格及びこれらの規格の標準的な運用方法を定めた IHE（Integrating the Healthcare Enterprise）は、国際的な標準や規格として提唱され、一部はわが国でも利用が進んでいる。

これらの国際的な標準や規格の中で、我が国の医療に適合するものについては、情報の相互利用性の観点から直接これらの規格や標準を採用するか、少なくともこれらの規格や標準に適合した情報形式に容易に変換可能な状態にしておくことが強く推奨される。

また、注意しなければならない点として外字の問題がある。外字とは JIS 文字コードのような容易に移行可能な文字セット以外の文字を独自に定義してもちいた表記文字であるが、そのような外字を使用したシステムではあらかじめ使用した外字のリストを管理し、システムを変更した場合や、他のシステムと情報を交換する場合には表記に齟齬のないように対策する必要がある。標準化の観点から見れば外字を使用する必要がない、文字セットが検討されることを期待したい。

6　情報システムの基本的な安全管理

情報システムの安全管理は、刑法等で定められた医療専門職に対する守秘義務等や個人情報保護関連各法（個人情報保護法、行政機関の保有する個人情報の保護に関する法律（平成１５年法律第５８号)、独立行政法人等の保有する個人情報の保護に関する法律（平成１５年法律第５９号)）に規定された安全管理・確保に関する条文によって法的な責務として求められている。守秘義務は医療専門職や行政機関の職員等の個人に、安全管理・確保は個人情報取扱事業者や行政機関の長等に課せられた責務である。安全管理をおろそかにすることは上記法律に違反することになるが、医療においてもっとも重要なことは患者等との信頼関係であり、単に違反事象がおこっていないことを示すだけでなく、安全管理が十分であることを説明できること、つまり説明責任を果たすことが求められる。この章での制度上の要求事項は個人情報保護法の条文を例示する。

A. 制度上の要求事項

（安全管理措置）

法第二十条　個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない。

（従業者の監督）

法第二十一条　個人情報取扱事業者は、その従業者に個人データを取り扱わせるに当たっては、当該個人データの安全管理が図られるよう、当該従業者に対する必要かつ適切な監督を行わなければならない。

（委託先の監督）

法第二十二条　個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない。

6.1　方針の制定と公表

「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」でも個人情報保護に関する方針を定め公表することが求められているが、情報システムの安全管理も個人情報保護対策の一部として考えることができるため、上記の方針の中に情報システムの安全管理についても言及する必要がある。

少なくとも情報システムで扱う情報の範囲、取扱いや保存の方法と期間、利用者識別を確実に行い不要・不法なアクセスを防止していること、安全管理の責任者、苦情・質問の窓口を含めること。

6.2　医療機関における情報セキュリティマネジメントシステム（ISMS）の実践

6.2.1　ISMS 構築の手順

ISMS の構築は PDCA モデルによって行われる。JIS Q27001:2006 では PDCA の各ステップを次の様に規定している。

ISMS プロセスに適用される PDCA モデルの概要

Plan－計画 (ISMS の確立)	組織の全般的方針及び目的に従った結果を出すための、リスクマネジメント及び情報セキュリティの改善に関連した、ISMS 基本方針、目的、プロセス及び手順の確立
Do－実施 (ISMS の導入及び運用)	ISMS 基本方針、管理策、プロセス及び手順の導入及び運用
Check－点検 (ISMS の監視及び見直し)	ISMS 基本方針、目的及び実際の経験に照らした、プロセスのパフォーマンスのアセスメント（適用可能ならば測定）、及びその結果のレビューのための経営陣への報告
Act－処置 (ISMS の維持及び改善)	ISMS の継続的な改善を達成するための、ISMS の内部監査及びマネジメントレビューの結果又はその他の関連情報に基づいた是正処置及び予防処置の実施

P では ISMS 構築の骨格となる文書（基本方針、運用管理規程など）と文書化された ISMS 構築手順を確立する。
D では P で準備した文書や手順を使って実際に ISMS を構築する。
C では構築した ISMS が適切に運用されているか、監視と見直しを行う。
A では改善すべき点が出た場合に是正処置や予防処置を検討し、ISMS を維持する。

上記のステップをより身近にイメージできるようにするために、医療行為における安全管理のステップがどのようにおこなわれているかについて JIPDEC（財団法人 日本情報処理開発協会）の「医療機関向け ISMS ユーザーズガイド」では次のような例が記載されている。

【医療の安全管理の流れ】

事故やミスの発見と報告

「ヒヤリ、ハット事例」や「インシデントレポート」による事故やミスの発見と報告

↓

原因の分析

- 「プロセスアプローチ」によって医療行為をプロセスと捉え、事故やミスの起きた業務全体を一つ一つの単体プロセス（動作）に分解し、フロー図として目に見える形にする。
  （例えば注射を例にプロセスに分解すれば、①医師が処方箋を出し、②処方箋が薬剤部に送られ、③薬剤部から処方が病棟に届けられ、④病棟では看護師が正しく準備し、⑤注射を実施する、となる）
- 作成したフロー図を分析し、どのプロセスに原因があったのかを調べる。

↓

予防／是正策

- 再発防止のための手段を検討と実施（手順の変更、エラーチェックの仕組み導入、職員への教育の徹底など）

上記を見ると、主にD→C→Aが中心になっている。これは医療分野においては診察、診断、治療、看護などの手順が過去からの蓄積によってすでに確立されているため、あとは事故やミスを発見したときにその手順を分析していくことで、どこを改善すればよいかがおのずと見え、それを実行することで安全が高まる仕組みが出来上がっているためと言える。

反面、情報セキュリティではIT技術の目覚しい発展により、過去の経験の蓄積だけでは想定できない新たなセキュリティ上の問題点や弱点が常に存在し得る。そのため情報セキュリティ独自の管理方法が必要であり、ISMSはそのために考え出された。ISMSは医療の安全管理と同様PDCAサイクルで構築し、維持して行く。

逆に言えば、医療関係者にとってISMS構築はPのステップを適切に実践し、ISMSの骨格となる文書体系や手順などを確立すれば、あとは自然にISMSが構築されていく土壌があると言える。

Pのステップを実践するために必要なことは何かについて次に述べる。

6.2.2 取扱い情報の把握

情報システムで扱う情報をすべてリストアップし、安全管理上の重要度に応じて分類を行い、常に最新の状態を維持する必要がある。このリストは情報システムの安全管理者が

必要に応じて速やかに確認できる状態で管理されなければならない。

安全管理上の重要度は、安全性が損なわれた場合の影響の大きさに応じて決める。少なくとも患者等の視点からの影響の大きさと、継続した業務を行う視点からの影響の大きさを考慮する必要がある。この他に医療機関等の経営上の視点や、人事管理上の視点等の必要な視点を加えて重要度を分類する。

一般に医療に係る情報が個人識別可能な状態で安全性に問題が生じた場合、患者等にきわめて深刻な影響を与える可能性があり、もっとも重要度の高い情報として分類される。

6.2.3 リスク分析

分類された情報ごとに、管理上の過誤、機器の故障、外部からの侵入、利用者の悪意、利用者の過誤等による脅威を列挙する。医療機関等では一般に他の職員等への信頼を元に業務を進めているために、同僚等の悪意や過誤を想定することに抵抗がある。しかし、情報の安全管理を達成して説明責任を果たすためには、たとえ起こりえる可能性は低くても、万が一に備えて対策を準備する必要がある。また説明責任を果たすためには、これらのリスク分析の結果は文書化して管理する必要がある。この分析の結果えられた脅威に対して、6.3～6.10 の対策を行うことになる。

特に安全管理や個人情報保護関連各法で原則禁止されている目的外利用の防止はシステム機能だけでは決して達成できないことに留意しなければならない。システムとして可能なことは人が正しく操作すれば誰が操作したかを明確に記録しつつ安全に稼動することを保障するのが限界である。したがって人の行為も含めた脅威を想定し、運用規程を含めた対策を講じることが重要である。

医療情報システムとして上記の観点で留意すべき点は、システムに格納されている電子データに関してだけでなく、入出力の際に露見等の脅威にさらされる恐れのある個人情報を保護するための方策を考える必要がある。以下にさまざまな状況で想定される脅威を列挙する。

① 医療情報システムに格納されている電子データ
- (a) 権限のない者による不正アクセス、改ざん
- (b) 権限のある者による不当な目的でのアクセス、改ざん
- (c) コンピュータウイルス等の不正なソフトウェアによるアクセス、改ざん

② 入力の際に用いたメモ・原稿・検査データ等
- (a) メモ・原稿・検査データ等の覗き見
- (b) メモ・原稿・検査データ等持ち出し
- (c) メモ・原稿・検査データ等のコピー

(d) メモ・原稿・検査データの不適切な廃棄

③ データを格納した可搬型媒体等

(a) 可搬型媒体の持ち出し

(b) 可搬型媒体のコピー

(c) 可搬型媒体の不適切な廃棄

(d) 非可搬型媒体（ハードディスクを搭載したパーソナルコンピュータ等（以下、PC 等という。）の不適切な廃棄

④ 参照表示した端末画面等

(a) 端末画面の覗き見

⑤ データを印刷した紙やフィルム等

(a) 紙やフィルム等の覗き見

(b) 紙やフィルム等の持ち出し

(c) 紙やフィルム等のコピー

(d) 紙やフィルム等の不適切な廃棄

⑥ 医療情報システム自身

(a) サイバー攻撃による IT 障害

- 不正侵入
- 改ざん
- 不正コマンド実行
- 情報かく乱
- ウイルス攻撃
- サービス不能（DoS：Denial of Service）攻撃
- 情報漏えい　等

(b) 非意図的要因による IT 障害

- システムの仕様やプログラム上の欠陥（バグ）
- 操作ミス
- 故障
- 情報漏えい　等

(c) 災害による IT 障害

- 地震、水害、落雷、火災等の災害による電力供給の途絶
- 地震、水害、落雷、火災等の災害による通信の途絶
- 地震、水害、落雷、火災等の災害によるコンピュータ施設の損壊等
- 地震、水害、落雷、火災等の災害による重要インフラ事業者等における IT の

機能不全

これらの脅威に対し、対策を行うことにより、発生可能性を低減し、リスクを実際上問題のないレベルにまで小さくすることが必要になる。

6.3　組織的安全管理対策（体制、運用管理規程）

B. 考え方

安全管理について、従業者の責任と権限を明確に定め、安全管理に関する規程や手順書を整備運用し、その実施状況を確認しなければならない。これは組織内で情報システムを利用するかどうかにかかわらず遵守すべき事項である。組織的安全管理対策には以下の事項が含まれる。

① 安全管理対策を講じるための組織体制の整備
② 安全管理対策を定める規程等の整備と規程等に従った運用
③ 医療情報取扱い台帳の整備
④ 医療情報の安全管理対策の評価、見直し及び改善
⑤ 事故又は違反への対処

管理責任や説明責任を果たすために運用管理規程はきわめて重要であり、必ず定めなければならない。運用管理規程には必ず以下の項目を含めること。

- 理念（基本方針と管理目的の表明）
- 医療機関等の内部の体制、外部保存に関わる外部の人及び施設
- 契約書・マニュアル等の文書の管理
- 機器を用いる場合は機器の管理
- 患者等への説明と同意を得る方法
- 監査
- 苦情の受け付け窓口

C. 最低限のガイドライン

1. 情報システム運用責任者の設置及び担当者（システム管理者を含む）の限定を行うこと。ただし小規模医療機関等において役割が自明の場合は、明確な規程を定めなくとも良い。
2. 個人情報が参照可能な場所においては、来訪者の記録・識別、入退を制限する等の入退管理を定めること。
3. 情報システムへのアクセス制限、記録、点検等を定めたアクセス管理規程を作成すること。
4. 個人情報の取扱いを委託する場合、委託契約において安全管理に関する条項を含めること。

5. 運用管理規程等において次の内容を定めること。

(a) 個人情報の記録媒体の管理（保管・授受等）の方法

(b) リスクに対する予防、発生時の対応の方法

6.4 物理的安全対策

B. 考え方

物理的安全対策とは、情報システムにおいて個人情報が入力、参照、格納される、情報端末やコンピュータ、情報媒体等を物理的な方法によって保護することである。具体的には情報の種別、重要性と利用形態に応じて幾つかのセキュリティ区画を定義し、以下の事項を考慮し、適切に管理する必要がある。

① 入退館（室）の管理（業務時間帯、深夜時間帯等の時間帯別に、入室権限を管理）
② 盗難、窃視等の防止
③ 機器・装置・情報媒体等の物理的な保護

C. 最低限のガイドライン

1. 個人情報が保存されている機器の設置場所及び記録媒体の保存場所には施錠すること。
2. 個人情報を入力、参照できる端末が設置されている区画は、業務時間帯以外は施錠等、権限者以外立ち入ることが出来ない対策を講じること。
   ただし、本体策項目と同等レベルの他の取りうる手段がある場合はこの限りではない。
3. 個人情報の物理的保存を行っている区画への入退管理を実施すること。
   - 入退者には名札等の着用を義務付け、台帳等に記入することによって入退の事実を記録すること。
   - 入退者の記録を定期的にチェックし、妥当性を確認すること。
4. 個人情報が存在する PC 等の重要な機器に盗難防止用チェーンを設置すること。
5. 離席時にも端末等での正当な権限者以外の者による窃視防止の対策を実施すること。

D. 推奨されるガイドライン

防犯カメラ、自動侵入監視装置等を設置すること。

6.5 技術的安全対策

B. 考え方

技術的な対策のみで全ての脅威に対抗できる保証はなく、一般的には運用管理による対策との併用は必須である。

しかし、その有効範囲を認識し適切な適用を行えば、これらは強力な手段となりうる。ここでは「6.2.3 リスク分析」で列挙した脅威に対抗するために利用できる技術的な対策として下記の項目について解説する。

(1) 利用者の識別及び認証
(2) 情報の区分管理とアクセス権限の管理
(3) アクセスの記録（アクセスログ）
(4) 不正ソフトウェア対策
(5) ネットワーク上からの不正アクセス

(1) 利用者の識別及び認証

情報システムへのアクセスを正当な利用者のみに限定するために、情報システムは利用者の識別と認証を行う機能を持たなければならない。

小規模な医療機関等で情報システムの利用者が限定される場合には、日常の業務の際に必ずしも識別・認証が必須とは考えられないケースが想定されることもあるが、一般的に言ってこの機能は必須である。

認証を実施するためには、情報システムへのアクセスを行う全ての職員及び関係者に対しID・パスワードやICカード、電子証明書、生体認証等、本人の識別・認証に用いられる手段を用意し、統一的に管理する必要がある。また更新が発生する都度速やかに更新作業が行われなければならない。

このような本人の識別・認証に用いられる情報は本人しか知り得ない、または持ち得ない状態を保つ必要がある。例えば、以下のような行為により、本人の識別・認証に用いられる情報が第三者に漏れないように防止策を取らなければならない。

- IDとパスワードが書かれた紙等が貼られていて、第三者が簡単に知ることができてしまう。
- パスワードが設定されておらず、誰でもシステムにログインできてしまう。
- 代行作業等のためにＩＤ・パスワードを他人に教えており、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い。
- 容易に推測できる、あるいは、文字数の少ないパスワードが設定されており、容易にパスワードが推測できてしまう。
- パスワードを定期的に変更せずに使用しているために、パスワードが推測される可能性が高くなっている。

- 認証用の個人識別情報を格納するトークン（IC カード、USB キー等）を他人に貸与する、または持ち主に無断で借用することにより、利用者が特定できない。
- 退職した職員の ID が有効になったままで、ログインができてしまう。
- 医療情報部等で、印刷放置されている帳票等から、パスワードが盗まれる。
- コンピュータウイルスにより、ID やパスワードが盗まれ、悪用される。

＜認証強度の考え方＞

ID、パスワードの組合せは、これまで広く用いられてきた方法である。しかし、ID、パスワードのみによる認証では、上記に列挙したように、その運用によってリスクが大きくなる。認証強度を維持するためには、交付時の初期パスワードの本人による変更や定期的なパスワード変更を義務づける等、システムの実装や運用を工夫し、必ず本人しか知り得ない状態を保つよう対策を行う必要がある。

このような対策を徹底することは一般に困難であると考えられ、その実現可能性の観点からは推奨されない。

認証に用いられる手段としては、IC カード等のセキュリティ・デバイス＋パスワードのように利用者しか持ち得ない 2 つの独立した要素を用いて行う方式（2 要素認証）やバイオメトリクス等、より認証強度が高い方式を採用することが望ましい。

また、入力者が端末から長時間、離席する場合には、正当な入力者以外の者による入力を防止するため、クリアスクリーン等の防止策を講じるべきである。

＜IC カード等のセキュリティ・デバイスを配布する場合の留意点＞

利用者の識別や認証、署名等を目的として、IC カード等のセキュリティ・デバイスに個人識別情報や暗号化鍵、電子証明書等を格納して配布する場合は、これらのデバイスが誤って本人以外の第三者の手に渡ることのないような対策を講じる必要がある。また、万一そのデバイスが第三者によって不正に入手された場合においても、簡単には利用されないようになっていることが重要である。

したがって、利用者の識別や認証、署名等が、これらデバイス単独で可能となるような運用はリスクが大きく、必ず利用者本人しか知りえない情報との組合せによってのみ有功になるようなメカニズム、運用方法を採用すること。

IC カードの破損等、本人の識別情報が利用できない時を想定し、緊急時の代替え手段による一時的なアクセスルールを用意するべきである。その際、安全管理のレベルを安易に下げることがないように、本人確認を十分におこなった上で代替手段の使用を許し、さらにログ等を残し後日再発行された本人の正規の識別情報により、上記緊急時の操作のログ等の確認操作をすることが望ましい。

＜バイオメトリクスを利用する場合の留意点＞

識別・認証に指紋や虹彩、声紋等のバイオメトリクス（生体計測情報）を用いる場合は、その測定精度にも注意を払う必要がある。医療情報システムで一般的に利用可能と思われる現存する各種のバイオメトリクス機器の測定精度は、１対 N 照合（入力された 1 つのサンプルが、登録されている複数のサンプルのどれに一致するか）には十分とは言えず、1 対 1 照合（入力されたサンプルが、特定の 1 つのサンプルと一致するか）での利用が妥当であると考えられる。

したがって、バイオメトリクスを用いる場合は、単独での識別・認証を行わず、必ずユーザ ID 等個人を識別できるものと組合せて利用するべきである。

また、生体情報を基に認証するために以下のような、生体情報特有の問題がある。

・事故や疾病等により認証に用いる部位の損失等
・成長等に認証に用いる部位の変化
・一卵性の双子の場合、特徴値が近似する手法がある
・赤外線写真等による"なりすまし"(IC カード等の偽造に相当)

上記の事を考慮のうえ、生体情報の特徴を吟味し適切な手法を用いる必要がある。

"なりすまし"や欠損等の対処として、異なる手法や異なる部位の生体情報を用いたり、IC カード等のセキュリティ・デバイスと組み合わせを行う方法や、従来のパスワードを付加する方法も有効である。

(2)　情報の区分管理とアクセス権限の管理

情報システムの利用に際しては、情報の種別、重要性と利用形態に応じて情報の区分管理を行い、その情報区分ごと、組織における利用者や利用者グループ（業務単位等）ごとに利用権限を規定する必要がある。ここで重要なことは、付与する利用権限を必要最小限にすることである。

知る必要のない情報は知らせず、必要のない権限は付与しないことでリスクが低減される。情報システムに、参照、更新、実行、追加等のようにきめ細かな権限の設定を行う機能があれば、さらにリスクは低減される。

アクセス権限の見直しは、人事異動等による利用者の担当業務の変更等に合わせて適宜行う必要があり、組織の規程で定められていなければならない。

(3)　アクセスの記録（アクセスログ）

個人情報を含む資源については、全てのアクセスの記録（アクセスログ）を収集し、定期的にその内容をチェックして不正利用がないことを確認しなければならない。

アクセスログは、それ自体に個人情報が含まれている可能性があること、さらにはセキュリティ事故が発生した際の調査に非常に有効な情報であるため、その保護は必須である。したがって、アクセスログへのアクセス制限を行い、削除／改ざん／追加等を防止する対

策を講じなければならない。

また、アクセスログの証拠性確保のためには、記録する時刻は重要である。精度の高いものを使用し、組織内の全てのシステムで同期をとらねばならない。

(4)　不正ソフトウェア対策

ウイルス、ワーム等と呼ばれる様々な形態を持つ不正なコードは、電子メール、ネットワーク、可搬媒体等を通して情報システム内に入る可能性がある。これら不正コードの侵入に際して適切な保護対策がとられていなければ、セキュリティ機構の破壊、システムダウン、情報の暴露や改ざん、情報の破壊、資源の不正使用等の重大な問題を引き起こされる。そして、何らかの問題が発生して初めて、不正コードの侵入に気づくことになる。

対策としては不正コードのスキャン用ソフトウェアの導入が最も効果的であると考えられ、このソフトウェアを情報システム内の端末装置、サーバ、ネットワーク機器等に常駐させることにより、不正コードの検出と除去が期待できる。しかし、これらのコンピュータウイルス等も常に変化しており、検出のためにはパターンファイルを常に最新のものに更新することが必須である。

ただし、たとえ優れたスキャン用ソフトウェアを導入し、適切に運用したとしても、全ての不正コードが検出できるわけではない。このためには、情報システム側の脆弱性を可能な限り小さくしておくことが重要であり、オペレーティング・システム等でセキュリティ・ホールの報告されているものについては、対応版（セキュリティ・パッチと呼ばれるもの）への逐次更新、さらには利用していないサービスや通信ポートの非活性化、マクロ実行の抑制等も効果が大きい。

(5) ネットワーク上からの不正アクセス

ネットワークからのセキュリティでは、クラッカーやコンピュータウイルスや不正アクセスを目的とするソフトウェアの攻撃から保護するための一つ手段としてファイアウォールの導入がある。

ファイアウォールは 「パケットフィルタリング」、「アプリケーションゲートウェイ」および「ステートフルインスペクション」の各種方式がある。またその設定によっても動作機能が異なるので、単にファイアウォールを入れれば安心ということにはならない。パケットフィルタリング以外の手法を用いて、ネットワークからの攻撃から保護することが望ましい。システム管理者はその方式が何をどのように守っているかを認識するべきである。

また、電子メールや Web に対してのセキュリティ商品として、ファイアウォールとウイルス対策ソフトを一つのものとして提供している商品もある。不正な攻撃を検知するシステム（IDS : Intrusion Detection System）もあり、システムの使用環境に合わせて、こうしたシステムとの組み合わせを行う必要がある。また、システムのネットワーク環境

におけるセキュリティホール（脆弱性等）に対する診断（セキュリティ診断）を定期的に実施し、パッチ等の対策を講じておく事も重要である。

無線 LAN や情報コンセントが部外者により、物理的にネットワークに接続できる可能性がある場合、不正なコンピュータを接続し、ウイルス等を感染させたり、サーバやネットワーク機器に対して攻撃（サービス不能攻撃 DoS：Denial of Service　等）を行なったり、不正にネットワーク上のデータを傍受したり改ざん等が可能となる。不正な PC に対する対策を行なう場合、一般的に MAC アドレスにて PC を識別する場合が多いが、MAC アドレスは改ざん可能であるため、その事を念頭に置いた上で対策を行なう必要がある。不正アクセスの防止は、いかにアクセス先の識別を確実に担保するかが問題であり、特に、“なりすまし“の問題は絶えずついて廻る。

C. 最低限のガイドライン

1. 情報システムへのアクセスにおける利用者の識別と認証を行うこと。
2. 動作確認等で個人情報を含むデータを使用するときは、漏洩等に十分留意すること。
3. 医療従事者、関係職種ごとに、アクセスできる診療録等の範囲を定め、そのレベルに沿ったアクセス管理を行うこと。複数の職種の利用者がアクセスするシステムでは職種別のアクセス管理機能があることが求められるが、現状でそのような機能がない場合は、システム更新までの期間、運用管理規定でアクセス可能範囲をさだめ、次項の操作記録を行なうことで担保する必要がある。
4. アクセスの記録及び定期的なログの確認を行うこと。アクセスの記録はすくなくとも利用者のログイン時刻および時間、ログイン中に操作した患者が特定できること。

   情報システムにアクセス記録機能があることが前提であるが、ない場合は業務日誌等で操作の記録（操作者及び操作内容）を必ず行うこと。
5. アクセスの記録に用いる時刻情報は信頼できるものであること。医療機関等の内部で利用する時刻情報は同期している必要があり、また標準時刻と定期的に一致させる等の手段で標準時と診療事実の記録として問題のない範囲の精度を保つ必要がある。
6. システム構築時や、適切に管理されていないメディアを使用したり、外部からの情報を受け取る際にはウイルス等の不正なソフトウェアの混入がないか確認すること。
7. パスワードを利用者識別に使用する場合

   システム管理者は以下の事項に留意すること。

   (1) システム内のパスワードファイルでパスワードは必ず暗号化(不可逆)され、適切な手法で管理及び運用が行われること。(利用者識別にＩＣカード等他の手

段を併用した場合はシステムに応じたパスワードの運用方法を運用規程にて定めること)

(2) 利用者がパスワードを忘れたり、盗用される恐れがある場合で、システム管理者がパスワードを変更する場合には、利用者の本人確認を行い、どのような手法で本人確認を行ったのかを台帳に記載(本人確認を行った書類等のコピーを添付)し、本人以外が知りえない方法で再登録を実施すること。

(3) システム管理者であっても、利用者のパスワードを推定できる手段を防止すること。(設定ファイルにパスワードが記載される等があってはならない。)

また、利用者は以下の事項に留意すること。

(1) パスワードは定期的に変更し（最長でも 2 ヶ月以内)、極端に短い文字列を使用しないこと（8 バイト以上の可変長の文字列が望ましい)。

(2) 類推しやすい、不注意によるパスワードの盗用は、盗用された本人の責任になることを認識すること。

D. 推奨されるガイドライン

1. 情報の区分管理を実施し、区分単位でアクセス管理を実施すること。
2. アクセスの記録として、誰が、何時、誰の情報にアクセスしたかを記録し、定期的な記録の確認を行うこと。
3. 常時ウイルス等の不正なソフトウェアの混入を防ぐ適切な措置をとること。また、その対策の有効性・安全性の確認・維持（たとえばパターンファイルの更新の確認・維持）を行なうこと。
4. 離席の場合のクローズ処理等を施すこと（クリアスクリーン：ログオフあるいはパスワード付きスクリーンセーバー等)。
5. 外部のネットワークとの接続点や DB サーバ等の安全管理上の重要部分にはファイアウォール（ステートフルインスペクション）を設置し、ACL(アクセス制御リスト)等を適切に設定すること。

   また、無線 LAN を用いる場合はリスクの増大を慎重に考慮し、総務省発行の「安心して無線 LAN を利用するために」を参考にし、暗号化や容易に推測できない SSID を用いる等、情報資産の評価にもとづき適切な配慮をおこなうこと。
6. パスワードを利用者識別に使用する場合以下の基準を遵守すること。
   (1) パスワード入力が不成功に終わった場合の再入力に対して一定不応時間を設定すること。
   (2) パスワード再入力の失敗が一定回数を超えた場合は再入力を一定期間受け付けない機構とすること。
7. 認証に用いられる手段としては、ID＋バイオメトリックスあるいは IC カード等の

セキュリティ・デバイス＋パスワードまたはバイオメトリックスのように利用者しか持ち得ない 2 つの独立した要素を用いて行う方式（2 要素認証）等、より認証強度が高い方式を採用することが望ましい。

6.6　人的安全対策

B. 考え方

医療機関等は、情報の盗難や不正行為、情報設備の不正利用等のリスク軽減をはかるため、人による誤りの防止を目的とした人的安全対策を策定する必要がある。これには守秘義務と違反時の罰則に関する規定や教育、訓練に関する事項が含まれる。

医療情報システムに関連する者として、次の 5 種類を想定する。

(a) 医師、看護師等の業務で診療に係わる情報を取扱い、法令上の守秘義務のある者
(b) 医事課職員、その事務委託者等の診療を維持するための業務に携わり、雇用契約の元に医療情報を取扱い、守秘義務を負う者
(c) システムの保守業者等の雇用契約を結ばずに診療を維持するための業務に携わる者
(d) 患者、見舞い客等の医療情報にアクセスする権限を有しない第三者
(e) 診療録等の外部保存の委託においてデータ管理業務に携わる者

このうち、(a) (b)については、医療機関等の従業者としての人的安全管理措置、(c)については、守秘義務契約を結んだ委託業者としての人的安全管理措置の２つに分けて説明する。

(d)の第三者については、そもそも医療機関等の医療情報システムに触れてはならないものであるため、物理的安全管理対策や技術的安全管理対策によって、システムへのアクセスを禁止する必要がある。また、万が一、第三者によりシステム内の情報が漏洩等した場合については、不正アクセス行為の禁止等に関する法律等の他の法令の定めるところにより適切な対処等をする必要がある。

(e)については、いわゆる「外部保存」の委託先の機関等に該当するが、これに関しては、その主旨と実施の詳細を 8 章に記述する。

(1) 従業者に対する人的安全管理措置

C. 最低限のガイドライン

医療機関等の管理者は、個人情報に関する施策が適切に実施されるよう措置するとともにその実施状況を監督する必要があり、以下の措置をとること。

1. 法令上の守秘義務のある者以外を事務職員等として採用するにあたっては、雇用及び契約時に守秘・非開示契約を締結すること等により安全管理を行うこと。
2. 定期的に従業者に対し教育訓練を行うこと。
3. 従業者の退職後の個人情報保護規程を定めること。

D. 推奨されるガイドライン

1. サーバ室等の管理上重要な場所では、モニタリング等により従業者に対する行動の管理を行うこと。

(2) 事務取扱委託業者の監督及び守秘義務契約

C. 最低限のガイドライン

1. プログラムの異常等で、保存データを救済する必要があるとき等、やむをえない事情で病院事務、運用等で、外部受託業者を採用する場合は、医療機関等の内部における適切な個人情報保護が行われるように、以下のような措置を行うこと。

   ① 包括的な委託先の罰則を定めた就業規則等で裏づけられた守秘契約を締結すること
   ② 保守作業等の医療情報システムに直接アクセスする作業の際には、作業者・作業内容・作業結果の確認をおこなうこと。
   ③ 清掃等の直接医療情報システムにアクセスしない作業の場合においても、作業後の定期的なチェックを行うこと。
   ④ 委託先事業者が再委託を行うか否かを明確にし、再委託を行う場合は委託先と同等の個人情報保護に関する対策及び契約がなされていることを条件とすること。

2. プログラムの異常等で、保存データを救済する必要があるとき等、やむをえない事情で外部の保守要員が診療録等の個人情報にアクセスする場合は、罰則のある就業規則等で裏づけられた守秘契約等の秘密保持の対策を行うこと。

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

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、安全な情報システムの構築を推進するため、システム全体の構成管理を適切に行い、定期的にシステム評価を実施し、最新のセキュリティ技術や標準を適切に取り入れ、客観的に評価された暗号、製品等を導入することも重要である。

なお、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. リモートメンテナンス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　災害等の非常時の対応

B. 考え方

医療機関等は医療情報システムに不具合が発生した場合でも患者安全を配慮した医療サービスの提供が最優先されなければならない。

ここでは、「6.2.3　リスク分析」の「⑥医療情報システム自身」に掲げる自然災害やサイバー攻撃による IT 障害などの非常時に、医療情報システムが通常の状態で使用が出来ない事態に陥った場合における留意事項について述べる。

「通常の状態で使用できない」とは、システム自体が異常動作または停止になる場合と、使用環境が非定常状態になる場合がある。

前者としては、医療情報システムが損傷を被ることにより、システムの縮退運用あるいは全面停止に至り、医療サービス提供に支障発生が想定される場合である。

後者としては、自然災害発生時には多数の傷病者が医療サービスを求める状態になり、医療情報システムが正常であったとしても通常時のアクセス制御下での作業では著しい不合理の発生が考えられる場合である。この際の個人情報保護に関する対応は、「生命、身体の保護のためであって、本人の同意を得ることが困難であるとき」に相当すると解せられる。

(1) 非常時における事業継続計画(BCP：Business Continuity Plan)

非常事態が発生している最中では適切な意思決定は望み難いので、事前にできるだけ多くの意思決定を準備しておくことが望ましい。非常事態を事前に適切に分類することは難しく、可能な限り計画内容を事前演習などで検証することが望ましい。

医療施設として定められる BCP においては､医療情報システムについての計画を含め、全体としての整合性が必要である。

以下に、BCP としての策定計画と運用に関する一般項目を参考に掲げる。

① BCP として事前に周知しておく必要がある事項

事前に対応策を知ってもらい、信頼してもらっておくべきである。

- ポリシと計画
  何が「非常事態」なのかを理解し、定義すべきである。
- 非常事態検知手段
  災害や故障の検知機能と発生情報の確認手段
- 非常時対応チームの連絡先リスト、連絡手段および対策ツール
- 非常時に公にすべき文書および情報

② BCP 実行フェーズ

災害や事故の発生（或いは発生の可能性）を検知してから、BCP 実行か通常の障

害対策かの判断を行い、BCP 発動と判断した場合は関係者の召集、対策本部等の設置、関係先への連絡･協力依頼を行い、システムの切替／縮退等の準備を行う。例えば、ネットワークから切り離したスタンドアロンでの使用や、紙での運用等が考えられる。

業務委託先との間の連絡体制や委託先と一体となったトラブル対処方法等が明示されるべきである。

具体的項目は、「基本方針の策定」、「発生事象の確認」、「安全確保・安否確認」、および「影響度の確認」である。

③ 業務再開フェーズ

BCP を発動してから、バックアップサイト・手作業などの代替手段により業務を再開し、軌道に乗せるまでフェーズで、代替手段への確実な切り替え、復旧作業の推進、要員などの人的資源のシフト、BCP 遂行状況の確認、BCP 基本方針の見直しがポイントである。

最も緊急度の高い業務（基幹業務）から再開する。

具体的項目は「人的資源の確保」、「代替施設および設備の確保」、「再開／復旧活動の両立」、および「リスク対策によって新たに生じるリスクへの対策」である。

④ 業務回復フェーズ

最も緊急度の高い業務や機能が再開された後、さらに業務の範囲を拡大するフェーズで、代替設備や代替手段を継続する中での業務範囲の拡大となるため、現場の混乱に配慮した慎重な判断がポイントとなる。

具体的項目は「拡大範囲の見極め」、「業務継続の影響確認」、「全面復旧計画の確認」および「制限の確認」である。

⑤ 全面復旧フェーズ

代替設備・手段から平常運用へ切り替えるフェーズで、全面復旧の判断や手続きのミスが新たな業務中断を引き起こすリスクをはらんでおり、慎重な対応が要求される。

具体的項目は「平常運用への切り替えの判断」、「復旧手順の再確認」、「確認事項の整備」および「総括」である。

⑥ BCP の見直し

正常な状態に復帰した後に、BCP に関する問題点や見直しを検討することが必要である。実際の非常事態においては、通常では予想し得ないような事象が起こることも少なくない。実際の対応における成功点、失敗点を率直に評価、反省し、BCP

の見直しを行い、次の非常時に備えることが重要である。

(2) 医療システムの非常時使用への対応

① 非常時用ユーザアカウントの用意

- 停電、火災、洪水への対策と同様に、正常なユーザ認証が不可能な場合の対応が必要である。医療情報システムは使用可能であっても、使用者側の状況が定常時とは著しく違い、正規のアクセス権限者による操作が望めない場合に備えなくてはならない。例えば、ブレークグラスとして知られた方法では、非常時の使用に備えたユーザアカウントを用意し、患者データへのアクセス制限が医療サービス低下を招かないように配慮している。ブレークグラスでは非常時用ユーザアカウントは通常時の明示的な封印、使用状態に入ったことの周知、使用の痕跡を残すこと、定常状態に戻った後は新しい非常時ユーザアカウントへ変更をすることを基本としている。

② 災害時は、通常時とは異なる人の動きが想定される。例えば、災害時は、受付での患者登録を経ないような運用を考慮するなど、必要に応じて非常時の運用に対応した機能を実装すること。

上記の様な非常時使用への対応機能の用意は、関係者に周知され非常時に適切に用いる必要があるが、逆にリスクが増えることに繋がる可能性がある。不用意な使用を行わないために管理・運用は慎重でなくてはならない。

C. 最低限のガイドライン

1. 医療サービスを提供し続けるための BCP の一環として“非常時”と判断する仕組み、正常復帰時の手順を設けること。すなわち、判断するための基準、手順、判断者、をあらかじめ決めておくこと。
2. 正常復帰後に、代替手段で運用した間のデータ整合性を図る規約を用意すること。
3. 非常時の情報システムの運用
   - 「非常時のユーザアカウントや非常時用機能」の管理手順を整備すること。
   - 非常時機能が定常時に不適切に利用されることがないようにし、もし使用された場合には使用されたことが多くの人にわかるようにする等、適切に管理および監査をすること。
   - 非常時用ユーザアカウントが使用された場合、正常復帰後は継続使用が出来ないように変更しておくこと。
4. サイバー攻撃で広範な地域での一部医療行為の停止など医療サービス提供体制に

支障が発生する場合は、別途定める所管官庁への連絡を行うこと。

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

B. 考え方

ここでは、組織の外部と情報交換を行う場合に、個人情報保護およびネットワークのセキュリティに関して特に留意すべき項目について述べる。外部と診療情報等を交換するケースとしては、地域医療連携で医療機関、薬局、検査会社等と相互に連携してネットワークで診療情報等をやり取りする、診療報酬の請求のために審査支払機関等とネットワークで接続する、ASP（Application Service Provider）型のサービスを利用する場合等が考えられる。

外部と医療情報を外部ネットワークを利用して交換する場合、送信元から送信先に確実に情報を送り届ける必要があり、「送付すべき相手に」、「正しい内容を」、「内容を覗き見されない方法で」送付しなければならない。すなわち、送信元の送信機器から送信先の受信機器までの間の通信経路において上記内容を担保する必要があり、送受信データに対する「盗聴」および「改ざん」、ネットワークに対する「侵入」および「妨害」などの脅威から守らなければならない。

ただし、本ガイドラインでは、これら全ての利用シーンを想定するのではなく、ネットワークを通じて医療情報を交換する際のネットワークの接続方式に関して幾つかのケースを想定して記述を行う。また、ネットワークが介在する際の情報交換における個人情報保護とネットワークセキュリティは考え方の視点が異なるため、それぞれの考え方について記述する。

なお、医療機関等が法令による義務の有無に関わらず、個人情報を含む医療情報の保存を外部に委託する場合は、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述を行う。

B-1. 責任分界点の明確化

医療情報を外部に提供することは個人情報保護法上、委託と第三者提供の２種類があり、遵守すべき事項が異なる。

委託の場合、管理責任は提供元医療機関等にあり、契約と監督で管理責任を果たす責務があり、説明責任・結果責任を負わなければならない。提供先機関は契約遵守と報告義務を負う。

第三者提供の場合、提供元は同法第２３条で規定された例外を除き、「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」のⅢ－５－（３）－①のア～エに相当する場合は同ガイドラインで明記された方法で黙示の同意、それ以外の場合は明示の同意を得なければならない。また提供先は同法第１５条、第１６条にしたがって利用目的を特定し、同法および「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」にしたがって個人情報保護を達成する責務を負う。これらの要件を満たして提供された情報に対して提供元は責任を負わない。

オンラインで情報を提供する場合、情報の主体である患者と情報が乖離する。患者と乖離している間は情報を取り扱う事業者のどれかが責任を負う必要があり、どの事業者が責任を負っているかが明確で誤解のないものでなければならない。また患者にとっての苦情の申し入れ先や開示等の要求先が明白でなければならない。

提供元医療機関等、オンラインサービス提供事業者、回線提供事業者、提供先機関または提供先になる可能性がある事業者等が関係事業者になりえる。以下の原則で責任分界点を考える必要がある。

まず、提供元医療機関等と提供先機関は通信経路における責任分界点を定め、不通時や事故発生時の対処も含めて契約などで合意する必要がある。その上で、自らの責任範囲において、オンラインサービス提供事業者や回線提供事業者と管理責任の分担について責任分界点を定め、委託する管理責任の範囲および、サービスに何らかの障害が起こった際の対処をどの事業者が主体となって行うかを明らかにする必要がある。ただし、前述のように結果責任、説明責任は委託の場合は提供元事業者、第三者提供の場合は提供元医療機関等または提供先機関にあり、オンラインサービス提供事業者や回線提供事業者に生じるのは管理責任の一部のみであることに留意する必要がある。

回線事業者の提供する回線の発信元との責任分界点以前に適切に暗号化され、送信先との責任分界点以降に復号される場合は、回線事業者は盗聴の脅威に対する個人情報保護上の責務とは無関係である。ただし、改ざん、侵入、妨害の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は契約で明らかにすること。

オンラインサービス提供事業者の管理範囲の開始される責任分界点に情報が到達する以前に適切に暗号化され、管理範囲の終了する責任分界点以降に復号される場合は、オンラインサービス提供事業者は盗聴の脅威に対する個人情報保護上の責務とは無関係である。ただし、改ざん、侵入、妨害の脅威に対する管理責任の範囲やサービスの可用性等の品質に関しては契約で明らかにすること。

法令で定められている場合などの特別な事情により、オンラインサービス提供事業者および回線提供事業者のいずれかに暗号化されていない医療情報が送信される場合は、オンラインサービスもしくは回線において盗聴の脅威に対する対策を施す必要があるため、当該医療情報の通信経路上の管理責任を負っている医療機関等はオンラインサービス提供事業者もしくは回線提供事業者と医療情報の管理責任についての明確化をおこない、オンラインサービス提供事業者もしくは回線提供事業者に対して管理責任の一部もしくは全部を委託する場合はそれぞれの事業者と個人情報に関する委託契約を適切に締結し、監督しなければならない。

提供元医療機関等と提供先機関が１対１通信である場合、または１対Ｎであってもあらかじめ提供先または提供先となる可能性がある機関を特定できる場合は委託または第三者提供の要件にしたがって両機関等が責務を果たさなければならない。

提供元医療機関等と提供先機関が１対Ｎ通信で、提供先機関が一つでも特定できない場

合は原則として医療情報を提供できない。ただし法令で定められている場合等の例外を除く。

リモートログイン機能を用いたデータアクセスには、代表的用途として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が考えられる。しかし、制限がゆるいと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、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。

B-2. 医療機関等における留意事項

ここでは「B-1. 責任分界点の明確化」で述べた責任の内、ネットワークを通じて診療情報等を含む医療情報を伝送する場合の医療機関等における留意事項を整理する。

まず、医療機関等で強く意識しなくてはならないことは、情報を伝送するまでの医療情報の管理責任は医療機関等にあるということである。これは、情報の送信元である医療機関等から、情報が通信事業者の提供するネットワークを通じ、適切に送信先の医療機関等に受け渡しされるまでの一連の流れ全般において適用される。

ただし、誤解のないように整理しておくべきことは、ここでいう管理責任とは電子的に記載されている情報の内容であり、その記載内容や記載者の正当性の保持（真正性の確保）のことを指す。つまり、後述する「B-3. 選択すべきネットワークのセキュリティの考え方」とは対処すべき方法が異なる。例えば、同じ「暗号化」を施す処置としても、ここで述べている暗号化とは、医療情報そのものに対する暗号化を施す等して、仮に送信元から送信先への通信経路上で通信データの盗聴があっても第三者がその情報を判読できないようにしておく処置のことを指す。また、改ざん検知を行うために電子署名を付与することも対策のひとつである。一方、「B-3. 選択すべきネットワークセキュリティの考え方」で述べる暗号化とはネットワーク回線の経路の暗号化であり、情報の伝送途中で情報を盗み見られない処置を施すことを指す。

このような視点から見れば、医療機関等において情報を送信しようとする場合には、その情報を適切に保護する責任が発生し、次のような点に留意する必要がある。

①「盗聴」の危険性に対する対応

ネットワークを通じて情報を伝送する場合には、この盗聴に最も留意しなくてはならない。盗聴は様々な局面で発生する。例えば、ネットワークの伝送途中で仮想的な迂回路を形成して情報を盗み取ったり、ネットワーク機器に物理的な機材を取り付けて盗み取る等、明らかな犯罪行為であり、必ずしも医療機関等の責任といえない事例も想定される。一方で、不適切なネットワーク機材の設定により、意図しない情報漏洩や誤送信等も想定され、

このような場合には医療機関等における責任が発生する事例も考えられる。

このように様々な事例が考えられる中で、医療機関等においては、万が一、伝送途中で情報が盗み取られたり、意図しない情報漏洩や誤送信等が発生した場合でも、医療情報を保護するために適切な処置を取る必要がある。そのひとつの方法として医療情報の暗号化が考えられる。ここでいう暗号化とは、先に例示した通りであり、情報そのものの暗号化のことを指している。

どの程度の暗号化を施すか、また、どのタイミングで暗号化を施すかについては伝送しようとする情報の機密性の高さや医療機関等で構築している情報システムの運用方法によって異なるため、ガイドラインにおいて一概に規定することは困難ではあるが、少なくとも情報を伝送し、医療機関等の設備から情報が乖離する段階においては暗号化されていることが望ましい。

さらに、この盗聴防止については、例えばIDとパスワードを用いたリモートログインによる保守を実施するような時も同様である。その場合、医療機関等は上記のような留意点を保守委託業者等に確認し、監督する責任を負う。

②「改ざん」の危険性への対応

ネットワークを通じて情報を伝送する場合には、正当な内容を送信先に伝えることも重要な要素である。情報を暗号化して伝送する場合には改ざんへの危険性は軽減するが、通信経路上の障害等により意図的・非意図的要因に係わらず、データが改変されてしまう可能性があることは認識しておく必要がある。

また、後述する「B-3. 選択すべきネットワークセキュリティの考え方」のネットワークの構成によっては、情報を暗号化せずに伝送する可能性も否定できず、その場合には改ざんに対する対処は確実に実施しておく必要がある。なお、改ざんを検知するための方法としては、電子署名を用いる等が想定される。

③「なりすまし」の危険性への対応

ネットワークを通じて情報を伝送する場合、情報を送ろうとする医療機関等は、送信先の医療機関等が確かに意図した相手であるかを確認しなくてはならない。逆に、情報の受け手となる送信先の医療機関等は、その情報の送信元の医療機関等が確かに通信しようとする相手なのか、また、送られて来た情報が確かに送信元の医療機関等の情報であるかを確認しなくてはならない。これは、ネットワークが非対面による情報伝達手段であることに起因するものである。

そのため、例えば通信の起点と終点で医療機関等を適切に識別するために、公開鍵方式や共有鍵方式等の確立された認証の仕組みを用いてネットワークに入る前と出た後で相互に認証する等の対応を取ることが考えられる。また、改ざん防止と併せて、送信元の医療機関等であることを確認するために、医療情報等に対して電子署名を組み合わせることも

考えられる。

また、上記の危険性がサイバー攻撃による場合の対応は「6.9　災害等の非常時の対応」を参照されたい。

B-3. 選択すべきネットワークのセキュリティの考え方

ネットワークを介して外部と医療情報を交換する場合の選択すべきネットワークのセキュリティについては、責任分界点を明確にした上で、医療機関における留意事項とは異なる視点で考え方を整理する必要がある。ここでいうネットワークとは、医療機関等の情報送信元の機関の外部ネットワーク接続点から、同じく医療機関等の情報を受信する機関の外部ネットワーク接続点までのことを指し、医療機関等の内部で構成される LAN は対象とならない。ただし、「B-1. 責任分界点の明確化」でも触れた通り、接続先の医療機関等のネットワーク構成や経路設計によって意図しない情報漏洩が起こる可能性については留意をし、確認をする責務がある。

ネットワークを介して外部と医療情報を交換する際のネットワークを構成する場合、まず、医療機関等としては交換しようとする情報の機密度の整理をする必要がある。「B-2. 医療機関等における留意事項」では情報そのものに対する暗号化について触れているが、同様の観点から、情報の機密度に応じてネットワーク種別も選択しなくてはならない。基本的に医療情報をやり取りする場合、確実なセキュリティ対策は必須であるが、例えば、機密度の高くない情報に対して過度のセキュリティ対策を施すと、高コスト化や現実的でない運用を招く結果となる。つまり、情報セキュリティに対する分析を行った上で、コスト・運用に対して適切なネットワークを選択する必要がある。この整理を実施した上で、ネットワークにおけるセキュリティの責任分界点がネットワークを提供する事業者となるか、医療機関等になるか、もしくは分担となるかを契約等で明らかにする必要がある。その際の考え方としては、大きく次の 2 つに類型化される。

- 回線事業者とオンラインサービス提供事業者がネットワーク経路上のセキュリティを担保する場合

  回線事業者とオンラインサービス提供事業者が提供するネットワークサービスの内、これらの事業者がネットワーク上のセキュリティを担保した形で提供するネットワーク接続形態であり、多くは後述するクローズドなネットワーク接続である。また、現在はオープンなネットワーク接続であっても、Internet-VPN サービスのような通信経路が暗号化されたネットワークとして通信事業者が提供するサービスも存在する。

  このようなネットワークの場合、通信経路上におけるセキュリティに対して医療機関等は最終的な結果責任を負うにせよ、管理責任の大部分をこれらの事業者に委託できる。

  もちろん自らの医療機関等においては、善良なる管理者として注意義務を払い、組織的・物理的・技術的・人的安全管理等の規程に則り自医療機関等のシステムの安全管理を確

認しなくてはならない。

- 回線事業者とオンラインサービス提供事業者がネットワーク経路上のセキュリティを担保しない場合

  例えば、インターネットを用いて医療機関等同士が同意の上、ネットワーク接続機器を導入して双方を接続する方式が考えられる。この場合、ネットワーク上のセキュリティに対して回線事業者とオンラインサービス提供事業者は責任を負わない。そのため、上述の安全管理に加え、導入されたネットワーク接続機器の適切な管理、通信経路の適切な暗号化等の対策を施さなくてはならず、ネットワークに対する正確な知識のない者が安易にネットワークを構築し、医療情報等を脅威にさらさないように万全の対策を実施する必要がある。

  そのため、例えば情報の送信元と送信先に設置される機器や医療機関内に設置されている情報発信端末、端末に導入されている機能、端末の利用者等を確実に確認する手段を確立したり、情報をやり取りする機関同士での情報の取り扱いに関する契約の締結、脅威が発生した際に備えて、通信事業者がネットワーク経路上のセキュリティを担保する場合よりも厳密な運用管理規程の作成、専任の担当者の設置等を考慮しなくてはならない。

このように、医療機関等において医療情報をネットワークを通じて交換しようとする場合には、提供サービス形態の視点から責任分界点のあり方を理解した上でネットワークを選定する必要がある。また、選択するセキュリティ技術の特性を理解し、リスクの受容範囲を認識した上で、必要に応じて説明責任の観点から患者等にもそのリスクを説明する必要がある。

ネットワークの提供サービスの形態は様々存在するため、以降では幾つかのケースを想定して留意点を述べる。

Ⅰ．クローズドなネットワークで接続する場合

ここで述べるクローズドなネットワークとは、業務に特化された専用のネットワーク網のことを指す。この接続の場合、いわゆるインターネットには接続されていないネットワーク網として利用されているものと定義する。このようなネットワークを提供する接続形式としては、「①専用線」、「②公衆網」、「③閉域 IP 通信網」がある。

これらのネットワークは基本的にインターネットに接続されないため、通信上における「盗聴」、「侵入」、「改ざん」、「妨害」の危険性は比較的低い。ただし、「B-2. 医療機関等における留意事項」で述べた物理的手法による情報の盗聴の危険性は必ずしも否定できないため、伝送しようとする情報自体の暗号化については考慮が必要である。また、ウイルス対策ソフトのウイルス定義ファイルや OS のセキュリティパッチ等を適切に適用し、コンピュータシステムの安全性確保にも配慮が必要である。

以下、それぞれの接続方式について特長を述べる。

①専用線で接続されている場合

専用線接続とは、2 地点間においてネットワーク品質を保ちつつ、常に接続されている契約機関専用のネットワーク接続である。通信事業者によってネットワークの品質と通信速度（「帯域」という）等が保証されているため、拠点間を常時接続し大量の情報や容量の大きな情報を伝送するような場合に活用される。

ただし、品質は高いといえるが、ネットワークの接続形態としては拡張性が乏しく、かつ、一般的に高コストの接続形態であるため、その導入にあたってはやり取りされる情報の重要性と情報の量等の兼ね合いを見極める必要もある。

図 B-3-①　専用線で接続されている場合

②公衆網で接続されている場合

公衆網とは ISDN（Integrated Services Digital Network）やダイアルアップ接続など、交換機を介した公衆回線を使って接続する接続形態のことを指す。

ただし、ここで想定する接続先はインターネットサービスプロバイダ（以下、ISP）に接続する接続方法ではなく、情報の送信元が送信先に電話番号を指定して直接接続する方式である。ISP を介して接続する場合は、ISP から先がいわゆるインターネット接続となるため、満たすべき要件としては後述する「Ⅱ．オープンなネットワークで接続する場合」を適用する。

この接続形態の場合、接続先に直接ダイアルしてネットワーク接続を確立するため、ネットワークを確立する前に電話番号を確認する等の仕組みを導入すれば、確実に接続先と通信ができる。

一方で、電話番号を確認する仕組みを用いなかったことによる誤接続、誤送信のリスクや専用線と同様で拡張性が乏しいこと、また、現在のブロードバンド接続と比べ通信速度が遅いため、大量の情報もしくは画像等の容量の大きな情報を送信する際に適用範囲を適切に見定める必要がある。

図 B-3-②　公衆網で接続されている場合

③閉域 IP 通信網で接続されている場合

ここで定義する閉域 IP 通信網とは、通信事業者が保有する広域ネットワーク網と医療機関等に設置されている通信機器とを接続する通信回線が他のネットワークサービス等と共用されていない接続方式を言う。このような接続サービスを本ガイドラインでは IP-VPN（Internet Protocol-Virtual Private Network）と呼び、クローズドなネットワークとして取り扱う。これに適合しない接続形態はオープンなネットワーク接続とする。主な利用形態としては、企業間における本店・支店間での情報共有網を構築する際に、遠隔地も含めた企業内 LAN のように利用され、責任主体が単一のものとして活用されることが多い。

この接続方式は、専用線による接続よりも低コストで導入することができる。また、帯域も契約形態やサービスの種類によっては確保できるため、大量の情報や容量の大きな情報を伝送することが可能である。

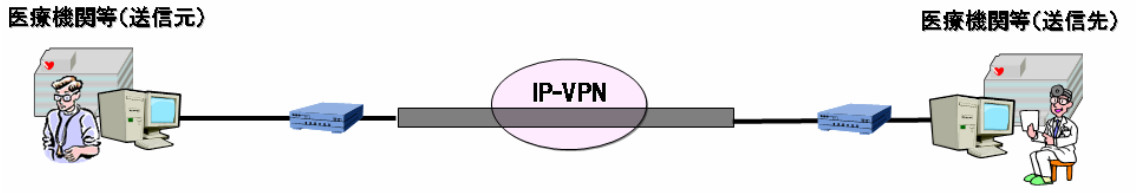


図 B-3-③-a　単一の通信事業者が提供する閉域ネットワークで接続されている場合

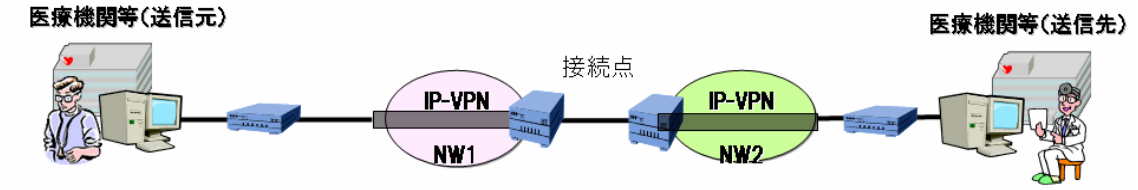


図 B-3-③-b　中間で複数の閉域ネットワークが相互接続して接続されている場合

以上の３つのクローズドなネットワークの接続では、クローズドなネットワーク内では外部から侵入される可能性はなく、その意味では安全性は高い。しかし、接続サービスだけでは一般に送られる情報そのものに対する暗号化は施されていない。また異なる通信事

業者のネットワーク同士が接続点を介して相互に接続されている形態も存在し得る。接続点を介して相互に接続される場合、送信元の情報を送信先に送り届けるために、一旦、送信される情報の宛先を接続点で解釈したり新たな情報を付加したりする場合がある。この際、偶発的に情報の中身が漏示する可能性がないとは言えない。電気通信事業法があり、万が一偶発的に漏示してもそれ以上の拡散は考えられないが、医療従事者の守秘義務の観点からは避けなければならない。そのほか、医療機関等から閉域 IP 通信網に接続する点など、一般に責任分界点上では安全性確保の程度が変化することがあり、特段の注意が必要である。

そのため、クローズドなネットワークを選択した場合であっても、「B-2. 医療機関等における留意事項」に則り、送り届ける情報そのものを暗号化して内容が判読できないようにし、改ざんを検知可能な仕組みを導入するなどの措置を取る必要がある。

Ⅱ. オープンなネットワークで接続されている場合

いわゆるインターネットによる接続形態である。現在のブロードバンドの普及状況から、オープンなネットワークを用いることで導入コストを削減したり、広範な地域医療連携の仕組みを構築したりする等、その利用範囲が拡大して行くことが考えられる。この場合、通信経路上では、「盗聴」、「侵入」、「改ざん」、「妨害」等の様々な脅威が存在するため、十分なセキュリティ対策を実施することが必須である。また、医療情報そのものの暗号化の対策を取らなければならない。

ただし、B-3 の冒頭で述べたように、オープンなネットワークで接続する場合であっても、回線事業者とオンラインサービス提供事業者がこれらの脅威の対策のためネットワーク経路上のセキュリティを担保した形態でサービス提供することもある。医療機関等がこのようなサービスを利用する場合は、通信経路上の管理責任の大部分をこれらの事業者に委託できる。そのため、契約等で管理責任の分界点を明確にした上で利用することも可能である。

一方で、医療機関等が独自にオープンなネットワークを用いて外部と個人情報を含む医療情報を交換する場合は、管理責任のほとんどは医療機関等に委ねられるため、医療機関等の自己責任において導入する必要がある。また、技術的な安全性について自らの責任において担保しなくてはならないことを意味し、その点に留意する必要がある。

オープンなネットワーク接続を用いる場合、ネットワーク経路上のセキュリティの考え方は、「OSI（Open Systems Interconnection）階層モデル※」で定義される 7 階層のうち、どこの階層でセキュリティを担保するかによって異なってくる。OSI 階層モデルを基本としたネットワーク経路上のセキュリティの詳細については「「医療情報システムの安全管理に関するガイドライン」の実装事例に関する報告書（保健・医療・福祉情報セキュアネットワーク基盤普及促進コンソーシアム；HEASNET）；平成 19 年 2 月」が参考になる。

※OSI 階層モデル（Open System Interconneciton）

開放型システム間相互接続のことで、異種間接続を実現する国際標準のプロトコール。

第7層	アプリケーション層	FTPやMail等のサービスをユーザに提供
第6層	プレゼンテーション層	データを人に分かる形式、通信に適した形式に変換
第5層	セッション層	データ経路の確立と開放に関係する層
第4層	トランスポート層	データを確実に届ける為に規定されている層
第3層	ネットワーク層	アドレス管理と経路の選択ための層
第2層	データリンク層	物理的通信経路の確立するために規定されている層
第1層	物理層	ビットデータを電気的、物理的に変換。機器の形状・特性を規定している層

例えば、SSL-VPN を用いる場合、5 階層目の「セッション層」と言われる部分で経路の暗号化手続きがなされるため、正しく経路が暗号化されれば問題ないが、経路を暗号化する過程で盗聴され、適切でない経路を構築されるリスクが内在する。一方、IPSec を用いる場合は、2 階層目もしくは 3 階層目の「ネットワーク層」と言われる部分より下位の層で経路の暗号化手続きがなされるため、SSL-VPN よりは危険度が低いが、経路を暗号化するための暗号鍵の取り交しに IKE（Internet Key Exchange）といわれる標準的手順を組み合わせる等して、確実にその安全性を確保する必要がある。

このように、オープンなネットワーク接続を利用する場合、様々なセキュリティ技術が存在し、内在するリスクも用いる技術によって異なることから、利用する医療機関等においては導入時において十分な検討を行い、リスクの受容範囲を見定める必要がある。多くの場合、ネットワーク導入時に業者等に委託をするが、その際には、リスクの説明を求め、理解しておくことも必要である。

図 B-3-④　オープンネットワークで接続されている場合

（患者等に診療情報等を提供する場合）

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、医療機関等間における情報のやり取りを想定しているが、今後、このような事例も十分想定される。そのため、ここでその際の考え方について触れる。ただし、ここで触れる考え方は、医療機関等が自ら実施して患者等に情報を提供する場合であり、第 8 章で定める診療録及び診療諸記録を外部に保存している場合は、第三者に委託しており、委託

先が情報提供を行うことになるため想定しない。

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洩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 B-1 や B-2 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。

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、正規利用者への成りすまし、許可機器への成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. 医療機関間の情報通信には、当該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。

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）

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 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

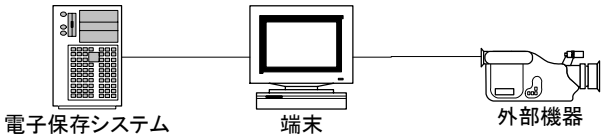
外部機器から送信される記録情報等を一旦電子保存システムの端末に格納し、受信情報の内容の確認と患者属性の付与（必要に応じて）、確認を行い、電子保存システムへ送信し格納する。

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。

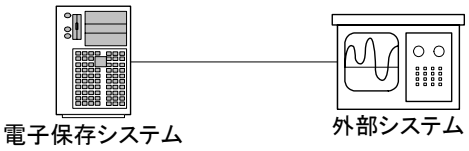
(2－3)　外部システムで確定された情報を取り込み記録する場合

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。
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）

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。

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。

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。

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。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、障害があっ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。

(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は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 **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証できるような互換性のある回線や設備に移行することが望ましい。

8.1.2　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っては、保存に係るホストコンピュータ、サーバ等の情報処理機器が医療法第１条の５第１項に規定する病院又は同条第２項に規定する診療所その他これに準ずるものとして医療法人等が適切に管理する場所に置かれるものであること。」

○「官民の地域医療機関間の有機的な連携を推進すること等が必要な地域等で、診療録等の電子保存を支援することで質の高い医療提供体制を構築することを目的とする場合は、情報管理体制の確保のための一定の安全基準を満たす場合に限り、行政機関等が開設したデータセンター等ついては、オンラインによる外部保存を受託可能とする。」

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

（外部保存改正通知　第２　１（２））

B. 考え方

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り、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、診療を開始するべきである。

患者は自分の個人情報が外部保存されることに同意しない場合は、その旨を申し出なければならない。ただし、診療録等を外部に保存することに同意を得られなかった場合でも、医師法等で定められている診療の応召義務には何ら影響を与えるものではなく、それを理由として診療を拒否することはできない。

② 外部保存終了時の説明

外部保存された診療録等が、予定の期間を経過した後に廃棄等により外部保存の対象から除かれる場合には、診療前の外部保存の了解をとる際に合わせて患者の了解を得ることで十分であるが、医療機関や外部保存先の都合で外部保存が終了する場合や保存先の変更がある場合には、改めて患者の了解を得る必要がある。

③　患者本人に説明をすることが困難であるが、診療上の緊急性がある場合

意識障害や認知症等で本人への説明をすることが困難な場合で、診療上の緊急性がある場合は必ずしも事前の説明を必要としない。意識が回復した場合には事後に説明をし、理解を得ればよい。

④　患者本人の同意を得ることが困難であるが、診療上の緊急性が特にない場合

乳幼児の場合も含めて本人の同意を得ることが困難で、緊急性のない場合は、原則として親権者や保護者に説明し、理解を得る必要がある。親権者による虐待が疑われる場合や保護者がいない等、説明をすることが困難な場合は、診療録等に、説明が困難な理由を明記しておくことが望まれる。

8.1.4　責任の明確化

A. 制度上の要求事項

「外部保存は、診療録等の保存の義務を有する病院、診療所等の責任において行うこと。
また、事故等が発生した場合における責任の所在を明確にしておくこと。」
（外部保存改正通知　第２　１（４））

B. 考え方

診療録等を電気通信回線等を通じて外部に保存する場合であっても、診療録等の真正性、見読性、保存性に関する責任は、保存義務のある医療機関等にある。

ただし、管理責任や説明責任は、実際の管理や説明の一部について、受託先の機関やネットワーク管理者、機器やソフトウェアの製造業者と責任を分担することができ、この場合、一般にネットワークで結合されたシステムでは管理境界や責任限界が自明でない場合が多いことから、文書等により、その責任分担を明確にしなければならない。

結果責任は、患者に対しては委託元の医療機関等が負うが、受託先の機関やこれらの機関と契約した電気通信回線提供事業者、機器やソフトウェアの製造業者は、委託元の医療機関等に対して契約等で定められた責任を負うことは当然であり、法令に違反した場合はその責任も負うことになる。

なお、これら責任分界点の考え方については、「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-1. 責任分界点の明確化」も併せて参照されたい。

C. 最低限のガイドライン

(1) 電子保存の 3 条件に対する責任

①　管理責任を明確にすること

媒体への記録や保存、伝送等に用いる装置の選定、導入、及び利用者を含めた運用及び管理等に関する責任については、委託元の医療機関等が主体になって対応するという前提で、個人情報の保護について留意しつつ、実際の管理を、外部保存を受託する機関や、これらの機関と契約した電気通信回線提供事業者、機器やソフトウェアの製造業者に行わせてもよい。

②　説明責任を明確にすること

外部保存の目的や利用者を含めた保存システムの管理運用体制等について、患者や社会に対して十分に説明する責任については、委託元の医療機関等が主体になって対応する必要がある。この際、個人情報の保護について留意しつつ、運用体制に関する実際の説明については、外部保存を受託する機関や、これらの契約先の電気通信回線提供事業者、機器やソフトウェアの製造業者にさせてもよい。

③ 結果責任を明確にすること

電気通信回線を通じて伝送し、外部保存を行った結果に対する責任は、患者に対しては、委託元の医療機関等が負うものである。ただし、委託元と受託先の機関や電気通信回線提供事業者等の間の契約事項に関しては、受託先の機関や、これらの機関と契約した電気通信回線提供事業者等が、委託元の医療機関等に対して責任を負う必要があり、法令に違反した場合はその責任も負う。

(2) 通信経路の各課程における責任の所在の明確化

診療録等の外部保存に関する委託元の医療機関等、受託先の機関及び電気通信回線提供者の間で、次の事項について管理･責任体制を明確に規定して、契約等を交わすこと。

- 委託元の医療機関等で発生した診療録等を、受託先の機関に保存するタイミングの決定と一連の外部保存に関連する操作を開始する動作
- 委託元の医療機関等が電気通信回線に接続できない場合の対処
- 受託先の機関が電気通信回線に接続できなかった場合の対処
- 電気通信回線の経路途中が不通または著しい遅延の場合の対処
- 受託先の機関が受け取った保存情報を正しく保存できなかった場合の対処
- 委託元の医療機関等が、受託先の機関内の保存情報を検索できなかった場合及び返送処理の指示が不成功であった場合の対処
- 委託元の医療機関等の操作とは無関係に、受託先の機関のシステムに何らかの異常があった場合の対処
- 受託先の機関内でやむを得ず個人情報にアクセスしなくてはならなくなった場合の委託元の医療機関等への承認を求める手続き事項、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委託元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
- 伝送情報の暗号化に不具合があった場合の対処
- 委託元の医療機関等と受託先の機関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
- 委託元の医療機関等による受託先の機関における外部保存の取扱いについて監督する方法
- 外部保存の受託先の機関に、患者から直接、照会や苦情、開示の要求があった場合の処置
- 委託元の医療機関等または受託先の機関が、外部保存を中止する場合の対処
- 外部保存に関する契約終了後の診療録等の扱いの取り決め

8.1.5　留意事項

電気通信回線を通じて外部保存を行い、これを受託先の機関において可搬型媒体に保存する場合にあっては、「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」に掲げる事項についても十分留意すること。

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

可搬型媒体に電子的に保存した情報を外部に保存する場合、委託元の医療機関等と受託先の機関はオンラインで結ばれないために、なりすましや盗聴、改ざん等による情報の大量漏洩や大幅な書換え等、電気通信回線上の脅威に基づく危険性は少なく、注意深く運用すれば真正性の確保は容易になる可能性がある。

可搬型媒体による保存の安全性は、紙やフィルムによる保存の安全性と比べておおむね優れているといえる。媒体を目視しても内容が見えるわけではないので、搬送時の機密性は比較的確保しやすい。セキュリティ MO 等のパスワードによるアクセス制限が可能な媒体を用いればさらに機密性は増す。

従って、一般的には次節の紙媒体による外部保存の基準に準拠していれば大きな問題はないと考えられる。しかしながら、可搬型媒体の耐久性の経年変化については、今後とも慎重に対応していく必要があり、また、媒体あたりに保存される情報量が極めて多いことから、媒体が遺失した場合に、紛失したり、漏洩する情報量も多くなるため、より慎重な取扱いが必要と考えられる。

なお、診療録等のバックアップ等、法令で定められている保存義務を伴わない文書を外部に保存する場合についても、個人情報保護の観点からは保存義務のある文書と同等に扱うべきである。

8.2.1　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

診療録等を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おおむね対応が可能と考えられるが、これに加え、搬送時や外部保存の受託先の機関における取扱いや事故発生時について、特に注意する必要がある。

具体的には、以下についての対応が求められる。

(1) 搬送時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
(2) 搬送時や外部保存を受託する機関の障害等に対する見読性の確保
(3) 搬送時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

C. 最低限のガイドライン

(1) 搬送時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 委託元の医療機関等、搬送業者及び受託機関における可搬型媒体の授受記録を行うこと。

可搬型媒体の授受及び保存状況を確実にし、事故､紛失や窃盗を防止することが必要である。また、他の保存文書等との区別を行うことにより、混同を防止しなければならない。

② 媒体を変更したり､更新したりする際に、明確な記録を行うこと

(2) 搬送時や外部保存を受託する機関の障害等に対する見読性の確保

① 診療に支障がないようにすること

患者の情報を可搬型媒体で外部に保存する場合、情報のアクセスに一定の搬送時間が必要であるが、患者の病態の急変や救急対応等に備え、緊急に診療録等の情報が必要になる場合も想定しておく必要がある。

一般に「診療のために直ちに特定の診療情報が必要な場合」とは、継続して診療を行っている場合であることから、継続して診療をおこなっている場合で、患者の診療情報が緊急に必要になることが予測され、搬送に要する時間が問題になるような診療に関する情報は、あらかじめ内部に保存するか、外部に保存しても、保存情報の複製またはそれと実質的に同等の内容を持つ情報を委託元の医療機関等の内部に保存しておかなければならない。

② 監査等に差し支えないようにすること

監査等は概ね事前に予定がはっきりしており、緊急性を求められるものではないことから、搬送に著しく時間を要する遠方に外部保存しない限りは問題がないと考えられる。

(3) 搬送時や外部保存を受託する機関の障害等における保存性の確保

① 標準的なデータ形式の採用

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 媒体の劣化対策

媒体の保存条件を考慮し、例えば、磁気テープの場合､定期的な読み書きを行う等の劣化対策が必要である。

③　媒体及び機器の陳腐化対策

媒体や機器が陳腐化した場合、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、媒体や機器の陳腐化に対応して、新たな媒体または機器に移行することが望ましい。

8.2.2　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、可搬媒体を用い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、外部保存の受託先の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。

具体的には、以下についての対応が求められる。

(1) 診療録等の記録された可搬型媒体が搬送される際の個人情報保護
(2) 診療録等の外部保存を受託する機関内における個人情報保護

C. 最低限のガイドライン

(1) 診療録等の記録された可搬型媒体が搬送される際の個人情報保護

診療録等を可搬型媒体に記録して搬送する場合は、なりすましや盗聴、改ざん等による情報の大量漏洩や大幅な書換え等、電気通信回線上の脅威に基づく危険性は少ないが、一方、可搬型媒体の遺失や他の搬送物との混同について、注意する必要がある。

- 診療録等を記録した可搬型媒体の遺失防止
- 運搬用車両を施錠したり、搬送用ケースを封印する等の処置を取ることによって、遺失の危険性を軽減すること。
- 診療録等を記録した可搬型媒体と他の搬送物との混同の防止
- 他の搬送物との混同が予測される場合には、他の搬送物と別のケースや系統に分けたり、同時に搬送しないことによって、その危険性を軽減すること。

・ 搬送業者との守秘義務に関する契約
・ 外部保存を委託する医療機関等は保存を受託する機関、搬送業者に対して個人情報保護法を順守させる管理義務を負う。従って両者の間での責任分担を明確化するとともに、守秘義務に関する事項等を契約上明記すること。

(2) 診療録等の外部保存を受託する機関内における個人情報保護

受託先の機関が、委託元の医療機関等からの求めに応じて、保存を引き受けた診療録等における個人情報を検索し、その結果等を返送するサービスを行う場合や、診療録等の記録された可搬型媒体の授受を記録する場合、受託先の機関に障害の発生した場合等に、診療録等にアクセスをする必要が発生する可能性がある。このような場合には、次の事項に注意する必要がある。

① 外部保存を受託する機関における医療情報へのアクセスの禁止

診療録等の外部保存を受託する機関においては、診療録等の個人情報の保護を厳格に行う必要がある。受託先の機関の管理者であっても、受託した個人情報に、正当な理由なくアクセスできない仕組みが必要である。

② 障害発生時のアクセス通知

診療録等を保存している設備に障害が発生した場合等で、やむをえず診療録等にアクセスをする必要がある場合も、医療機関等における診療録等の個人情報と同様の秘密保持を行うと同時に、外部保存を委託した医療機関等に許可を求めなければならない。

③ 外部保存を受託する機関との守秘義務に関する契約

診療録等の外部保存を受託する機関は、法令上の守秘義務を負っていることからも、委託元の医療機関等と受託先の機関、搬送業者との間での責任分担を明確化するとともに、守秘義務に関する事項等を契約に明記する必要がある。

④ 外部保存を委託する医療機関等の責任

診療録等の個人情報の保護に関する責任は、最終的に、診療録等の保存義務のある委託元の医療機関等が責任を負わなければならない。従って、委託元の医療機関等は、上記の受託先の機関における個人情報の保護の対策が実施されることを契約等で要請し、その実施状況を監督する必要がある。

D. 推奨されるガイドライン

C の最低限のガイドラインに加えて以下の対策をおこなうこと。

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医療機関等は、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機関に送られ、保存されることについて、その安全性やリスクを含めて院内掲示等を通じて説明し、理解を得る必要がある。

① 診療開始前の説明

患者から、病態、病歴等を含めた個人情報を収集する前に行われるべきであり、外部保存を行っている旨を院内掲示等を通じて説明し理解を得た上で、診療を開始するべきである。

患者は自分の個人情報が外部保存されることに同意しない場合は、その旨を申し出なければならない。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、医療機関等や外部保存先の都合で外部保存が終了する場合や保存先の変更がある場合には、改めて患者の了解を得る必要がある。

③ 患者本人に説明をすることが困難であるが、診療上の緊急性がある場合

意識障害や認知症等で本人への説明をすることが困難な場合で、診療上の緊急性がある場合は必ずしも事前の説明を必要としない。意識が回復した場合には事後に説明をし、理解を得ればよい。

④ 患者本人の同意を得ることが困難であるが、診療上の緊急性が特にない場合

乳幼児の場合も含めて本人の同意を得ることが困難で、緊急性のない場合は、原則として親権者や保護者に説明し、理解を得る必要がある。親権者による虐待が疑われる場合や保護者がいない等、説明をすることが困難な場合は、診療録等に、説明が困難な理由を明記しておくことが望まれる。

8.2.3　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））

B. 考え方

診療録等を電子的に記録した可搬型媒体で外部の機関に保存する場合であっても、診療録等の真正性、見読性、保存性に関する責任は保存義務のある医療機関等にある。

管理責任や説明責任については、実際の管理や部分的な説明の一部を受託先の機関や搬送業者との間で責任を分担することについて問題がないと考えられる。

また、結果責任については、患者に対する責任は、委託元の医療機関等が負うものであるが、受託先の機関や搬送業者等は、委託元の医療機関等に対して、契約等で定められた責任を負うことは当然であるし、法令に違反した場合はその責任も負うことになる。

具体的には、以下についての対応が求められる。

(1) 電子保存の 3 条件に対する責任の明確化
(2) 事故等が発生した場合における責任の所在

C. 最低限のガイドライン

(1) 電子保存の 3 条件に対する責任の明確化

①　管理責任

媒体への記録や保存等に用いる装置の選定、導入、及び利用者を含めた運用及び管理等に関する責任については、委託元の医療機関等が主体になって対応するという前提で、個人情報の保護について留意しつつ、実際の管理を、搬送業者や受託先の機関に行わせることは問題がない。

②　説明責任

利用者を含めた保存システムの管理運用体制について、患者や社会に対して十分に説明する責任については、委託元の医療機関等が主体になって対応するという前提で、個人情報の保護について留意しつつ、実際の説明を、搬送業者や受託先の機関にさせることは問題がない。

③　結果責任

可搬型媒体で搬送し、外部保存を行った結果に対する責任は、患者に対しては、委託元の医療機関等が負うものである。ただし、委託元の医療機関等と受託先の機関ま

たは搬送業者の間の契約事項に関しては、受託先の機関や搬送業者等が、委託元の医療機関等に対して責任を負う必要があり、法令に違反した場合はその責任も負うことになる。

(2) 事故等が発生した場合における責任の所在

診療録等を外部保存に関する委託元の医療機関等、受託先の機関及び搬送業者の間で、次の事項について管理・責任体制を明確に規定して、契約等を交わすこと。

- 委託元の医療機関等で発生した診療録等を、外部機関に保存するタイミングの決定と一連の外部保存に関連する操作を開始する動作
- 委託元の医療機関等と搬送（業）者で可搬型媒体を授受する場合の方法と管理方法
- 事故等で可搬型媒体の搬送に支障が生じた場合の対処方法
- 搬送中に秘密漏洩があった場合の対処方法
- 受託先の機関と搬送（業）者で可搬型媒体を授受する場合の方法と管理方法
- 受託先の機関で個人情報を用いた検索サービスを行う場合、作業記録と監査方法、取扱い従業者等の退職後も含めた秘密保持に関する規定、秘密漏洩に関して患者からの照会があった場合の責任関係
- 受託先の機関が、委託元の医療機関等の求めに応じて可搬型媒体を返送することができなくなった場合の対処方法
- 外部保存の受託先の機関に、患者から直接、照会や苦情、開示の要求があった場合の対処方法

8.3　紙媒体のままで外部保存を行う場合

紙媒体とは、紙だけを指すのではなく、X線フィルム等の電子媒体ではない物理媒体も含む。検査技術の進歩等によって、医療機関等では保存しなければならない診療録等が増加しており、その保存場所の確保が困難な場合も多い。本来、法令に定められた診療録等の保存は、証拠性と同時に、有効に活用されることを目指すものであり、整然と保存されるべきものである。

一定の条件の下では、従来の紙媒体のままの診療録等を当該医療機関等以外の場所に保存することが可能になっているが、この場合の保存場所も可搬型媒体による保存と同様、医療機関等に限定されていない。

しかしながら、診療録等は機密性の高い個人情報を含んでおり、また必要な時に遅滞なく利用できる必要がある。保存場所が当該医療機関等以外になることは、個人情報が存在する場所が拡大することになり、外部保存に係る運用管理体制を明確にしておく必要がある。また保存場所が離れるほど、診療録等を搬送して利用可能な状態にするのに時間がかかるのは当然であり、診療に差し障りのないように配慮しなければならない。

さらに、紙やフィルムの搬送は注意深く行う必要がある。可搬型媒体は内容を見るために何らかの装置を必要とするが、紙やフィルムは単に露出するだけで、個人情報が容易に漏出するからである。

8.3.1　利用性の確保

A. 制度上の要求事項

「診療録等の記録が診療の用に供するものであることにかんがみ、必要に応じて直ちに利用できる体制を確保しておくこと。」
（外部保存改正通知　第２　２（１））

B. 考え方

一般に、診療録等は、患者の診療や説明、監査、訴訟等のために利用するが、あらゆる場合を想定して、診療録等をいつでも直ちに利用できるようにすると解釈すれば、事実上、外部保存は不可能となる。

診療の用に供するという観点から考えれば、直ちに特定の診療録等が必要な場合としては、継続して診療を行っている患者等、緊急に必要になることが容易に予測される場合が挙げられる。具体的には、以下ついての対応が求められる。

(1) 診療録等の搬送時間
(2) 保存方法及び環境

C. 最低限のガイドライン

(1) 診療録等の搬送時間

外部保存された診療録等を診療に用いる場合、搬送の遅れによって診療に支障が生じないようにする対策が必要である。

① 外部保存の場所

搬送に長時間を要する機関に外部保存を行わないこと。

② 複製や要約の保存

継続して診療をおこなっている場合等で、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、外部に保存する場合でも、診療に支障が生じないようコピーや要約等を内部で利用可能にしておくこと。

また、継続して診療している場合であっても、例えば入院加療が終了し、適切な退院時要約が作成され、それが利用可能であれば、入院時の診療録等自体が緊急に必要になる可能性は低下する。ある程度時間が経過すれば外部に保存しても診療に支障をきたすことはないと考えられる。

(2) 保存方法及び環境

① 診療録等の他の保存文書等との混同防止

診療録等を必要な利用単位で選択できるよう、他の保存文書等と区別して保存し、管理しなければならない。

② 適切な保存環境の構築

診療録等の劣化、損傷、紛失、窃盗等を防止するために、適切な保存環境・条件を構築・維持しなくてはならない。

8.3.2 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　２（２））

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、紙やフィルム等の媒体のままで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、外部保存の受託先の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。

具体的には、以下についての対応が求められる。

(1) 診療録等が搬送される際の個人情報保護
(2) 診療録等の外部保存を受託する機関内における個人情報保護

C. 最低限のガイドライン

(1) 診療録等が搬送される際の個人情報保護

診療録等の搬送は遺失や他の搬送物との混同について、注意する必要がある。

① 診療録等の封印と遺失防止

診療録等は、目視による情報の漏出を防ぐため、運搬用車両を施錠したり、搬送用ケースを封印すること。また、診療録等の授受の記録を取る等の処置を取ることによって、その危険性を軽減すること。

② 診療録等の搬送物との混同の防止

他の搬送物との混同が予測される場合には、他の搬送物と別のケースや系統に分けたり、同時に搬送しないことによって、危険性を軽減すること。

③　搬送業者との守秘義務に関する契約

診療録等を搬送する業者は、「個人情報保護法」が成立し、法令上の守秘義務を負うことからも、委託元の医療機関等と受託先の機関、搬送業者の間での責任分担を明確化するとともに、守秘義務に関する事項等を契約上、明記すること。

(2) 診療録等の外部保存を受託する機関内における個人情報保護

診療録等の外部保存を受託する機関においては、依頼元の医療機関等からの求めに応じて、診療録等の検索を行い、必要な情報を返送するサービスを実施する場合、また、診療録等の授受の記録を取る場合等に、診療録等の内容を確認したり、患者の個人情報を閲覧する可能性が生じる。

①　外部保存を受託する機関内で、患者の個人情報を閲覧する可能性のある場合

診療録等の外部保存を受託し、検索サービス等を行う機関は、サービスの実施に最小限必要な情報の閲覧にとどめ、その他の情報は、閲覧してはならない。また、情報を閲覧する者は特定の担当者に限ることとし、その他の者が閲覧してはならない。

さらに、外部保存を受託する機関は、個人情報保護法による安全管理義務の面から、委託元の医療機関等と受託先の機関、搬送業者の間で、守秘義務に関する事項や、支障があった場合の責任体制等について、契約を結ぶ必要がある。

②　外部保存を受託する機関内で、患者の個人情報を閲覧する可能性のない場合

診療録等の外部保存を受託する機関は、もっぱら搬送ケースや保管ケースの管理のみを実施すべきであり、診療録等の内容を確認したり、患者の個人情報を閲覧してはならない。また、これらの事項について、委託元の医療機関等と受託先の機関、搬送業者の間で契約を結ぶ必要がある。

③　外部保存を委託する医療機関等の責任

診療録等の個人情報の保護に関する責任は、最終的に、診療録等の保存義務のある委託元の医療機関等が責任を負わなければならない。従って、委託元の医療機関等は、上記の受託先の機関における個人情報の保護の対策が実施されることを契約等で要請し、その実施状況を監督する必要がある。

D. 推奨されるガイドライン

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医療機関等は、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機関に送られ、保存されることについて、その安全性やリスクを含めて院内掲示等を通じて説明し、理解を得る必要がある。

① 診療開始前の説明

患者から、病態、病歴等を含めた個人情報を収集する前に行われるべきであり、外部保存を行っている旨を院内掲示等を通じて説明し理解を得た上で、診療を開始するべきである。患者は自分の個人情報が外部保存されることに同意しない場合は、その旨を申し出なければならない。

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、医療機関等や外部保存先の都合で外部保存が終了する場合や保存先の変更がある場合には、改めて患者の了解を得る必要がある。

③ 患者本人に説明をすることが困難であるが、診療上の緊急性がある場合

意識障害や認知症等で本人への説明をすることが困難な場合で、診療上の緊急性がある場合は必ずしも事前の説明を必要としない。意識が回復した場合には事後に説明をし、理解を得ればよい。

④ 患者本人の同意を得ることが困難であるが、診療上の緊急性が特にない場合

乳幼児の場合も含めて本人の同意を得ることが困難で、緊急性のない場合は、原則として親権者や保護者に説明し、理解を得る必要がある。親権者による虐待が疑われる場合や保護者がいない等、説明をすることが困難な場合は、診療録等に、説明が困難な理由を明記しておくことが望まれる。

8.3.3　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　２（３））

B. 考え方

診療録等を外部の機関に保存する場合であっても、診療録等の保存に関する責任は保存義務のある医療機関等にある。

管理責任や説明責任については、実際の管理や部分的な説明の一部を受託先の機関や搬送業者との間で責任を分担することで問題がないと考えられる。

また、結果責任については、患者に対する責任は委託元の医療機関等が負うものであるが、受託先の機関や搬送業者等は、委託元の医療機関等に対して、契約等で定められた責任を負うことは当然であるし、法令に違反した場合はその責任も負うことになる。

具体的には、以下についての対応が求められる。

(1) 責任の明確化
(2) 事故等が発生した場合における責任の所在

C. 最低限のガイドライン

(1) 責任の明確化

①　管理責任

診療録等の外部保存の運用及び管理等に関する責任については、委託元の医療機関等が主体になって対応するという前提で、個人情報の保護について留意しつつ、実際の管理を、搬送業者や受託先の機関に行わせることは問題がない。

②　説明責任

利用者を含めた管理運用体制について、患者や社会に対して十分に説明する責任については委託元の医療機関等が主体になって対応するという前提で、個人情報の保護について留意しつつ、実際の説明を、搬送業者や受託先の機関にさせることは問題がない。

③　結果責任

診療録等を搬送し、外部保存を行った結果に対する責任は、患者に対しては、委託元の医療機関等が負うものである。ただし、委託元の医療機関等と受託先の機関や搬送業者等の間の契約事項に関して、受託先の機関や搬送業者等が、委託元の医療機関

等に対して責任を負う必要があり、法令に違反した場合はその責任も負うことになる。

(2) 事故等が発生した場合における責任の所在

診療録等を外部保存に関する委託元の医療機関等、受託先の機関及び搬送業者の間で、次の事項について管理・責任体制を明確に規定して、契約等を交わすこと。

- 委託元の医療機関等で発生した診療録等を、外部機関に保存するタイミングの決定と一連の外部保存に関連する操作を開始する動作
- 委託元の医療機関等と搬送（業）者で診療録等を授受する場合の方法と管理方法
- 事故等で診療録等の搬送に支障が生じた場合の対処方法
- 搬送中に秘密漏洩があった場合の対処方法
- 受託先の機関と搬送（業）者で診療録等を授受する場合の方法と管理方法。
- 受託先の機関で個人情報を用いた検索サービスを行う場合、作業記録と監査方法
- 取扱い従業者等の退職後も含めた秘密保持に関する規定、秘密漏洩に関して患者から照会があった場合の責任関係
- 受託先の機関が、委託元の医療機関等の求めに応じて診療録等を返送することができなくなった場合の対処方法
- 外部保存の受託先の機関に、患者から直接、照会や苦情、開示の要求があった場合の対処方法

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」の項を参照のこと。

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、委託側の医療機関等及び受託側の機関双方で一定の配慮をしなくてはならない。

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、受託先の機関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くてはならない。また、受託先の機関も、委託先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、処理を行った旨を委託先の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側と受託側で取り交わす契約書にも明記を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。

委託先、受託先双方に厳正な取扱いを求めるのは、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。

〈紙媒体、可搬媒体で保存する場合の留意点〉

紙媒体や可搬型媒体での外部保存する場合は、原則として上記の点に注意すれば大きな問題はない。ただし、患者の個人情報に関する検索サービスを実施している場合は、検索のための台帳やそれに代わるもの、及び検索記録も機密保持できる状態で廃棄しなければならない。

また、委託先、受託先が負う責任は、先に述べた通りであり、紙媒体、可搬媒体で保存しているからという理由で、廃棄に伴う責任を免れるのものではないことには十分留意する必要がある。

〈電気通信回線を通じて外部保存する場合〉

電気通信回線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委託側、受託側が確実に確認できるようにしておかなくてはならない。

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。電子カルテ等へシェ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 ビットのカラースキャン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な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)　外部事業者に委託する場合には、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。したが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 ビットのカラースキャン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 6 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 6 章から 9 章において「推奨」に記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

監査証跡の取組方については、「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

⑤　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

⑥　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

⑦　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

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 外部と医療情報を交換する場合

a) 安全を技術的、運用的面から確認した文書の管理
b) リスク対策の検討文書の管理
c) 責任分界点を定めた契約文書の管理
d) リモートメンテナンスの基本方針

⑩ 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当たっては、本項を参照して「医療機関等としての管理事項」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
受託機関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限定」に記された要件を参照のこと。
b) 委託元での管理責任者
c) 受託機関への監査体制
d) 保存業務受託機関との責任分界点
e) 受託機関の管理責任、説明責任、結果責任の範囲を明文化した契約書等の文書作成と保管
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
受託機関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限定」に記された要件を参照のこと。

② 外部保存契約終了時の処理

受託先に診療録等が残ることがない様な処理法

a) 受託先に診療録等が残ることがないことの受託先との契約、管理者による確認

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) 緊急に必要になることが予測される医療情報の見読性の確保手段

b) 緊急に必要になる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機関での保存確認機能

b) 標準的なデータ形式及び転送プロトコルの採用

＊ 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機関の設備の劣化対策

e) 電気通信回線や外部保存を受託する機関の設備の互換性確保

＊ 上記事項は推奨

f) 情報保護機能

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

受託機関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限定」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

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　受託機関への監査項目

a)　保存記録（内容、期間等）

b)　受託機関側での管理策とその実施状況監査

(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）していかねばならない。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。

付表1　一般管理における運用管理の実施項目例

A：医療機関の規模を問わない
B：大/中規模病院
C：小規模病院、診療所

管理事項番号	運用管理項目	実施項目	対象	技術的対策	運用的対策	運用管理規程文例
①	総則	目的	A		・情報システムの安全管理に関する方針に基づき、本規程の目的を述べる	この規程は、〇〇病院（以下「当病院」という。）において、情報システムで使用される機器、ソフトウェア及び運用に必要な仕組み全般について、その取扱い及び管理に関する事項を定め、当病院において、診療情報を適正に保存するとともに、適正に利用することに資することを目的とする。
		対象	A		・対象者、対象システム、対象情報を定める	・対象者は、情報システムを扱う全ての利用者である。 ・対象システムは、電子カルテシステム、オーダエントリシステム、画像管理システム、・・・である。 ・対象情報は、全ての診療に関する情報である。
②	管理体制	システム管理者、運用責任者の任命	B		・システム管理者の任命規程 ・運用責任者の任命規程 ・運営管理委員会の設置	・当病院に情報システム管理者を置き、病院長をもってこれに充てること。 ・病院長は必要な場合、情報システム管理者を別に指名すること。 ・情報システムを円滑に運用するため、情報システムに関する運用を担当する責任者（以下「運用責任者」という。）を置くこと。 ・運用責任者は病院長が指名すること。 ・情報システムに関する取扱い及び管理に関し必要な事項を審議するため、病院長のもとに情報システム管理委員会を置くこと。 ・情報システム管理委員会の運営については、別途定めること。 ・その他、この規程の実施に関し必要な事項がある場合については、情報システム管理委員会の審議を経て、病院長がこれを定めること。
			C		・院長がシステム管理者と運用責任者を兼ねる場合、その旨を明記する	・当クリニックに情報システム管理者を置き、院長をもってそれに充てること。 ・院長は必要な場合、情報システム管理者を別に指名すること。
		作業担当者の限定	A		・作業担当者の限定を規定する	・本規程が対象とする業務に携わる担当者は別表に定める通りとする。[別表に任務と担当者名を記載する]
		契約書・マニュアル等の文書管理	A		・別途定めてある文書管理規程に従うことを規定する	・契約書、マニュアル等の文書の管理については、別途規程を定めること。
		監査体制と監査責任者の任命	B		・監査体制（監査の周期、監査結果の評価・対応等）を規程 ・監査責任者の任命規程	・情報システムを円滑に運用するため、情報システムに関する監査を担当する責任者（以下「監査責任者」という。）を置くこと。 ・監査責任者の責務は本規程に定めるものの他、別に定めること。 ・監査責任者は病院長が指名すること。 ・情報システム管理者は、監査責任者に毎年4回、情報システムの監査を実施させ、監査結果の報告を受け、問題点の指摘等がある場合には、直ちに必要な措置を講じること。 ・監査の内容については、情報システム管理委員会の審議を経て、病院長がこれを定めること。 ・情報システム管理者は必要な場合、臨時の監査を監査責任者に命ずること。
			C		・院内で監査体制を整えることができない場合、第三者監査機関への監査依頼を規定する	・電子保存システムの監査をXXXとの契約により毎年4回行い、監査結果の報告を受け、問題点の指摘等がある場合には、直ちに必要な措置を講じること。

		問合せ・苦情の受付窓口の設置	A		・患者あるいは利用者からの問合せ・苦情受付窓口の設置 ・受付後の処置を規定	・患者又は利用者からの、情報システムについての問合せ・苦情を受け付ける窓口を設けること。 ・苦情受け付け後は、その内容を検討し、直ちに必要な措置を講じること。
		事故対策	A		・緊急時あるいは災害時の連絡、復旧体制並びに回復手段を規定する	・情報システム管理者は、緊急時及び災害時の連絡、復旧体制並びに回復手順を定め、非常においても参照できるような媒体に保存し保管すること。
		利用者への周知法	A		・各種規程書、指示書、取扱説明書等の作成 ・定期的な利用者への教育、訓練	・情報システム管理者は、情報システムの取扱いについてマニュアルを整備し、利用者に周知の上、常に利用可能な状態におくこと。 ・情報システム管理者は、情報システムの利用者に対し、定期的に情報システムの取扱い及びプライバシー保護に関する研修を行うこと。
③	管理者及び利用者の責務	システム管理者や運用責任者の責務	A		・機器、ソフトウェア導入時の機能確認 ・運用環境の整備と維持 ・情報の安全性の確保と利用可能な状況の維持 ・情報の継続的利用の維持 ・不正利用の防止 ・利用者への教育、訓練 ・患者または利用者からの問合せ・苦情窓口設置	・情報システムに用いる機器及びソフトウェアを導入するに当たって、システムの機能を確認すること。 ・情報システムの機能要件に挙げられている機能が支障なく運用される環境を整備すること。 ・診療情報の安全性を確保し、常に利用可能な状態に置いておくこと。 ・機器やソフトウェアに変更があった場合においても、情報が継続的に使用できるよう維持すること。 ・管理者は情報システムの利用者の登録を管理し、そのアクセス権限を規定し、不正な利用を防止すること。 ・情報システムを正しく利用させるため、作業手順書の整備を行い利用者の教育と訓練を行うこと。 ・患者又は利用者からの、情報システムについての苦情を受け付ける窓口を設けること。
		監査責任者の責務	B		・監査責任者の役割、責任、権限を規定	・情報システムを円滑に運用するため、情報システムに関する監査を担当する責任者（以下「監査責任者」という。）を置くこと。 ・監査責任者の責務は本規程に定めるものの他、別に定めること。
			C		・第三者機関へ監査依頼している場合は、監査実施規定は不要 ・監査結果に対する対応を規定	・情報システムの監査をXXXとの契約により毎年4回行い、監査結果の報告を受け、問題点の指摘等がある場合には、直ちに必要な措置を講じること。
		利用者の責務	B		・自身の認証番号やパスワードあるいはICカード等の管理 ・利用時にシステム認証を必ず受けること ・確定操作の実施による入力情報への責任の明示 ・権限を超えたアクセスの禁止 ・目的外利用の禁止 ・プライバシー侵害への配慮 ・システム異常、不正アクセスを発見した場合の速やかな運用管理者へ通知	・利用者は、自身の認証番号やパスワードを管理し、これを他者に利用させないこと。 ・利用者は、情報システムの情報の参照や入力（以下「アクセス」という。）に際して、認証番号やパスワード等によって、システムに自身を認識させること。 ・利用者は、情報システムへの情報入力に際して、確定操作（入力情報が正しい事を確認する操作）を行って、入力情報に対する責任を明示すること。 ・利用者は、与えられたアクセス権限を越えた操作を行わないこと。 ・利用者は、参照した情報を、目的外に利用しないこと。 ・利用者は、患者のプライバシーを侵害しないこと。 ・利用者は、システムの異常を発見した場合、速やかに運用責任者に連絡し、その指示に従うこと。 ・利用者は、不正アクセスを発見した場合、速やかに運用責任者に連絡し、その指示に従うこと。

			C		・利用者が限定される運用の場合、その旨を明記し、責任の所在を明確にする。 ・目的外利用の禁止 ・プライバシー侵害への配慮 ・システム異常時の対応を規定	・利用者は、XXX、XXX、XXXである。 ・利用者は、参照した情報を、目的外に利用しないこと。 ・利用者は、患者のプライバシーを侵害しないこと。 ・利用者は、システムの異常を発見した場合、速やかに運用責任者に連絡し、その指示に従うこと。 ・利用者は、不正アクセスを発見した場合、速やかに運用責任者に連絡し、その指示に従うこと。
④	一般管理における運用管理事項	入退者の記録・識別、入退の制限などの入退管理	B	・IDカード利用による入退者の制限、名札着用の実施 ・PCの盗難防止チェインの設置 ・防犯カメラの設置 ・施錠	・入退者の名簿記録と妥当性チェックなどの定期的チェック	・個人情報が保管されている機器の設置場所及び記録媒体の保存場所への入退者は名簿に記録を残すこと。 ・入退出の記録の内容について定期的にチェックを行うこと。
			C	技術的対策なし	・入退者の名簿記録と妥当性チェックなどの定期的チェック	・個人情報が保管されている機器の設置場所及び記録媒体の保存場所への入退者は名簿に記録を残すこと。 ・入退出の記録の内容について定期的にチェックを行うこと。
		情報システムへのアクセス制限、記録、点検等のアクセス管理	B	・ID、パスワード等により診療録データへのアクセスにおける識別と認証を行う ・監査ログサーバを設置し、アクセスログの収集を行う。	・管理規則に則ったハードウェア・ソフトウェアの設定を行う ・アクセスできる診療録等の範囲を定め、そのレベルに沿ったアクセス管理を行う ・誰が、いつ、誰の情報にアクセスしたかを記録し、定期的な記録の確認を行う	・システム管理者は、職務により定められた権限によるデータアクセス範囲を定め、必要に応じてハードウェア・ソフトウェアの設定を行う。また、その内容に沿って、アクセス状況の確認を行い、監査責任者に報告をする。
			C	技術的対策なし	システム操作業務日誌を備え、システムを操作するものはシステム操作業務日誌に操作者氏名、作業開始時間、作業終了時間、作業内容、作業対象を記載する。 システム管理者は定期的にシステム操作業務日誌をチェックし、記載内容の正当性を確認する。	システム管理者はシステム操作業務日誌を設置する。 システム操作者はシステム操作をおこなった場合、操作者氏名、作業開始時間、作業終了時間、作業内容、作業対象を記載する。 システム管理者は定期的にシステム操作業務日誌をチェックし、記載内容の正当性を評価する。
		個人情報の記録媒体の管理（保管・授受等）	A	・個人情報の記録媒体は、空調等が完備された安全な部屋で保管する。 ・媒体の劣化を考慮し、定期的なバックアップを行う。	・保管、バックアップ作業を的確に行う。	・保管、バックアップの作業に当たる者は、手順に従い行い、その作業の記録を残し、責任者の承認をうること。
		個人情報を含む媒体の廃棄の規程	A	・技術的に安全（再生不可）な方式で破棄を行う	・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事者の特定、具体的な破棄の方法を含めること。	・個人情報を記した媒体の廃棄に当たっては、安全かつ確実に行われることを、システム管理者が作業前後に確認し、結果を記録に残すこと。
		リスクに対する予防、発生時の対応	A		・情報に対する脅威を洗い出し、そのリスク分析の結果に対し予防対策を行う。 ・リスク発生時の連絡網、対応、代替手段などを規定する	・情報システム管理者は、業務上において情報漏えいなどのリスクが予想されるものに対し、運用規程の見直しを行う。また、事故発生に対しては、速やかに責任者に報告すること周知する。
⑤	教育と訓練	マニュアルの整備	A		・マニュアルの整備	・システム管理者は、情報システムの取扱いについてマニュアルを整備し、利用者に周知の上、常に利用可能な状態におくこと。 ・システム管理者は、情報システムの利用者に対し、定期的に情報システムの取扱い及びプライバシー保護に関する研修を行うこと。また、研修時のテキスト、出席者リストを残すこと。

		定期または不定期なシステムの取り扱い及びプライバシー保護に関する研修	A		・定期または不定期な電子保存システムの取扱及びプライバシー保護に関する教育、研修	
		従事者に対する人的安全管理措置	A		・守秘契約、業務規程。 ・退職後の守秘規程。 ・規程遵守の監査	・本院の業務従事者は在職中のみならず、退職後においても業務中に知った個人情報に関する守秘義務を負う。
⑥	業務委託の安全管理措置	委託契約における安全管理に関する条項	A		・包括的な委託先の罰則を定めた就業規則等で裏付けられた守秘契約を締結すること。	・業務を当院外の所属者に委託する場合は、守秘事項を含む業務委託契約を結ぶこと。契約の署名者は、その部門の長とする。また、各担当者は委託作業内容が個人情報保護の観点から適正に且つ安全に行われていることを確認すること。
		システム改造及び保守でのデータ参照	A	・保守要員用のアカウントを設定する	・保守要員用のアカウントを確認する	・システム管理者は、保守会社における保守作業に関し、その作業者、作業内容、につき報告を求め適切であることを確認する。必要と認めた場合は適時監査を行う。
					・保守作業等の情報システムに直接アクセスする作業の際には、作業者・作業内容・作業結果の確認を行うこと。 ・清掃など直接情報システムにアクセスしない作業の場合、定期的なチェックを行うこと	
					保守契約における個人情報保護の徹底	
				保守作業におけるログの取得と保存	・保守作業の安全性についてログによる確認。	
		再委託における安全管理	A		・委託先事業者が再委託を行うか否かを明確にし、再委託を行う場合は委託先と同等の個人情報保護に関する対策及び契約がなされていることを条件とすること	
⑦	監査		B		・定期的な監査の実施 ・監査責任者の任命、役割、責任、権限を規定 ・監査結果の検討、規程見直しといった手順の規程	・情報システムを円滑に運用するため、情報システムに関する監査を担当する責任者（以下「監査責任者」という。）を置くこと。 ・監査責任者の責務は本規程に定めるものの他、別に定めること。 ・監査責任者は病院長が指名すること。 ・情報システム管理者は、監査責任者に毎年4回、情報システムの監査を実施させ、監査結果の報告を受け、問題点の指摘等がある場合には、直ちに必要な措置を講じること。 ・監査の内容については、情報システム管理委員会の審議を経て、病院長がこれを定めること。 ・情報システム管理者は必要な場合、臨時の監査を監査責任者に命ずること。
			C		・第三者機関に監査を委託している場合、その旨を記載する	・電子保存システムの監査をXXXとの契約により毎年4回行い、監査結果の報告を受け、問題点の指摘等がある場合には、直ちに必要な措置を講じること。
⑩	その他		A		・運用管理規程の公開について規程 ・運用管理規程の改定の規程	・本運用管理規程はXX年XX月より施行される。

付表2　電子保存における運用管理の実施項目例

A：医療機関の規模を問わない
B：大/中規模病院
C：小規模病院、診療所

管理事項番号	運用管理項目	実施項目	対象	技術的対策	運用的対策	運用管理規程文例
①	真正性確保	作成者の識別及び認証	B	利用者識別子、パスワードによる識別と認証	・利用者識別子とパスワードの発行、管理 ・パスワードの最低文字数、有効期間等の規定 ・認証の有効回数、超過した場合の対処 ・利用者への認証操作の義務づけ ・識別子、パスワードの他人への漏洩やメモ書きの禁止 ・利用者への教育 ・緊急時認証の手順規定	・システム管理者は、電子保存システムの利用者の登録を管理し、そのアクセス権限を規定し、不正な利用を防止すること。 ・パスワードの最低文字数、有効期間等を別途規定すること。 ・認証の有効回数、超過した場合の対処を別途規定すること。 ・利用者は、自身の認証番号やパスワードを管理し、これを他者に利用させないこと。 ・利用者は、電子保存システムの情報の参照や入力（以下「アクセス」という。）に際して、認証番号やパスワード等によって、システムに自身を認識させること。 ・システム管理者は、電子保存システムを正しく利用させるため、利用者の教育と訓練を行うこと。
				ログアウト操作、自動ログアウト機能、スクリーンセーブ後の再認証等	・利用者への終了操作義務づけ ・離席時の対処の規定と周知	・利用者は、作業終了あるいは離席する際は、必ずログアウト操作を行うこと。
			A	運用状況において作成者が自明の場合は、技術的対策なし	・作成責任者を明記すること ・定期的な実施状況の監査	・電子保存システムにおいて保存されている情報の作成責任者はXXであること。
		情報の確定手順と、作成責任者の識別情報の記録	B	技術的に入力した情報の確定操作を行う機能	・利用者への確定操作法の周知・教育 ・代行入力の場合、責任者による確定を義務づけ	・利用者は、電子保存システムへの情報入力に際して、確定操作（入力情報が正しい事を確認する操作）を行って、入力情報に対する責任を明示すること。 ・代行入力の場合、入力権限を持つ者が最終的に確定操作を行い、入力情報に対する責任を明示すること。
			B	技術的に情報に作成責任者の識別情報を記録する機能	・利用者への確定操作法の周知・教育	・利用者は、電子保存システムへの情報入力に際して、確定操作（入力情報が正しい事を確認する操作）を行って、入力情報に対する責任を明示すること。 ・代行入力の場合、入力権限を持つ者が最終的に確定操作を行い、入力情報に対する責任を明示すること。
			A	運用において確定の状況が自明の場合は、「確定」操作はなし	・「確定」を定義する状況を運用規程に明記する。	・本規程が対象とする情報システムの作成データの「確定」については、付表に記す。[付表として、各システムの操作における「確定」の定義を行う。”xx機器のyy釦操作の時点”、”確定操作”等]。
		更新履歴の保存	B	技術的に更新履歴を保管し、必要に応じて更新前の情報を参照する機能	・利用者への確定操作法の周知・教育	・利用者は、電子保存システムへの情報入力に際して、確定操作（入力情報が正しい事を確認する操作）を行って、入力情報に対する責任を明示すること。 ・代行入力の場合、入力権限を持つ者が最終的に確定操作を行い、入力情報に対する責任を明示すること。

		代行操作の承認記録	A	技術的に更新履歴を保管し、必要に応じて更新前の情報を参照する機能	・代行者を依頼する可能性のある担当者に、確定の任務を徹底すると同時に適宜履歴の監査を行う。	・代行入力の場合、入力権限を持つ者が最終的に確定操作を行い、入力情報に対する責任を明示すること。
		一つの診療記録を複数の医療従事者が共同して作成する場合の管理	A	複数の入力者を識別可能な機能	・各入力者毎に操作方法の周知・教育	・一つの診療記録を複数者で共同して作成する場合のは、各人がログインすること。
		機器・ソフトウェアの品質管理	A		・定期的な機器、ソフトウェアの動作確認	・システム管理者は、機器・ソフトウェアの品質維持のため、保守点検を行う。
②	見読性確保	情報の所在管理	A	技術的に情報の所在管理を行う	・技術的管理手法に応じた運用を規定 ・監査時に情報の真正性を確認	
		見読化手段の管理	A		・見読化手段の維持、管理（例えば、モニタの管理やネットワークの管理） ・運用に関する利用者要件を明記	・電子保存に用いる機器及びソフトウェアを導入するに当たって、システムの機能を確認し、これらの機能が「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ガイドライン」に示されている各項目に適合するように留意すること。 ・システムの機能要件に挙げられている機能が支障なく運用される環境を整備すること。 ・保存義務のある情報として電子保存された情報（以下「電子保存された情報」という。）の安全性を確保し、常に利用可能な状態に置いておくこと。
		見読目的に応じた応答時間とスループット	A	・応答時間の確保が出来る、システム構成、機器の選定。	・システム利用における見読目的の定義と、システム管理により業務上から要請される応答時間の確保をおこなう。	・システム管理者は、応答時間の劣化がないように維持に努め、必要な対策をとること。
		システム障害対策	A	・システムの冗長化 ・データのバックアップ	・システム障害時の体制を決める。	・システム管理者は障害時の対応体制が最新のものであるように管理すること。 データバックアップ作業が適切に行われている事を確認する。
③	保存性確保	ソフトウェア・機器・媒体の管理	A		・記録媒体劣化以前の情報の複写を規定 ・定期的な機器、ソフトウェアの動作確認	・記録媒体は、記録された情報が保護されるよう、別の媒体にも補助的に記録する。 ・品質の劣化が予想される記録媒体は、あらかじめ別の媒体に複写する。
		不適切な保管・取り扱いによる情報の滅失、破壊の防止策			・業務担当者の変更に当たっては、教育を行う。	・システム管理者は新規の業務担当者には、操作前に教育を行う。

		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			・記録媒体劣化以前の情報の複写を規定	・記録媒体は、記録された情報が保護されるよう、別の媒体にも補助的に記録する。 ・品質の劣化が予想される記録媒体は、あらかじめ別の媒体に複写する。
		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	A		・システムで使用するソフトウェアの管理を規定 ・定期的なバグフィックスやウイルス対策の実施 ・機器の設置場所、入退室管理、定期点検の規程 ・媒体の保存場所、入退出管理の規程	・運用責任者は、電子保存システムで使用されるソフトウェアを、使用の前に審査を行い、情報の安全性に支障がないことを確認すること。 ・運用責任者は、ネットワークや可搬型媒体によって情報を受け取る機器について、必要に応じてこれを限定すること。 ・運用責任者は、定期的にソフトウェアのウィルスチェックを行い、感染の防止に努めること。 ・電子保存システムの記録媒体を含む主要機器は独立した電算機室に設置すること。 ・電算機室の出入り口は常時施錠し、運用責任者がその入退出を管理すること。 ・電算機室には無水消火装置、漏電防止装置、無停電電源装置等を備えること。 ・設置機器は定期的に点検を行うこと。 ・記録媒体は、記録された情報が保護されるよう、別の媒体にも補助的に記録すること。 ・品質の劣化が予想される記録媒体は、あらかじめ別の媒体に複写すること。
		情報の継続性の確保策	A		・システム変更時に継続性が確保されるような方策を検討することを規定	・機器やソフトウェアに変更があった場合においても、電子保存された情報が継続的に使用できるよう維持すること。
		情報保護機能策	A	・ライトワンス型媒体への記録 ・バックアップ	・媒体管理規程 ・媒体の保存場所、その場所の環境、入退出管理	・電子保存システムの記録媒体を含む主要機器は独立した電算機室に設置すること。 ・電算機室の出入り口は常時施錠し、運用責任者がその入退出を管理すること。 ・電算機室には無水消火装置、漏電防止装置、無停電電源装置等を備えること。 ・設置機器は定期的に点検を行うこと。 ・記録媒体は、記録された情報が保護されるよう、別の媒体にも補助的に記録すること。 ・品質の劣化が予想される記録媒体は、あらかじめ別の媒体に複写すること。
④	相互利用性確保	システムの改修に当たっての、データ互換性の確保策	A		・異なる施設間の場合、契約により責任範囲を明確にすることを規程 ・標準的な規約（例えば、HL7、DICOM、HELICS、IHE等）に従った形式での情報の入出力を義務づけ	・機器やソフトウェアに変更があった場合においても、電子保存された情報が継続的に使用できるよう維持すること。
		システム更新に当たっての、データ互換性の確保策	A			
(4)	スキャナ読み取り書類の運用	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	A	本書8章に示す精度のスキャナの使用	・スキャナ読み取りの運用管理を規定する	・スキャナ読み取りによる・スキャナ読み取り作業に関しては、別途に作業手順を規定する。[規程中には対象文書、作業責任者、作業を行うことが許される情報作成または入手後の期間を定める]。
		スキャナ読み取り電子情報への作業責任者の電子署名及び認証業務に関する法律に適合した電子署名	A	電子署名環境の構築	・作業責任者を限定し、操作教育を行う。	
		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	A	タイムスタンプ機能		

付表3　外部保存における運用管理の例

管理事項番号	運用管理項目	実施項目	対象	技術的対策	運用的対策	運用管理規程文例
①、⑨	管理体制と責任	管理体制の構築、委託施設の選定、責任範囲の明確化、契約	B		管理体制の構築、委託施設の評価・選定、契約	この規程は、〇〇病院(以下「当院」という)において、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(以下「診療記録」という)の、ネットワークを経由してXXにおいて保管する為の仕組みと管理に関する事項を定めたものである。本規程の付表に、当院における管理体制(管理責任者、運用管理者、各作業実務者(外部の実業務委託者を含む))、XXへの監査体制(監査者)、を定める。また、保管を委託するXXへの評価を添付する。
			C		管理体制の構築、委託施設の評価・選定、契約	この規程は、〇〇病院(以下「当院」という)において、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(以下「診療記録」という)の、ネットワークを経由してXXにおいて保管する為の仕組みと管理に関する事項を定めたものである。管理責任者は院長とし、運用内容の管理実務および監査は△△に委託する。また、保管を委託するXXの評価、管理・監査を委託する△△への評価を添付する。
		受託施設への監査	A		受託先に対する保管記録の監査規程作成、契約	運用管理者は、XXにおける「診療記録」の保管内容を示す記録を監査し、正しいことを確認する。異常の発見時には直ちに管理責任者に報告すると共に、XXと契約の責任分担に基づき対処に着手する。また、これらの確認記録を残す。
					受託先での管理策の承認、実施監査規程作成、契約	運用管理者は、XXにおける受信「診療記録」の管理策を精査し、承認する。その管理策の実施状況を必要時に監査する。異常の発見時には直ちに管理責任者に報告すると共に、XXに対し対処を指示し、結果を確認する。また、これらの監査記録を残す。
		責任の明確化	A		管理責任・説明責任・結果責任の分担を定める。	付表に各管理事項(7．1．4参照)の責任分界点を定める。
		動作の監査	B	委託元での送信記録、受託先での受信記録の保持(監査目的に耐える記録レベル、保存期間であること)	委託元での送信記録、受託先での受信記録の合致監査	運用管理者は、XXから「診療記録」の受信記録を受け取り、送信した「診療記録」との合致を確認する。また、確認した旨の作業記録を残す。異常の発見時には直ちに管理責任者に報告すると共に、XXと契約の責任分担に基づき対処に着手する。
			C		監査(上記を含む全)を第三者へ委託した場合は、定期的報告(6ヶ月程度)を受けること	管理責任者は、監督を委託した△△から、『XXからの「診療記録」の受信記録、送信した「診療記録」との合致を確認した』旨の報告を受け、確認後に報告内容の保管を行う。また、異常発生時には直ちに報告を受け、△△と共に対処に着手する。
		異常時の対処	A		受託先との間で、異常時(異常の可能性も含む)の責任対処作業範囲を定める	管理責任者は「診療記録」流出の危険があると判断した時には、直ちに外部保存の運用を停止する。
②	外部保存契約終了時の処理		A		保管データの破棄契約と管理者による確認、守秘義務契約	【契約事項として】当院とXXとの契約終了時には、それまでに保管を受託した全ての「診療記録」を当院に戻す(あるいは、利用不可能な形で廃棄する)こととし、その結果につき当院の監査を受けるものとする。また、XXが受託期間中に異常への対応等で「診療記録」の内容にアクセスした場合、その内容についての守秘義務は、本保管委託契約終了後も有効である。
③	真正性確保	委託元の医療機関への成りすまし防止	A	SSL/TLSあるいは相互認証付きVPNの使用	認証局を使う場合は、両施設間でお互いに相手方の証明書を認証可能な認証局を選定する事。	運用管理者は、記録による動作の監査において、委託元、受託先双方の成りすましが無い事を確認する。
		受託先施設への成りすまし防止	A		双方が合意すれば、特に独立した第三者の認証局である必要性は無い。	
		通信上で「改ざんされていない」ことの保証	A	SSL/TLSあるいはメッセージ認証付きのVPNの使用	認証局を使う場合は、両施設間でお互いに相手方の証明書を認証可能な認証局を選定する事。双方が合意すれば、特に独立した第三者の認証局である必要性は無い。	運用管理者は、記録による動作の確認において、通信上の改竄の発見に努める。
		リモートログインの制限	A	ログインの記録(正常なログインと不正なログインが識別可能な記録レベル、監査機関より長い保存期間であること)	ログイン記録の監査	運用管理者は、記録による動作の確認において、不正と疑われるログインが無い事を確認する。
④	見読性確保	緊急に必要になることが予測される診療情報の見読性の確保	A	院内システムにおいて、緊急に必要になることが予測される診療情報を格納するに充分な記憶容量	原本と同等の内容を院内に保持	運用管理者は、緊急時における「診療記録」のアクセスに支障が無いように、院内システムにおける記憶容量の過不足を管理する。
		緊急に必要になるとまではいえない診療情報の見読性の確保	A	可搬型媒体やバックアップ媒体からもデータが読み取れる手段があることが望ましい	外部保存委託したデータの、可搬型媒体へのコピーやバックアップを取り、	運用管理者は、XXに委託した「診療記録」の、XX以外の場所にあるコピーやバックアップの存在について確認をし、アクセスが可能である事の確認をおこなう。
		ネットワークや受託先施設の障害等の場合による見読性の確保	A		受託先施設とは異なる場所に保持しておく事が望ましい。委託元でも良い。	
⑤	保存性確保	外部保存を受託する施設での保存確認機能	A	受託先施設との間で、改ざんされることの無いデータとして保存された事を確認できる機能　①ネットワークを介したStrage Commitment的機能　②保存記録の委託元への送信機能(1時間～1日単位)	左記推奨案が不可のときは、同等の事を運用で行う作業規定、あるいは、保存されているべきデータへの読み出しで確認する	運用管理者は、記録による動作の確認において、XXにおける保存が正常である事を確認する。監査者は必要に応じてXXの設備を監査する。
		標準的なデータ形式及び転送プロトコルの採用	A	DICOM、HL7、標準コードの使用あるいはこれらへの変換機能		

		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	A		継続性の保証契約を交わす	【契約事項として】当院とXXは互いに各自のシステム変更に当たっては、相互にデータ通信の継続性に配慮し、変更内容が外部保存の障害にならないように協議をする。
		電気通信回線や外部保存を受託する施設の設備の劣化対策	A		受託施設の設備内容を契約時に確認する	監査者は必要に応じてXXの設備を監査する。【契約事項として】XXは保管設備の劣化に意を払い、機能の保全に努めなければならない。
		電気通信回線や外部保存を受託する施設の設備の互換性確保	A		受託施設の設備内容を契約時に確認する	監査者は必要に応じてXXの設備を監査する。【契約事項として】XXは、保管データの全てがネットワーク経由で当院から読み出せる様に、保管設備のデータ互換性を維持しなければならない。
		情報保護機能	A		受託施設の設備内容を契約時に確認する	監査者は必要に応じてXXの設備を監査する。【契約事項として】XXは、XXの責に帰す保管データの故意または過失による破壊に備えて、回復できる機能を備えなければならない。
⑥	外部保存を受託する施設内での 個人情報保護策	秘匿性の確保のための適切な暗号化	A	メッセージの暗号化が可能な通信手段 暗号の強度は、電子署名法に準じること		
		通信の起点・終点識別のための認証	A	SSL/TLSあるいは相互認証付きVPNの使用 暗号の強度は、電子署名法に準じること	認証局を使う場合は、両施設間でお互いに相手方の証明書を認証可能な認証局を選定する事 双方が合意すれば、特に独立した第三者の認証局である必要性は無い。	運用管理者は、記録による動作の監査において、委託元、受託先双方が正当である事を確認する。
⑦	個人情報保護策	外部保存を受託する施設における個人情報保護	A		受託施設と「受託施設側における業務従事者への教育、守秘義務	監査者は必要に応じてXXを監査する。【契約事項として】①XXは当院から受けた保管委託を再委託してはならない ②XXは「診療記録」の保管業務に従事する従業員に対して「個人情報保護の重要性」の教育を年1回行う。また、その業務を離れた後も有効な守秘契約を当該従業員と交わすこと。
		外部保存を受託する施設における診療情報へのアクセス禁止	A	アクセス制御機能とアクセスログ機能、監査目的に耐えるログ保存期間であること	委託元によるアクセスログの監査	監査者は、XXにおける保管された「診療記録」及びアクセスログへのアクセス記録を監査する。
		外部保存を受託する施設における障害対策時のアクセス通知	A	アクセス制御機能とアクセスログ機能、監査目的に耐えるログ保存期間であること	アクセス許可、秘密保持に関する契約と委託元によるアクセスログの監査	【契約事項として】XXにおいては正当な理由無く、保管した「診療記録」及びアクセスログにアクセスしてはならない。出来る限り事前に当院の許可を得ることとし、やむを得ない事情で許可を得ずアクセスした場合は遅滞無く当院に報告するものとする。また、目的外に利用してはならないし、正当で明確な目的が無く他の媒体などに保管してはならない。
		外部保存を受託する施設におけるアクセスログの完全性とアクセス禁止	A	アクセスログファイルへのアクセス制御とアクセスログ機能、監査目的に耐えるログ保存期間であること	委託元によるアクセスログへのアクセスの監査	
⑧	患者への説明と同意	外部保存を行っている旨を院内掲示等を通じて周知し、同意を得ること	A		外部保存を行っている旨を院内掲示等を通じて周知し、同意を得ること	管理責任者は、外部保存している事の患者への周知が計られている事（例、掲示内容、位置）、また同意を得られなかった患者の「診療記録」の管理状況を適宜(例、1回/月)確認する。
						付録 1. 管理体制・委託施設との責任分担規定 2. XXに保管を委託する「診療記録」の定義 3. XXへの監査事項 4. XXとの契約

A：医療機関の規模を問わない
B：大/中規模病院
C：小規模病院、診療所