医 療 情 報 システム

運用管理規程

初版　平成22年　3月　1日
改定　平成22年　9月　1日
改定　平成23年　4月　1日
改訂　平成31年　4月　1日

独立行政法人　国立病院機構

信州上田医療センター

目　　次

１　運用管理規定の発行 1

２　総則 2
2,1　目的 2
2.2　適用範囲 2
2.3　運用管理規定の要件、要求事項 2
2.4　用語の定義 3
2.5　組織 4

３　情報システム管理者と情報系管理組織 5
3.1　情報システム管理者の情報管理に関する責務 5
3.2　医療情報部運営委員会 5
3.3　監査体制と責任者の任命 6

４　医療情報システムのデータ保護に関する倫理規程 8
4.1　総則 8
4.2　責任 9
4.3　運用 10
4.4　罰則 11
4.5　その他 11

５　医療情報システムのセキュリティ方針 12
5.1　総則 12
5.2　管理体制（組織的安全対策） 12
5.3　教育と訓練 13
5.4　監査 13
5.5　物理的安全対策 14
5.6　技術的な安全対策 14
（医療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）
5.7　人的安全対策 15
5.8　情報の破棄 15
5.9　医療情報システムの改造と保守 15
5.10　真正性の確保 16
5.11　見読性の確保 16
5.12　保存性の確保 16
5.13　法的に使用される情報の管理 17
5.14　オーダリングシステムへのアクセス 17
5.15　運用管理 17

１　運用管理規定の発行

適用範囲　　：院内規程
適用開始日　：2010/03/01
公開制限　　：信州上田医療センター
見直し期間　：原則年１回（必要時は随時）
配布元　　：事務部医療情報部

改版履歴

版数	適用開始日	変更理由／内容
１	2010/03/01	
２	2010/09/01	電子カルテ稼働に伴う変更
３	2011/04/01	病院名称の変更
４	2019/4/1	

2　総則

2,1　目的

医療機関においては、診療情報及び診療諸記録を電子媒体に保存し、それを利用して診療業務の全部あるいはその一部を行う場合は、それらの情報の利用について、それに直接あるいは間接に関与する全職員に運用管理規定を設け、それを利用するための基本的な考え方及びその方針、さらに患者のプライバシーの保護と利用者の情報利用に関する保証を確保するための組織と利用方法の原則を規定しなければならない。

この規程は、独立行政法人国立病院機構信州上田医療センター（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「保存義務のある情報」という。）の電子媒体による保存のために使用される機器、ソフトウェア及び運用に必要な仕組み全般（以下「医療情報システム」という。）について、その取扱い及び管理に関する事項を定め、当院において、保存義務のある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。

2.2　適用範囲

（１）対象者

医療情報システムを扱う全ての利用者を対象とする。

（２）対象システム

医療情報システムを構成する全ての部分(コンピュータシステムに関する装置、システムの運用に携わる人、システムの利用者等をいう。以下同じ。)

（３）対象情報

全ての診療に関する情報とする。

2.3　運用管理規定の要件、要求事項

本規程は、以下の関連法令、関連ガイドラインの基準に則って、各要求事項を満たすものとする。

（１）診療情報等の保護に関する法令の適用（電子媒体による保存を認める文書等）

①医師法（昭和２３年法律第２０１号）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）に規定されている診療録

③保健婦助産婦看護師法（昭和２３年法律第２０３号）に規定されている助産録

④医療法（昭和２３年法律第２０５号）に規定されている診療に関する諸記録及び病院の管理及び運営に関する諸記録

⑤歯科技工士法（昭和３０年法律第１６８号）に規定されている指示書

⑥薬剤師法（昭和３５年法律第１４６号）に規定されている調剤録

⑦救急救命士法（平成３年法律第３６号）に規定されている救急救命処置録

⑧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）に規定されている診療録等

⑨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）に規定されている調剤録

⑩歯科衛生士法施行規則（平成元年厚生省令第４６号）に規定されている歯科衛生士の業務記録

（２）電子保存の３原則（真正性・保存性・見読性の確保）

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と所在が明確であり、かつ、故意又は過失による、虚偽入力、書き換え、消

去、及び混同が防止されていることをいう。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の記録内容を誤ることをいう。

見読性とは、電子媒体に保存された内容を必要に応じて肉眼で見読可能な状態に容易にできることである。なお、”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、その目的に応じて」という意味であり、”容易に”とは、「目的にあった速度、操作で見読を可能にすること」を意味する。

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わたって、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。

（３）自己責任の原則

自己責任とは、当院が運用する医療情報システムについて説明責任、管理責任、結果責任を果たすことをいう。

なお、医療情報システムとは、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ために使用される機器、ソフトウェア及び運用に必要な仕組み全般をいう。

説明責任とは、このシステムが電子媒体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り、管理責任とは、このシステムの運用面の管理を当院が行う責任をいう。

（４）医療情報システムの安全管理に関するガイドライン第５版

厚生労働省　平成２９年　５月

（５）医療・介護関係者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

厚生労働省　平成１６年１２月

（６）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。）

（７）独立行政法人国立病院機構情報セキュリティ対策規程

平成 28 年 11 月 1 日

（８）公文書保存に関する規程

2.4　用語の定義

（１）医療情報システム

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作成及び電子媒体による保存のために、使用されている機器、ソフトウェア及び運用に必要な仕組みをいう。

主としてコンピュータ、通信設備機器、院内ＬＡＮ、各種ソフトウェア等で構成され、それらにより情報が蓄積され、処理され、検索され、電送される機能の総称。

データ及び情報には、プログラムや仕様、保守・運用・使用手順が含まれる。

（２）オーダリング

診療に関わる全ての情報とその支援情報

（コンピュータで処理するために電子情報となっているものも含む。

例：磁気媒体上に格納されている情報、回線上を転送されている情報、主記憶上で処理されている情報など。）

（３）ログ

オーダリングの処理内容や利用状況を時間の流れに沿って記録したもの。あるいは記録すること。

（４）機密性

利用者に対して、その利用者が権限行使できる責任範囲に限り、その権限の条件に従ってデータ及び情報が書き換えられ、あるいは見読できること。

（５）一貫性

データ及び情報が正確で完全であり、かつその真正性、保存性が維持されること。

（６）可用性

データ、情報、電子計算システムが、適時に、必要な様式に従いアクセスでき、利用できること。

（７）運用責任者

医療情報システムへのアクセス権限の登録、管理を統括する。

医療情報システムの利用者登録の管理を行い、登録情報を医療情報部運営委員会又は医療情報部会議に通知する。

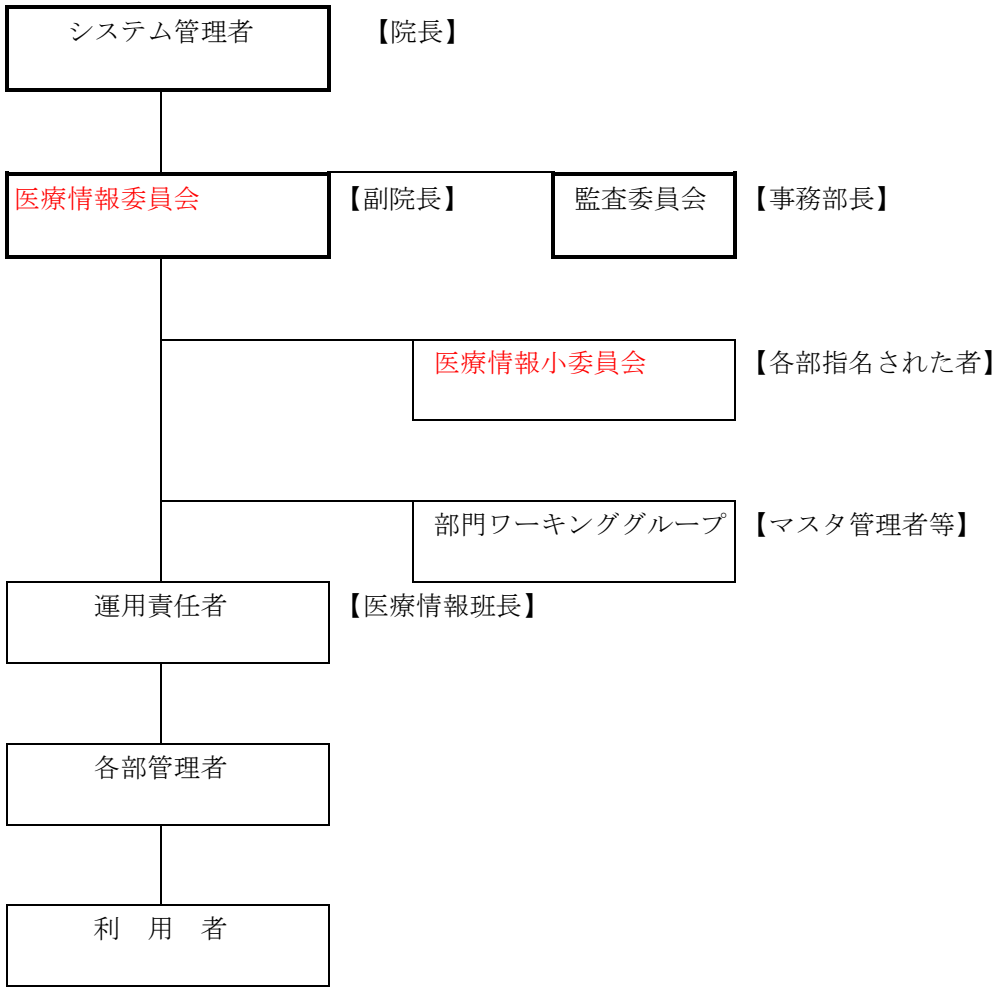
（８）各部の管理者

各部が管理する医療情報システムを管理するため、各部の長がこれにあたり、各部の利用者に対して個々具体的な指示を行う。

また、医療情報部会議に出席する各部の代表者を指名する。

2.5　組織

医療情報システム運用組織



3　情報システム管理者と情報系管理組織

3.1　情報システム管理者の情報管理に関する責務

（1）当院に情報システム管理者（以下「システム管理者」という。）を置き、システム管理者をもってこれにあてる。

（2）システム管理者は、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」に示される各項目に適合するよう留意すること。

（3）システム管理者は、「情報システム運用管理規程」と「セキュリティ方針」を作成し、さらに効率的に運用するために「情報管理をする組織」を設けなければならない。

（4）システム管理者は、医療情報システムに関する「運用管理規程」を整備運用し、その実施状況を確認しなければならない。

（5）システム管理者は、医療情報システムを円滑に運営し、医療情報システム全体の管理状況を把握しなければならない。

（6）システム管理者は、業務の効率性と円滑化のために常に医療情報システムの情報を収集し、合理的運営を指針するために適切に医療情報部運営委員会に諮問しなければならない。

（7）システム管理者は、医療情報部運営委員会の委員長を選任し、委員長から委員会の協議内容について報告を受けなければならない。

3.2　医療情報委員会

3.2.1　医療情報委員会

（1）医療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、システム管理者のもとに医療情報システムを管理する医療情報委員会（以下委員会という。）を置く。

委員会はシステム管理者から質問された時は直ちに検討し、その内容を報告しなければならない。

委員会の長は、システム管理者が指名する。

（2）委員会は、システムを円滑に運用するため、医療情報システムに関する運用・監査について、それぞれを担当する責任者（運用責任者及び監査責任者）を置く。

（3）委員会は、病院情報マスタ等に関する部門（部門ワーキンググループ）を統括管理し、電子保存に関わらず効率的な運用を実践するために運用管理規程の見直し等についてシステム管理者に提言する責務がある。

（4）委員会は、病院内の各組織に対して横断的な調整機能を持つ。

（5）委員会は、情報系委員会等から具申される問題について積極的に調整しなければならない。

（6）委員会は、委員会の協議内容についてシステム管理者に報告しなければならない。

（7）委員会の運用責任者及び監査責任者は、委員長が委員の中から選出しシステム管理者が承認する。

（8）委員会は、ハードコピーをとった資料などの不要となった診療情報等を安全な方法で、速やかに廃棄・消去することを各部門に指導しなければならない。

（9）委員会には、次の組織を設置する。

3.2.2　病院情報小委員会

（1）医療情報小委員会（以下「小委員会」という。）は、医療情報システムにおける病院情報マスタの管理以外の運用に関する管理を行う。

（2）小委員会は、医療情報システムが機能しなくなった時でも診療に大きな混乱を来さないための方策を検討し、各部門の詳細な対応を定める。

（3）小委員会は、基幹医療情報システムに留まらず部門システムあるいはその周辺システムの障害時対応も全て網羅的に管理する。

（4）小委員会は、その対応策の解決について必要に応じて医療情報委員会に検討内容を具申することができる。

（5）小委員会は、外部及び内部ネットワークを利用して各種情報を病院利用者あるいは院内職員に提供する内容について検討し、作成する。

（6）小委員会は、外部ネットワークの院内利用者についてその利用者権限を管理する。特に職員が臨床研究情報を個人の端末に保有しなければならないとき、その端末のセキュリティ管理について指導する。

（7）小委員会は、内部ネットワークの職員向け情報提供について職員の要望を反映した編集を行う。

（8）小委員会は、医療情報システムの使用について効率的な使用ができるように新規採用職員の教育プログラムスケジュールの作成について、各部門に助言を行う。

（9）小委員会は、ローカルに設置された教育研修用のＬＡＮ及びそこに配置された端末・周辺機器も同様に管理する。

(10) 小委員会は、各部門を調整する教育研修について医療情報部運営委員会に具申することができる。

(11) 患者又は利用者からの医療情報システムについての問い合わせ・苦情を受け付ける窓口を設け、苦情を受け付けた場合は、その内容を検討し、直ちに必要な措置を講じなければならない。

(12) 小委員会の協議内容についてシステム管理者に報告しなければならない。

3.2.3　部門ワーキンググループ

（1）部門ワーキンググループ（以下「ワーキンググループ」という。）は、ネットワークを介して使用する全ての用語を共有化するためにその関係するマスタを統合管理する。

（2）ワーキンググループは、成長するシステムを構築するためにプログラムに組み込むステップを可能な限りロジックに置き換えてマスタ上で管理する。

（3）ワーキンググループは、システム開発ＳＥあるいは運用支援関係者と協調してマスタ管理を行う。

（4）ワーキンググループで生じる問題について必要に応じて委員会に具申することができる。

（5）ワーキンググループは、協議内容についてシステム管理者に報告しなければならない。

3.3　監査体制と責任者の任命

（1）監査委員会は、監査責任者を置く。

（2）監査責任者は、システム管理者が指名する。
（3）監査委員会は、必要に応じて開催し、結果をシステム管理者に報告する。
（4）監査委員会は、システム管理者から要請があったとき、監査を直ちに行い、その結果を速やかに答申しなければならない。
（5）収集した情報について必要を認めた場合、監査委員会を開催し、その結果をシステム管理者に報告しなければならない。
（6）監査委員会は、委員会に対し監査に必要な情報及び人選を要求することができる。
（7）監査が行われる際は、医療情報システムの利用者全てが誠意を持って協力しなければならない。

4　医療情報システムのデータ保護に関する倫理規程

4.1　総則

1）目的

この規程は、独立行政法人国立病院機構信州上田医療センター医療情報システム（以下「医療情報システム」という。）の利用者及び管理者の正当性を確保するとともに、医療情報システムの運用並びにそれに関する責任及び罰則を定めることにより、診療情報等の不適切な取扱いに起因する患者の権利・利益の侵害の防止及び基本的人権の保護と同時に、利用者間の情報の共同利用に関する保護を図ることを目的とする。

2）医療情報システムのデータ保護の規程等

当院の医療情報システムのデータは、この規程の定めにより保護されるものとする。

3）データ及び秘密情報の保護

オーダリングを中心とした医療情報システムの診療情報等を含むデータ及び秘密情報は、機密性、一貫性、可用性の欠如に起因する危害から保護されなければならない。

4）診療情報等の保護に関する法律の適用

（1）電子媒体による保存を認める文書等

①医師法（昭和２３年法律第２０１号）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）に規定されている診療録

③保健婦助産婦看護師法（昭和２３年法律第２０３号）に規定されている助産録

④医療法（昭和２３年法律第２０５号）に規定されている診療に関する諸記録及び病院の管理及び運営に関する諸記録

⑤歯科技工士法（昭和３０年法律第１６８号）に規定されている指示書

⑥薬剤師法（昭和３５年法律第１４６号）に規定されている調剤録

⑦救急救命士法（平成３年法律第３６号）に規定されている救急救命処置録

⑧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）に規定されている診療録等

⑨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）に規定されている調剤録

⑩歯科衛生士法施行規則（平成元年厚生省令第４６号）に規定されている歯科衛生士の業務記録

5）適用範囲

この規程は、医療情報システムを利用する当院の全ての業務及び利用者に適用される。

6）原則

この規程は、以下の基本原則に拠る。

（1）自己責任の原則

自己責任とは、当院が運用する医療情報システムについて説明責任、管理責

任、結果責任を果たすことをいう。

なお、医療情報システムとは、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のために使用される機器、ソフトウェア及び運用に必要な仕組み全般をいう。

説明責任とは、このシステムが電子媒体の基準を満たしていることを第三者に説明する責任をいう。

管理責任とは、このシステムにより発生した問題点や損失に対する責任をいう。

（2）真正性・保存性・見読性の原則

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と所在が明確であり、かつ、故意又は過失による、虚偽入力、書き換え、消去、及び混同が防止されていることをいう。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の記録内容を誤ることをいう。

見読性とは、電子媒体に保存された内容を必要に応じて肉眼で見読可能な状態に容易にできることである。なお、”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、その目的に応じて」という意味であり、”容易に”とは、「目的にあった速度、操作で見読を可能にすること」を意味する。

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わたって、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。

（3）周知原則

利用者は医療情報システムへの信頼を高めるために､診療情報等の保護対策、手続き、規則の存在及びその範囲について適切な知識を得ることができ、管理者はこれらについて周知を図る。

（4）倫理原則

医療情報システムの保護対策は、利用者及び患者の権利及び利益を尊重して行われること。

（5）一貫性原則

診療情報等の保護のための対策、手続き、規則には、技術、管理、組織、運営、教育、法律を含めた範囲での関連する考え方を考慮に入れて院内の対策、手続き、規則の調和を図ること。

（6）再評価原則

医療情報システムの保護施策の要求は、運用形態、利用形態及び技術とともに変化するため、診療情報等の保護のための対策、手続き、規則は必要に応じ再評価しなければならない。

4.2 責任

1）業務の明確化

業務の管理者は、医療情報システムを利用する業務内容を、以下の範囲において明確にしておかなければならない。

（1）業務の名称

（2）業務の目的

（3）業務の管理者とその者の権限の範囲

（4）利用者とその者の権限の範囲・診療情報等の記録の内容

2）利用者権限の付与の決定

（1）医療情報部運営委員会（以下「委員会」という。）は、利用者権限の付与の請求が有ったとき、速やかに決定しなければならない。

（2）各部門の長は、部門間の整合性を図りながら業務の管理者と協議して、その権限付与について委員会に諮問することができる。

（3）委員会は、診療情報等の取扱い権限を決定し、職員全員にその内容を周知し、その徹底を図らなければならない。

3）診療情報等の取扱い権限

業務の管理者は、診療情報等に対して、以下の方針により取扱い権限の付与に関し、各部管理者と協議を行うものとする。

（1）診療情報等の登録、参照、更新の各権限は、原則として分離されること。

（2）利用者への権限の付与の決定は、委員会のみが行うこと。

（3）業務の管理者は常に利用者に付与されている権限の最新状況を把握しておくこと。

（4）業務上不必要な権限は付与しないこと。

4）医療情報システム利用者の責務

病院職員は本倫理規定を遵守するとともに個人情報保護法令をはじめとする、各種法令を遵守すること。

4.3　運用

1）医療情報システムの監査

（1）運用責任者は、診療情報等の登録、参照、更新、削除を行う際のログ情報を収集し、必要の都度、その結果を監査責任者に提出し、監査責任者は、監査内容を委員会へ報告しなければならない。

（2）ログ情報は、以下の情報とする。

①利用者ＩＤ

②操作内容（端末ＩＤ・患者ＩＤ）

③対象となる診療情報等（指示番号・各種エラーメッセージ）

④操作年月日と時刻

2）教育及び訓練

各部管理者は、利用者あるいは利用者になるものに対して、診療情報等を保護する目的とその必要性を十分に理解させ、その対策を推進するために、教育研修を行うものとする。

3）廃棄

委員会は、ハードコピーをとった資料などの不要となった診療情報等を安全な方法で、かつ、速やかに廃棄・消去することを各部門に指導しなければならない。

4）協力

この規程の実施及び診療情報等の保護のための対策、手続き及び規則を可能な限り有効なものにするため、各部管理者は委員会と協議し、調整し、協力しなけれ

ばならない。

4.4　罰則

1）義務と罰則

診療情報等については、秘密を守る義務を課するとともに、これに違反した場合には罰則を科する。

4.5　その他

1）規程の見直し

この規程は、業務の大幅な変更や医療情報システムの構成変更時には見直されるものとする。

5　医療情報システムのセキュリティ方針

5.1　総則

5.1.1　目的

本セキュリティ方針は、当院の個人情報保護方針、「データ保護に関する倫理規程」及び次項 5.1.2 基本方針に則って、医療情報システムの運用プロセスにおけるセキュリティ方針を定めることを目的とする。

5.1.2　基本方針

（1）医療情報システムが取り扱う情報は阿東に暴露されたり、不当に内容が改ざんされたり、不当に処理が妨害されたりしないように管理及び保護されなければならない。

（2）診療情報等患者の個人情報への不正アクセス、紛失、破壊、改ざん及び漏洩を防止し、安全で正確な管理を確保する。

（3）医療情報システムで処理、保管されているデータに関するいかなる情報もこのシステムに関係のない者には公表しないことを原則とする。

（4）個人情報保護に関する法令及びガイドラインを遵守し、個人情報保護に関する体制を整備し、内部規定を作成して安全管理体制を確立する。

（5）医療情報システムの安全管理に関するガイドラインに準拠して、安全管理のための組織的対策、技術的対策、運用管理対策、利用者や管理者への教育などの人的対策について運用面と技術面でバランスのとれた総合的な対策を検討する。

（6）セキュリティ管理は、セキュリティ対策と保護対象となる情報の価値とのバランスを維持するために下記の点に留意する。

・医療情報システムのセキュリティ上の想定脅威（発生が懸念される不正暴露、改ざん、処理妨害等）

・想定脅威に対して、その発生が及ぼす損失とそのセキュリティ対策費用及び利便性を考慮した有効な対策とその速やかな実施

（7）診療に関わる情報にアクセスできる者は、医師及び関連する医療スタッフとし、患者による直接アクセスは行えないこととする。ただし、医師の判断により診療に関わる情報を患者に開示する場合は、アクセスした医師の責任において行うこととする。

なお、診療の準備、奨励研究、カンファレンス等の目的で診療に関わる情報にアクセスする場合も同様に、アクセスした医師の責任において行うこととする。

5.1.3　適用範囲

本セキュリティ方針は、医療情報システムを構成する全ての部分（コンピュータシステムに関連する装置、システムの運用に携わる人、システムの利用者等をいう。以下同じ。）に適用する。

5.2　管理体制（組織的安全対策）

5.2.1　医療情報部運営委員会及び医療情報部会議の役割

（1）情報セキュリティ方針を実施するため、その実施方法について、その評価や問題点などを検討し、情報セキュリティの保護、管理を行うとともに、病院内で

実施される情報セキュリティ対策に矛盾が生じないよう調整を行う。

（2）委員会及び部会は、次のような次項を担当する。

・当院の情報セキュリティ方針の適切な運用とそれに関する責任についての検討
・当院の情報財産に対する脅威についての監視と予防対策の検討
・当院内で発生したセキュリティ事件の検討及び監視
・情報セキュリティを強化するための検討
・セキュリティ対策を実践するためのシステム管理者への提言

5.2.2　システム管理者の責任

システム管理者は、医療情報システムのセキュリティ確保のために、以下の管理者・責任者を承認する。

（1）運用責任者【経営企画室長】
（2）各部管理者【業務の管理者及び情報管理部門担当者】

5.2.3　委員長の責任

（1）医療情報部運営委員会の委員長は、少なくとも毎年一回、医療情報システムのセキュリティ管理状況を調査する。
（2）必要に応じて、その内容の見直しをシステム管理者に提言する。

5.2.4　管理者及び利用者の責務

管理者及び利用者は、この規程を遵守するものとする。

5.2.5　違反者に対する処置

本セキュリティ方針を含む組織、機関の定めたセキュリティ方針に違反した者には、罰則を科す。罰則については、独立行政法人国立病院機構職員就業規則、独立行政法人国立病院機構非常勤職員就業規則における懲戒等に基づく処分とする。

5.3　教育と訓練

（1）マニュアルの整備

管理者は、医療情報システムの取扱いについて利用者マニュアルを整備し、利用者に周知のうえ、常に利用可能な状態に置かなければならない。

（2）教育・訓練

管理者は、医療情報システムの利用者に対し、必要に応じシステムの取扱い及びプライバシー保護、ルール遵守に関する教育、研修を行わなければならない。

（3）医療情報システムの利用者及び利用する全てのスタッフは、前項において実施する教育・研修を受けなければならない。

5.4　監査

（1）医療情報システムを円滑に運用するために、医療情報システムに関する監査を担当する責任者（監査責任者）を置き、必要な都度、監査を実施する。
（2）監査責任者は、システム管理者が指名すること。
（3）監査責任者は監査情報を収集し、それらを監査し、その結果を医療情報部運営委員会又は医療情報部会に報告する。
（4）監査責任者は、常に第三者的立場を堅持して公正に医療情報システムの不正ある

いは改ざんあるいは混同の混在について指摘しなければならない。

（５）監査の内容については、医療情報部運営委員会の審議を経てシステム管理者がこれを定めること。

5.5　物理的安全対策

5.5.1　来訪者の記録・識別、入退の制限などの入出管理

（１）院内では、職員カードを第三者が見える所に着用すること。

（２）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は施錠等の対策を講ずること。

（３）個人情報を入力、参照できる端末が設置されている区域は、業務時間帯以外は施錠など権限者以外が立ち入ることができない対策を講じること。なお、やむを得ない場合は、医療情報システムにパスワードを設け、権限者が以外が参照できないようにすること。

（４）個人情報の物理的保存を行っているサーバ室は入退室管理を実施すること。

・静脈認証システムによる入退者の制限

・錠については、防災センターでの一元管理及び使用する際は台帳に記入のこと。

（５）サーバ室への関係者以外の入室は原則として禁止する。やむを得ない場合は運用管理者が立ち会うこと。

5.5.2　物理的な安全対策

（１）コンピュータ装置本体、ネットワーク管理装置等、システムの処理に重大な影響を与える装置は盗難や破壊、関係者以外の使用から保護するために物理的な方法によって保護する。

（２）全装置の一覧表を維持管理し、不正な持ち出し等を防ぐこと。

（３）回線は、全ての部分で物理的に保護されることとし、定期的に検査する。

（４）電源装置の故障により遮断や停電の場合でも、サーバ機が安全に停止する電力を無停電電源供給装置（ＵＰＳ）等により供給を可能とする。

5.6　技術的な安全対策

（医療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）

5.6.1　利用者の識別と認証

（１）個々の情報に対して、権限を持っている利用者に対し、その権限の範囲内でのみ利用させるようにするため、利用者権限チェック表を作成し、システム管理者にて管理する。

（２）利用者は、利用者ＩＤによって識別し、本人の確認はパスワードによって行う。

5.6.2　ファイル管理

（１）ファイル（データベース含む）やプログラムを管理しているシステムあるいは業務上特別な条件下で必要なツールさらに後利用データベースにおいて患者のプライバシーに影響を与えるデータなどは、特別に権限を付与された利用者のみ利用できる。

（２）医療情報システムの運用関連及びファイル（データベース含む）管理関連のプログラムやデータの変更は、特別な権限を付与された者のみが行うことができる。

（３）前項（２）の変更については、事前に変更手続きを規定し、その規定に則って実施する。

（4）ファイル（データベース含む）やプログラムを管理しているシステムは、運用中は常時、管理者が管理できる状態にしておく。
（5）利用されるソフトウェアは、ライセンス契約に準拠したものであることが保証できるようにしておく。

5.6.3　ネットワークセキュリティ管理

（1）ネットワークの利用及びネットワークの構成の登録・変更は、事前の手続きを規定し、その規定に則って実施するようにする。
（2）内部ネットワークから部門システム等を介して外部と通信する場合（リモートメンテナンス等）には、院外のリモートメンテナンス端末の管理方法も把握して許可を与えなければならない。
（3）院内の外部ネットワークは、内部ネットワーク（業務で使用するサーバ及び端末が接続されたネットワーク）と当面接続しないものとする。
（4）特に許可された者以外は、院外回線を通じて内部ネットワークを利用できない。
（5）外部ネットワークは、ファイアウォールで外部からのアクセスを制御する。
（6）プライバシーに関係するような重要なデータをネットワーク上で使用する場合は、ネットワーク環境がセキュリティの確保上完全ではないことを考慮した上で使用しなければならない。

5.7　人的安全対策

5.7.1　従業者に対する人的安全管理措置

システム管理者は、個人情報保護に関する施策が適切に実施されるように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作業員として採用するときは、雇用及び契約時に守秘・非開示契約を締結すること。
（2）定期的に従事者に対し教育訓練を行うこと。
（3）従事者の退職後の個人情報保護について徹底させること。

5.7.2　事務委託業者の監督及び守秘義務契約

（1）業務を当院以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締結すること。
（2）プログラムの異常等で、保守データを救済する必要があるときなど、やむを得ない事情で外部の保守要員が診療情報など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付けられた守秘契約等の秘密保持の対策を行うこと。

5.8　情報の破棄

（1）全ての不要となった診療情報等は安全確実な方法で、かつ、速やかに廃棄・消去しなければならない。
（2）情報種別ごとに破棄を行う条件、具体的な破棄の方法など廃棄手順を委員会において検討させること。

5.9　医療情報システムの改造と保守

（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作業者に指示すること。
（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、

保守要員個人のアカウントを使用し、個人情報へのアクセスの有無、及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。

（３）作業員各人と保守会社の守秘義務契約を指示・確認すること。

5.10　真正性の確保

5.10.1　アクセス管理

（１）医療情報システムへのアクセスは、利用者ＩＤとパスワードによる識別と認証を行う。

（２）システム管理者は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。

（３）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。

（４）利用者は、作業終了時あるいは離席する際は、必ずログアウト操作をしなければならない。

5.10.2　機器・ソフトウェアの品質管理

（１）医療情報システムの機器構成、ソフトウェア構成と各機器、ソフトの機能、用途（利用目的）が明確化されており、システムの仕様が明確に定義されていること。

（２）機器、ソフトウェアの改版履歴、導入時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。

5.11　見読性の確保

（１）電子保存に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しなければならない。

（２）システムの機能要件にあげられている機能が支障なく適用される環境を整備しなければならない。

（３）電子保存された情報の安全性を確保し、常に利用可能な状態に置かなければならない。

（４）見読目的に応じた応答時間が確保できるシステム構成、機器を選定し、業務上から要請される応答時間の確保を行う。また、システム管理者は、応答時間の劣化がないように維持、管理しなければならない。

（５）システムの冗長化、データのバックアップなど必要なシステム障害対策をとり、システム障害時の体制を決定する。また、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しなければならない。

5.12　保存性の確保

5.12.1　ウイルスや不適切なソフトウェアなどによる情報の破壊などの防止

ウイルス又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などの情報が破壊される恐れがあるため、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書通りに動作していることを確認しなければならない。

・利用者が持ち込むデータや、システム運用に直接関連するプログラム等重要なプログラムを扱う場合には、利用前にウイルスチェックを実施する。
・ウイルスワクチンプログラムは全ての端末に配置しておく。
・利用者は、使用中にウイルス感染の疑いが生じた場合は運用責任者に通知する。
・情報管理部門は、障害の状況を分析しウイルスが確認された場合は、その旨を全利用者に通知して注意を喚起し、同時に委員会又は部会に報告しなければならない。

5.12.2　不適切な保管・取扱いによる情報の滅失、破壊の防止

不適切な保管・取扱いによる情報の滅失、破壊を防止するため、システム管理者は新規の業務担当者に対して操作前に教育を行う。

5.12.3　記録媒体、設備の劣化による読み取り不能または不完全読み取りの防止

（１）記録媒体に記録された情報が保護されるよう、記録媒体劣化以前の情報を別の媒体に補助的に記録する。

（２）これを防止するため、品質の劣化が予想される記録媒体は、あらかじめ別の記録媒体や記憶機器に複写する。

5.12.4　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

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情報等の情報が復元できなくなることがある。このため、システムの全部又は一部の変更に際して、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。

5.13　法的に使用される情報の管理

（１）法的に使用されるオーダリング情報は、その真正性を確保するように講じられていること。

（２）法的に使用されるオーダリング情報の真正性は、操作を行う者の利用者ＩＤとパスワードで認識させ、確定情報は、確定入力を動機付けできる画面で構成し、その修正は原本を保存しながら修正データが見読できるよう構築されていること。

（３）法的に使用されるオーダリング情報は、法的に求められる期間中保存でき、機器等の更新によるデータの互換性は保持できるように講じてあること。

（４）法的に使用されるオーダリング情報を保存及び出力するシステムは、法的に求められる期間内は、常に稼働できる状態にしておくこと。

（５）法的に使用されるオーダリング情報の所在を明確にし、法的保存期間の情報の開示を求められた場合、速やかに開示できるうにすること。

（６）紙面での保存が法的に必要な情報は、その法的根拠が保たれる状態で保存しなければならない。

5.14　オーダリングシステムへのアクセス

（１）通常時のオーダリングシステムへのアクセスは、外来・入院を問わず、診療を希望する旨の根拠となる情報が患者又は患者の代理人の意志により表明され、かつ、患者の登録手続きが済まされていなければ行うことができない。

（２）なお、受診者が本人であることが判明しない場合には、患者の診察券の患者番号を電子カルテ端末に入力することにより、確認しなければならない。

5.15　運用管理

医療情報システムは、本運用管理規程及び各システム運用マニュアルに基づき運用されるとともに、以下の条件に従って適切に管理されなければならない。

（1）システムが災害にあった場合の対処方法と復旧方法について明確にし、必要に応じて情報管理部門で見直しを実施すること。

（2）システムのバックアップを実施するとともに、バックアップ媒体は安全な場所に保管すること。

（3）機密性の高いバックアップデータは、厳重に保管されること。

（4）システム資源の容量を定期的に確認し、容量不足が予想される場合には速やかに対処すること。

附　則

１．この規程は、平成２２年３月１日から施行する。

２．この規程に定める事務は、医療情報部運営委員会が所掌する。

３．この規程は、平成２２年９月１日から改定する。

４．この規程は、平成２３年４月１日から改定する。

５．この規程は、平成３１年４月１日から改定する。