三宿病院

医療情報システム運用管理規程

第１版

国家公務員共済組合連合会

三　宿　病　院

三宿病院　医療情報システム運用管理規程

１．目　的

この規程は、三宿病院（以下「病院」という。）において、医療情報システム(以下「電子カルテ」という。)で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全般について、厚生労働省「医療情報システムの安全管理に関するガイドライン」に則り、その取扱い及び管理に関する事項を定め、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を目的とする。

２．対　象

1)　対象者は、電子カルテを扱う全ての利用者とする。

2)　対象システムは、電子カルテシステム、オーダリングシステム、各部門システムとする。

3)　対象情報は、全ての診療に関する情報とする。

３．情報システム管理者及び運用責任者等の任命

1)　病院に医療情報システム管理者を置き、病院長を以てこれに充てる。

2)　電子カルテを円滑に運用するため、医療情報システム管理者が指名する電子カルテ運用委員長を充て電子カルテに関する運用を担当する責任者(以下「運用責任者」という。)とする。

3)　電子カルテを円滑に運用するため、電子カルテに関する運用を担当する担当者(以下「運用担当者」という。)として情報システム課長を充てる。

4)　電子カルテ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、電子カルテ運用委員会を置く。なお、電子カルテ運用委員会の運用規程については、別途定める。

5)　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、電子カルテ運用委員会の審議を経て、医療情報システム管理者がこれを定める。

４．監査体制と監査責任者の任命

1)　電子カルテを円滑に運用するため、医療情報システム管理者が指名する電子カルテ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。

　監査責任者は、副院長とする。

2)　運用責任者は、監査責任者に随時、電子カルテの監査を実施させ、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。

3)　監査の内容については、電子カルテ運用委員会の審議を経て、医療情報システム管理者がこれを定める。

4)　運用責任者は、必要な場合、臨時の監査を監査責任者に命ずること。

５．作業担当者の限定

この規定が対象とする業務に携わる担当者は、以下のとおりとする。

1) 電子カルテ不具合調整等
情報システム課員及び各部門システム担当者
2) 電子カルテ及び部門システムマスター管理
各部門システム担当者

６．電子カルテ運用マニュアル・契約書等の管理体制

1) 電子カルテ運用マニュアルの管理について
情報システム課が管理すること。
2) 契約書の管理について
用度課が管理すること。

７．患者及び電子カルテ利用者からの苦情・質問受付体制

1) 患者からの苦情・質問受け付け
各部署責任者を受付窓口とする。
2) 電子カルテ利用者からの苦情・質問受け付け
情報システム課を受付窓口とする。

８．事故対策時の責任体制

運用責任者は、緊急時及び災害時の連絡、復旧体制並びに回復手順を電子カルテ運用マニュアルに定める。

９．電子カルテ利用者への教育及び訓練等周知体制

1) 運用責任者及び運用担当者は、電子カルテのマニュアルを作成し、利用者に周知させること。
2) 運用責任者及び運用担当者は、必要に応じ操作訓練を実施すること。
3) 運用責任者及び運用担当者は、電子カルテの利用者に対し、定期的に電子カルテ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。

１０．運用責任者及び運用担当者の責務

1) 電子カルテに用いる機器及びソフトウェアを導入するにあたり、システムの機能を確認すること。
2) 電子カルテ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。
3) 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。
4) 電子カルテの利用者の登録を管理し、不正な使用を防止すること。
5) 前７項の患者及び電子カルテ利用者からの苦情・質問を受け付ける窓口を設けること。
6) 電子カルテ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。

１１．監査責任者の責務

監査責任者の責務は、前項の責務が正しく履行されているかを監査することである。

１２．電子カルテ利用者の責務

1) 電子カルテ利用者(以下「利用者」という。)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。
2) 利用者は、電子カルテ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。
3) 利用者は、電子カルテへの情報入力に際して、確定操作(入力情報が正しいことを確認する操作)を行って入力情報に対する責任を明示すること。
4) 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。
5) 利用者は、参照した情報を目的以外に使用しないこと。
6) 利用者は、患者のプライバシーを侵害しないこと。
7) 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またはシステム担当者に連絡し、その指示に従うこと。
8) 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または運用担当者に連絡し、その指示に従うこと。
9) 利用者は、離席する際は、電子カルテを一旦ログアウトすること。

１３．一般管理における運用管理事項

1) 来訪者の記録・識別、入退の制限など
   ① 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する。
   ② 入退出の記録の内容について、定期的にチェックを行う。
2) 電子カルテへのアクセス制限、記録、点検等のアクセス管理

   運用責任者は、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、監査責任者に報告する。
3) 委託契約における安全管理に関する条項

   業務を病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締結する。また、各担当者は委託作業の内容が個人情報保護の観点から適正且つ安全に行われていることを確認する。
4) 個人情報の記録媒体の管理及び廃棄の規程
   ① 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、責任者の承認を得る。
   ② 個人情報を記した媒体の廃棄にあたっては、安全かつ確実に行なわれることを運用責任者又は運用担当者が作業前に確認し、結果を記録に残す。
5) リスクに対する予防、発生時の対応

   運用責任者は、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を周知する。

１４．電子カルテ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規程

1) 各システムはその設計時、運用開始時に技術的対策と運用による対策を、基準適合チェックリストに記載し、必要時には第三者への説明に使える状態で保存する。

2) 電子カルテの保守時には、基準適合チェックリストに従って、技術的対策と運用による対策の分担を見直す。

3) 電子カルテ改造時は、最新の基準適合チェックリストに従って、技術的対策と運用による対策の分担を見直す。

１５．技術的安全対策規定

1) 利用者識別と認証の方法

① ユーザーID とパスワードを組み合わせて認証を行う。

② ユーザーID の管理は、情報システム課で行う。

2) IC カード等セキュリティ・デバイス配付の方法

① 各部門責任者が管理する。

② パソコンと Windows アカウント、デバイス ID とを Active Directory の Group Policy により制限する。

3) 情報区分とアクセス権限管理及び人事異動等に伴う見直し

ユーザーマスタの保守は情報システム課担当者が行う。

4) 時刻同期の方法

サーバーからの時刻同期を行う。

5) ウィルス等不正ソフト対策

① ウィルスバスターによりウィルス対策を行う。

② 外部データのインストール制限を行う。

6) パスワードの管理

パスワード管理から３ヶ月周期で強制変更日を設定する。

１６．情報及び情報機器の持ち出しについて

1) 持ち出し対象となる情報及び情報機器の規程

① 情報システム管理者は、情報及び情報機器の持ち出しに関しリスク分析を行い、持ち出し対象となる情報及び情報機器を規程し、それ以外の情報及び情報機器の持ち出しを禁止する。

② 持ち出し対象となる情報及び情報機器は別表としてまとめ、利用者に公開する。

2) 持ち出した情報及び情報機器の運用管理規程

① 情報及び情報機器を持ち出す場合は、所属、氏名、連絡先、持ち出す情報の内容、格納する媒体、持ち出す目的、期間を別途定める書式で情報システム管理者に届け出

て承認を得る。

② 情報システム管理者は、情報が格納された可搬媒体及び情報機器の所在について台帳に記録する。そして、その内容を定期的にチェックし、所在状況を把握する。

3) 持ち出した情報及び情報機器への安全管理措置

① 持ち出す情報機器について、起動パスワードを設定する。そのパスワードは推定しやすいものは避け、また定期的に変更する。

② 持ち出す情報機器について、ウィルス対策ソフトをインストールしておく。

③ 持ち出した情報機器を定められている以外のアプリケーションがインストールされた情報機器で取り扱わない。

④ 持ち出した情報機器には、定められている以外のアプリケーションをインストールしない。

4) 盗難、紛失時の対応策

持ち出した情報及び情報機器の盗難、紛失時には、直ちに情報システム管理者に届ける。

5) 利用者への周知徹底方法

① 運用責任者及び運用担当者は、情報及び情報機器の持ち出しについて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しておく。

② 運用責任者及び運用担当者は、利用者に対し、情報及び情報機器の持ち出しについて研修を行う。また、研修時のテキスト、出席者リストを残す。

１７．外部の機関と医療情報を提供・委託・交換する場合

1) 安全を技術的、運用的面から確認する規程

① 運用責任者及び運用担当者は、外部の機関と医療情報を交換する場合、リスク分析を行い、安全に運用されるように技術的及び運用的対策を講じる。

② 技術的対策が適切に実施され問題がないか定期的に監査を行って確認する。

１８．教育と訓練の取扱い及びプライバシー保護に関する研修

1) マニュアルの整備

運用責任者及び運用担当者は、電子カルテの取扱いについて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しておく。

2) 定期または不定期な電子保存システムの取扱い及びプライバシー保護に関する教育・研修

運用責任者及び運用担当者は、利用者に対し、定期的に電子カルテの取扱い及びプライバシー保護に関する研修を行う。また、研修時のテキスト、出席者リストを残す。

１９．災害等の非常時の対応

1) 運用について

① 災害、サイバー攻撃等により一部医療行為の停止等医療サービス提供体制に支障が発生する非常時の場合、電子カルテ運用マニュアルに従い紙カルテで運用を行う。

② どのような状態を非常時と見なすかについては、別途定める基準、手順に従って運用責任者が判断する。

2) 報告先と内容一覧

災害、サイバー攻撃等により一部医療行為の停止等医療サービス提供体制に支障が発生した場合、別途定める非常連絡網の連絡先に連絡する。

２０．電子保存のための運用管理事項

1) 真正性確保

① 作成者の認識及び認証

運用責任者または運用担当者は、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程し、不正な使用を防止する。

② パスワードの最低文字数、有効期間等を規程する。

③ 認証の有効回数、超過した場合の対処を規程する。

④ 運用管理者又は運用担当者は、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。

⑤ 情報の確定手順と、作成責任者の識別情報の記録

- 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(入力情報が正しいことを確認する操作)を行って、入力情報に対する責任を明示する。
- 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。

⑥ 更新履歴の保存

- 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(入力情報が正しいことを確認する操作)を行って、入力情報に対する責任を明示する。
- 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。

⑦ 代行操作の承認記録

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。

⑧ 機器・ソフトウェアの品質管理、動作状況の内部監査規程

運用責任者または運用担当者は、システム構成やソフトウェアの動作状況に関する内部監査を定期的に実施する。

2) 見読性確保

① 情報の所在確認

運用責任者または運用担当者は、定期的に情報の所在確認を行う。

② 見読化手順の管理

電子保存に用いる機器及びソフトウェアを導入するにあたって、保存義務のある情報として電子保存された情報毎に見読用機器を常に可能な状態に置いておく。

③ 見読目的に応じた応答時間とスループット

運用責任者または運用担当者は、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。

④　システム障害対策

運用責任者または運用担当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。また、データバックアップ作業が適切に行われていることを確認する。

3)　保存性確保

①　ソフトウェア・機器・媒体の管理

- 運用責任者または運用担当者は、電子保存システムで使用されているソフトウェアを、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。
- 電子保存システムの記録媒体を含む主要機器は、管理者によって入退室管理された場所に保存する。
- 運用責任者または運用担当者は、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。
- 設置場所には無水消火装置、漏電防止装置、無停電電源装置等を備える。
- 設置機器は定期的に点検を行う。

②　不適切な保管・取扱いによる情報の滅失、破壊の防止策

- 運用責任者または運用担当者は、新規の業務担当者には操作前に教育を行う。
- 定期的な差分バックアップとフルバックアップのスケジュール化を行う。
- ログ記録と操作履歴の表示を行うとともにログ採取と監視を行う。

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策

- 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。

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策

機器・媒体やソフトウェアの変更にあたっては、データ移行のための業務計画を作る。

⑤　相互運用性確保

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。

２１．その他

この規程は、平成３０年１２月１８日から適用する。