公立福生病院医療情報システムの安全管理に関する運用管理規程

平成31年２月18日
規程第３号

改正
令和２年９月１日企業管理規程第38号
公立福生病院医療情報システムの安全管理に関する運用管理規程

（目的）
第１条　この規程は、公立福生病院（以下「当院」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。
（対象情報）
第２条　対象システムは、電子カルテシステム及び別に定めるシステムである。
２　対象システムの扱う情報については、そのシステムごとに別途定義と安全管理上の重要度の分類を行い、リスク分析を行い表に記入し保管すること。
（標準規格）
第３条　システム管理者は、厚生労働省標準規格についての変更状況を確認し、システムの変更・改造時の対象とすること。
（管理体制）
第４条　当院に運用責任者及び個人情報保護責任者を置き、院長をもってこれに充てること。
２　院長は必要な場合、運用責任者及び個人情報保護責任者を別に指名すること。
３　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管理者（以下「システム管理者」という。）を置くこと。
４　システム管理者は院長が指名すること。
５　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、院長のもとに公立福生病院情報セキュリティ会議（以下「セキュリティ会議」という。）を置くこと。
６　セキュリティ会議の運営については、別途定めること。
７　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、セキュリティ会議の審議を経て、院長がこれを定めること。
（マニュアル・契約書等の文書の管理体制）
第５条　契約書、マニュアル等の文書の管理については、福生病院企業団文書管理規程（平成12年４月１日規程第１号）に基づくこと。
（監査体制と監査責任者）
第６条　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。
２　監査責任者は院長が指名すること。
３　運用責任者は、監査責任者に必要な都度、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。
４　監査の内容については、セキュリティ会議の審議を経て、院長がこれを定めること。
５　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。
（システム利用者からの苦情・質問の受け付け体制）
第７条　利用者からの、情報システムについての苦情・質問を受け付ける窓口を設けること。

２　苦情・質問受け付け後は、その内容を検討し、速やかに必要な措置を講じること。

（事故対策時の責任体制）

第８条　システム管理者は、緊急時及び災害時の連絡、復旧体制を定め、利用者に周知の上、常に利用可能な状態に置くこと。

（システム利用者への教育・訓練等周知体制）

第９条　システム管理者は、情報システムの取扱いを利用者に周知し、常に利用可能な状態に置くこと。

２　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。

（管理者の責務）

第10条　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。

２　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。

３　診療情報の安全性を確保し、常に利用可能な状態に置くこと。

４　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。

５　システム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設定し、不正な利用を防止すること。

６　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。

７　患者及び利用者からの、情報システムについての問い合わせや苦情を受け付ける窓口を設けること。

（利用者の責務）

第11条　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。

２　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。

３　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。

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、目的外に利用しないこと。

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、速やかにシステム管理者に連絡し、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、速やかにシステム管理者に連絡し、その指示に従うこと。

９　利用者は、離席する際は、ログアウトすること。

（来訪者の記録・識別、入退の制限等の入退管理）

第12条　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。

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こと。

（情報保存装置、アクセス機器の設置区画の管理・監視）

第13条　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こと。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こと。

（情報へのアクセス権限の決定方針）

第14条　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こと。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こと。

（個人情報を含む記録媒体の管理（保管・授受等））

第15条　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、システム管理者の承認をうること。

（個人情報を含む媒体の廃棄）

第16条　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、発生時の対応方法）

第17条　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、運用管理方法の見直しを行うこと。また、事故発生に対しては、速やかに運用責任者に報告し利用者に周知すること。

（情報システムの安全に関する技術的と運用的対策）

第18条　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こと。

２　システムの保守時には、基準適合チェックリスト記載にしたがっていることを確認すること。

３　システム改造時は、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こと。

（無線ＬＡＮに関する事項）

第19条　システム管理者は、無線ＬＡＮアクセスポイントの設定状態を適宜確認すること。

２　システム管理者は、無線ＬＡＮ利用規則を院内関係者へ説明をすること。

（電子署名・タイムスタンプに関する管理）

第20条　システム管理者は、電子署名、タイムスタンプに関する作業手順を定めること。

２　システム管理者は、電子的に受領した文書に電子署名が有る場合の、署名検証手順を定めること。

（業務委託（システムの運用・保守・改造）の安全管理措置）

第21条　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医療機関関係者による作業管理・監督、作業報告確認）

第22条　システム管理者は、保守会社における保守作業に関し、その作業者及び作業内容につき報告を求め適切であることを確認すること。必要と認めた場合は適時監査を行うこと。

（持ち出し対象となる情報及び情報機器の管理）

第23条　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管理し、それ以外の情報及び情報機器の持ち出しを禁止すること。

２　持ち出し対象となる情報及び情報機器は電子カルテシステムを除くこと。

（持ち出した情報及び情報機器の運用管理）

第24条　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、期間を管理者に届け出て、承認を得ること。

２　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こ

と。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こと。

（持ち出した情報及び情報機器への安全管理措置）

第25条　持ち出す情報機器について起動パスワードを設定すること。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こと。

２　持ち出す情報機器について、ウイルス対策ソフトをインストールして置くこと。

３　持ち出した情報を、不正な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こと。

４　持ち出した情報機器には、不正なアプリケーションをインストールしないこと。

（盗難、紛失時の対応策）

第26条　持ち出した情報及び情報機器の盗難､紛失時には､直ちにシステム管理者に届け出ること。

２　届け出を受け付けたシステム管理者は、その情報及び情報機器の重要度にしたがって対応すること。

（利用者への周知徹底方法）

第27条　システム管理者は、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、利用者に周知の上、常に利用可能な状態に置くこと。

２　システム管理者は、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こと。また、研修時のテキスト、出席者リストを残すこと。

（外部の機関と医療情報を提供・委託・交換する場合）

第28条　システム管理者は、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こと。

２　技術的対策が適切に実施され問題がないかを定期的に監査を行って確認すること。

（リスク対策の検討文書の管理）

第29条　システム管理者は、リスク対策の検討文書を作成し管理すること。

（外部の機関との医療情報の提供・交換・委託）

第30条　外部の機関と医療情報を交換する場合、相手の医療機関、通信事業者及び運用委託業者等との間で、責任分界点や責任の所在を契約書等で明確にすること。

２　上記契約状態が適切に維持管理されているか定期的に監査を行って確認すること。

（リモートメンテナンスの基本方針）

第31条　外部の保守会社からリモートメンテナンスを受ける場合､相手の保守会社等､通信事業者、運用委託業者等との間で、責任分界点や責任の所在を契約書等で明確にすること。

２　上記契約状態が適切に維持管理されているか定期的に監査を行って確認すること。

（従業者による医療機関等の外部からアクセスする場合の運用管理規程）

第32条　外部からアクセスを許容する機器については、その機器が許可された際の状態を保持していることを定期的に確認すること。

（災害等の非常時の対応）

第33条　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、事業継続計画（ＢＣＰ）にしたがって運用を行うこと。

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

（システムの縮退運用管理）

第34条　システムの縮退運用時や非常時の運用に関しては、利用者に周知し常に利用可能な状態に置くこと。

（非常時の機能と運用管理）

第35条　別途定める、「障害時運用マニュアル」により、非常時の運用を行う。

（報告先と内容一覧）

第36条　災害、サイバー攻撃などにより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した場合、関係者に連絡すること。

（教育と訓練）

第37条　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置くこと。

（従業者に対する人的安全管理措置）

第38条　当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。

附　則

この規程は、平成31年４月１日から施行する。

附　則（令和２年９月１日企業管理規程第38号）

この規程は、令和２年９月１日から施行し、令和２年４月１日から適用する。