

国保国吉病院組合医療情報システム運用管理規程

(趣旨)

第1条 この規程は、国保国吉病院組合情報セキュリティ基本方針（以下「基本方針」という。）に基づき、国保国吉病院組合（以下「当組合」という。）の医療情報を適正に保存、活用するため、医療情報システムで使用される機器、ソフトウェア及びその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し必要な事項を定める。

(対象システム及び対象情報)

第2条 この規程の対象となるシステムは、当組合で運用する電子カルテシステム及び同システムと接続する全ての部門システム並びに接続機器など診療情報を取り扱うシステム（以下「医療情報システム」という。）とする。

(職及び組織)

第3条 医療情報システムの適正な運用を図るため、基本方針第7項に基づき、次の職及び組織を置く。

- (1) 医療情報システム運用責任者（以下「運用責任者」という。）
- (2) 個人情報保護責任者
- (3) 医療情報システム管理者（以下「システム管理者」という。）
- (4) 医療情報システム安全管理者
- (5) 医療情報システム部門管理者（以下「部門管理者」という。）
- (6) 医療情報システム監査責任者（以下「監査責任者」という。）
- (7) 医療情報システム委員会（以下「システム委員会」という。）

(窓口の設置)

第4条 基本方針第15項に基づき、医療情報システムに関する苦情、相談等を受け付ける窓口を設置するものとし、苦情、相談等を受け付けたときは、その内容を検討し、直ちに必要な措置を講ずる。

(医療情報システム)

第5条 医療情報システムは、次の各号に掲げる基本原則に則り運用する。

- (1) 保存義務のある情報の電子媒体による保存については、情報の真正性、見読性、保存性を確保する。

- (2) 医療情報システムの利用にあたっては、守秘義務を遵守し、患者個人の情報を保護する。
- (3) 医療情報システムへのコンピュータ・ウイルスの侵入及び外部からの不正アクセスに対しては、必要な対策を直ちに講じる。ソフトウェアのインストールは、システム管理者が必要と認定したもののみとし、それ以外のインストールを禁止する。許可のない端末へは、U S Bメモリ等との接続を禁止する。
- (4) 医療情報システムは、原則として外部への情報持出しは禁止とする。
- (5) 医療情報システムのパスワードは英数字、記号が混在した8文字以上とし、定期的に変更すること。

(電子保存に関する理念)

第6条 医療情報システムの管理者及び利用者は、保存義務のある情報の電子媒体による保存が、自己責任の原則に基づいて行われることをよく理解しておかなければならない。

- 2 管理者及び利用者は、電子媒体に保存された情報の真正性、見読性、保存性を確保し、かつ、情報が患者の診療や病院の管理運営上必要とされるときに、信頼性のある情報を迅速に提供できるよう、協力して環境を整え、適正な運営に努めなければならない。
- 3 管理者及び利用者は、診療情報の二次的利用についても、患者のプライバシーが侵害されることのないよう「国保国吉病院組合個人情報保護規程」に基づき取り扱わなければならない。

(運用責任者の責務)

第7条 運用責任者は、医療情報システムの機能が支障なく運用される環境を整備しなければならない。

- 2 運用責任者は、監査責任者に監査を実施させ、その結果の報告を受けて、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なければならない。

(システム管理者の責務)

第8条 システム管理者は、次の各号に掲げる事項を確実に実施しなければならない。

- (1) 医療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場合は、それにより医療情報システムの機能に支障が生じないよう十分に確認すること。
- (2) 医療情報の漏えい等に対して十分な安全性を確保すると同時に、医療情報が常に利用可能な状態に置いておくこと。
- (3) 医療情報システムに用いる機器やソフトウェアに変更があった場合にも、医療情報が支障なく継続して使用できるように維持すること。
- (4) 利用者の登録を管理し、利用者の職種等から、そのアクセス権限を規定し、不正な利用を

防止すること。

- (5) 医療情報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。
- (6) 医療情報システムについての患者又は利用者からの苦情、相談等に対し必要な措置を講じること。
- (7) 事業者から製造業者／サービス事業者による医療情報セキュリティ開示書の提示を求め、確認を行うこと。
- (8) 退職者や長期間使用していないアカウントは削除または無効化すること。
- (9) その他、医療情報システムの維持管理に必要と認められること。

(部門管理者の責務)

第9条 部門管理者は、次の各号に掲げる事項を確実に実施しなければならない。

- (1) 自部門のシステムの運用の管理に責任を持つこと。
- (2) 自部門のマスタを管理すること。
- (3) 自部門のマスタに変更・追加が生じた場合には、速やかに関連部署の部門管理者ならびにシステム管理者に報告すること。
- (4) マスタの変更の際に、過去の情報に対する内容の変更が起こらない機能を備えること。
- (5) その他、部門システムの維持管理に必要と認められること。

(監査責任者の責務)

第10条 監査責任者は、次の各号に掲げる事項を確実に実施しなければならない。

- (1) 監査計画を立案し、監査を指揮し、監査報告書を作成し、医療情報システム運用責任者に報告すること。
- (2) 医療情報システムの監査を円滑に実施するため、監査を担当する監査員を置くことができる。
- (3) 監査員の選定及び監査の実施においては、監査の客観性及び公平性を確保すること。
- (4) 監査員は自らの所属する部門を監査しないこと。

(利用者の責務)

第11条 利用者は、次の各号に掲げる事項を遵守しなければならない。

- (1) 自身の認証番号やパスワードを適切に管理し、これを他者に利用させないこと。
- (2) 医療情報システムへのアクセスに際して、認証番号やパスワード等によって、システムに利用者自身を認識させること。
- (3) 情報入力に際して確定操作を行い、入力情報に対する責任を明示すること。

- (4) 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) 参照した情報を、目的外に利用しないこと。
- (6) 患者のプライバシーを尊重し、職務上必要な情報以外の情報にアクセスしてはならない。
- (7) アクセスにより知り得た情報を正当な理由なしに漏らしてはならない。職務を離れた後も同様とする。
- (8) 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。
- (9) 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。
- (10) 離席する際には、ログアウト操作またはスクリーンロック等を行うこと。
- (11) ウイルス感染またはその恐れを発見した場合は、ネットワークから端末を切り離すとともに、システム管理者へ連絡し、その指示に従うこと。

(アクセス管理)

第12条 システム管理者は、以下の内容に沿ってアクセス管理を行い、必要に応じて管理状況を安全管理者等に報告する。

- (1) 職種によりアクセス権限を設定し、必要に応じた権限を付与すること。
- (2) サーバへのアクセスは許可を得た者のみとし、パスワードはシステム管理者が管理すること。
- (3) ID、パスワード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こと。
- (4) アクセスログは、特定の担当者以外がアクセスできない仕組みとすること。
- (5) USBメモリ等の使用は原則禁止とし、サーバにて接続制御すること。業務上必要な場合は、所定の手続きにより許可を得ること。

(システムの機能要件)

第13条 医療情報システムは、次の機能を備えるものとする。

- (1) アクセスしようとする者の識別と認証
- (2) 機密度に応じたアクセス権限の設定と不正アクセスの排除機能
- (3) 入力情報についての確定操作機能
- (4) 確定操作が行われた情報の正確な保存機能
- (5) 情報の記録・更新に際し、その日時及び実施者を記録する機能
- (6) 必要がある場合、記録されている情報を速やかに出力する機能
- (7) 情報の所在を一元的に管理できる機能
- (8) 情報の利用範囲、更新履歴、機密度等に応じた管理区分設定機能

(9) アクセスログの保存及び追跡調査機能

(10) 情報のバックアップ作成機能

(機器の管理)

第14条 医療情報システムの記録媒体を含む主要機器は、原則として独立したサーバ室に設置する。

2 サーバ室は常時施錠し、システム管理者が入退室の管理を行う。

3 サーバ室には必要な防災設備、無停電電源装置等を備え、定期的に点検を行う。

4 管理者は、機器の台帳管理を行い、リモート保守の状況についても適切に管理する。

(データのバックアップ)

第15条 医療情報システムのバックアップを定期的に取り得し、適切に保管する。

2 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。

(ソフトウェアの管理)

第16条 システム管理者は、使用されるソフトウェアについて事前に審査を行い、安全性を確認する。

2 システム管理者は、ネットワークや可搬型媒体による情報授受について、必要に応じて制限を設ける。

3 システム管理者は、定期的にウィルスチェックを行い、感染防止に努める。

(ネットワークの管理)

第17条 システム管理者は、定期的に利用履歴を検査し、不正利用の有無を確認する。

2 ネットワークの不正利用を発見した場合には、直ちに原因究明と対策を実施する。

3 ネットワーク機器の接続制限については、FortiClient等の認証やSSID隠蔽、暗号化(WPA2/WPA3等)により、許可された端末のみを接続可能とする。

(事故対策)

第18条 システム管理者は、緊急時・災害時の体制として事業継続計画(BCP)を定め、非常時にも参照可能な形態で保管する。

2 利用者に対し、事故発生時の速やかな報告を徹底させる。

3 重大な障害が発生した場合には、速やかにシステム委員会を開催し対策を協議する。

4 部門システムでの障害時は、部門管理者が業者と連携して復旧にあたり、状況を報告する。

(マニュアルの整備)

第19条 管理者は、システムの取扱いマニュアルを整備し、利用者が常に参照できる状態におく。

(教育と訓練)

第20条 システム管理者は、利用者に対し、システムの取扱い及び個人情報保護に関する研修を定期的に行う。

(監査)

第21条 運用責任者は、監査責任者に定期的な監査を実施させ、報告に基づく改善措置を講じる。

2 運用責任者は、必要に応じて臨時の監査を命ずることができる。

3 監査の詳細は、別途定める「監査細則」等による。

(罰則)

第22条 この規程に違反したときは、当組合の服務規程等に基づき処分を行う。

(その他)

第23条 この規程の実施に関し必要な事項は、医療情報システム運用責任者がこれを定める。

附 則

この訓令は、令和8年3月1日から施行する。