医療情報システムに関する運用管理規程

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、下記の運用管理を規程する。

(1). 一般管理事項

① 総則

a) 理念

・この規程は、下越病院（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。

b) 対象情報

・当院において、対象とする情報の範囲については、②に規程する委員会の審議を経て、病院長がこれを定める。

c) 情報システムにおいて採用し変更をフォローすべき標準規格

・システム管理者は、情報システムで使われている標準規格についてベンダへ情報提供を要求し、システムの変更・改造時の対象とする。

② 管理体制

a) システム管理者、機器管理者、運用責任者、安全管理者、個人情報保護責任者等

・当院に運用責任者および個人情報保護責任者を置き、病院長をもってこれに充てる。

・病院長は必要な場合、運用責任者および個人情報保護責任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管理者（以下「システム管理者」という。）を置く。

・システム管理者は病院長が指名する。

・情報システムに関する取り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。

・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~~管理会議がこれを定める。

b) マニュアル・契約書等の文書の管理体制

・マニュアルについては診療情報課が管理し、契約書等の文書については事務長室が管理する。

c) 監査体制と監査責任者

・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。

・監査責任者は病院長が指名する。

・運用責任者は、監査責任者に随時、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。

・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。

・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。

d)　患者及びシステム利用者からの苦情・質問の受け付け体制

・患者及び利用者からの、情報システムについての苦情・質問については各職場責任者を受け付け窓口とする。

・苦情・質問受付後は、その内容を検討し、速やかに必要な措置を講じる。

e)　事故対策時の責任体制

・システム管理者は、緊急時および災害時の連絡、復旧体制並びに回復手順を定め文書化し、利用者に周知の上、常に利用可能な状態におく。

f)　システム利用者への教育・訓練等周知体制

・システム管理者は、情報システムの取り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。

・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り扱い及びプライバシー保護に関する研修を行う。

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

・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。

・情報システムの機能案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。

・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。

・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。

・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規程し、不正な利用を防止する。

・情報システムを正しく利用させるため、作業手順の整備を行い利用者の教育と訓練を行う。

・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については各職場責任者を受付窓口とする。

b)　監査責任者の責務

・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。

c)　利用者の責務

・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。

・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。

・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。

・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。

・利用者は、参照した情報を、目的外に利用しない。

・利用者は、患者のプライバシーを侵害しない。

・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。

・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。

・利用者は、離席する際は、ログアウトする。

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規程

・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。

・入退出の記録の内容について定期的にチェックを行う。

b)　情報保存装置、アクセス機器の設置区画の管理・監査規程

・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)　情報へのアクセス権限の決定方針

・②に規程する委員会の審議を経て、病院長がこれを定める。

d)　個人情報を含む記録媒体の管理（保管・授受等）規程

・保管、バックアップの作業に当たるものは、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。

e)　個人情報を含む媒体の廃棄の規程

・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。

f)　リスクに対する予防、発生時の対応方法

・システム管理者は、業務上において情報漏洩などのリスクが予想されるものに対し、運用管理規程の見直しを行う。また、事故発生に対しては、速やかに運用担当者に報告し利用者に周知する。

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規程

・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。

・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。

・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。

h)　技術的安全対策規程

- 利用者識別と認証の方法
  - ・ユーザ ID とパスワードを組み合わせて認証を行う。
  - ・ユーザ ID の管理は人事担当者が行う。
- IC カード等セキュリティ・デバイス配布の方法
  - ・各職場責任者が管理する。

・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。

- 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
  ・ユーザマスタの保守は人事担当者が行う。
- アクセスログ取得と監査の手順
  ・ RevoHIS によるログ記録と操作履歴の表示。
  ・ MyLogstar によるログ採取と監視を行う。
- 時刻同期の方法
  ・ NTP サーバからの時刻同期を行う。
- ウイルス等不正ソフト対策
  ・ウイルスバスターによりウイルス対策を行う。
  ・ Active Directory の Group Policy を使い、インストール制限、Winny 等の動作制限を行う。
- ネットワークからの不正アクセス対策
  ・ TCP/IP プロトコルのみとし、Active Directory による機器の管理を行う。
  ・ L2Blocker による ARP(Address Resolution Protocol)パケットの監視を行う。
- パスワードの管理
  ・ RevoHIS により、パスワード変更から ~~40 日周期~~ 3 ヶ月周期で強制変更日を設定する。

i)　無線 LAN に関する事項

・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。

- 無線 LAN 設定（アクセス制限、暗号化等）
  ・ WPA/AES による暗号化。SSID 対応。
  ・ L2Blocker による ARP(Address Resolution Protocol)パケットの監視を行う。
- 電波障害の恐れがある機器の使用制限
  ・ IEEE802.11a(5.2GHz 帯)を使用する。

⑤　業務委託（システムの運用・保守・改造）の安全管理措置

a)　業務委託契約における安全管理・守秘条項

・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。

b)　再委託の場合の安全管理措置事項

・業務委託の契約書には、再委託での安全管理に関する事項を含む。

c)　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

・システム管理者は、保守会社における保守作業に関し、その作業者およ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。必要と認めた場合は適時監査を行う。

- 保守要員専用のアカウントの作成及び運用管理
  ・専用のアカウントを用意する。

- アクセスログの採取と確認
  - MyLogstar によるログ採取と監視を行う。

⑥ 情報及び情報機器の持ち出しについて

a) 持ち出し対象となる情報及び情報機器の規程

・システム管理者は、情報およ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および情報機器を規程し、それ以外の情報および情報機器の持ち出しを禁止する。

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

b) 持ち出した情報及び情報機器の運用管理規程

・情報およ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システム管理者に届け出て、承認を得る。

・システム管理者は、情報が格納された過般媒体およ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。

c) 持ち出した情報及び情報機器への安全管理措置

・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。

・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おく。

・持ち出した情報を、別途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。

・持ち出した情報機器には、別途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。

d) 盗難、紛失時の対応策

・持ち出した情報および情報機器の盗難、紛失時には、直ちにシステム管理者に届け出る。

e) 利用者への周知徹底方法

・システム管理者は、情報およ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おく。

・システム管理者は、利用者に対し、情報およ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。

⑦ 外部の機関と医療情報を提供・委託・交換する場合

a) 安全を技術的、運用的面から確認する規程

・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別途定める技術的および運用的対策を講じる。

・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。

b) リスク対策の検討文書の管理規程

c) 情報処理事業者等との通常運用時、事故対処時それぞれでの責任分界点を定めた契約文書の管理と契約状態の維持管理規程

d)　リモートメンテナンスの基本方針

・定期的に監査を行って確認する。

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

・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、紙カルテで運用を行う。

・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。

d)　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。

⑨　教育と訓練

a)　マニュアルの整備

・システム管理者は、情報システムの取り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。

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

・システム管理者は、利用者に対し、定期的に情報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を行う。また、研修時のテキスト、出席者リストを残す。

c)　従業者に対する人的安全管理措置

・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。

⑩　監査

a)　監査の内容

・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。

・監査責任者は病院長が指名する。

・システム管理者は、監査責任者に随時、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。

・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。

・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。

(2). 電子保存のための運用管理事項

①　真正性確保

a)　作成者の識別及び認証

・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程し、不正な利用を防止する。

・パスワードの最低文字数、有効期間等を別途規程する。
・認証の有効回数、超過した場合の対処を別途規程する。
・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。
・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。
・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。
・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。

b) 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。

c) 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。

d) 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。

e) 機器・ソフトウェアの品質管理、動作状況の内部監査規程
・システム管理者は、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

a) 情報の所在管理
・システム管理者は定期的に情報の所在確認を行う。

b) 見読化手段の管理
・電子保存に用いる機器及びソフトウェアを導入するに当たって、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利用可能な状態に置いておく。

c) 見読目的に応じた応答時間とスループット
・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。

d) システム障害対策
・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ことを確認する。

- 冗長性
  - SQL Server の分散化とレプリケーション。

・主サーバ群を RAID5 構成、レプリケーションサーバ群を RAID1 構成にする。
・ドメインコントローラと DNS サーバを冗長構成にする。

- バックアップ

・ Backup Exec により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。
・SQL Server による定期的なトランザクション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。

- 緊急対応

・リアルタイムにトランザクションレプリケーションを行うワークステーションで閲覧可能な状態を確保する。
・機器が動作しなくなった場合は、「臨時紙カルテ」用紙での対応とする。

③ 保存性確保

a) ソフトウェア・機器・媒体の管理

・システム管理者は、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。
・システム管理者は、定期的にソフトウェアのウイ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。

- 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

・ウイルスバスターによりウイルス対策を行う。
・ Active Directory の Group Policy を使い、インストール制限、Winny 等の動作制限を行う。

b) 不適切な保管・取扱いによる情報の滅失、破壊の防止策

・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。

- バックアップ、作業履歴管理

・ Backup Exec により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。
・SQL Server による定期的なトランザクション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。
・ RevoHIS によるログ記録と操作履歴の表示。
・ MyLogstar によるログ採取と監視を行う。

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

・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。

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

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

④　相互運用性確保

a)　システムの改修に当たっての、データ互換性の確保策

・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。

この規程は 2009 年 6 月 1 日より施行する。

2009 年 12 月 11 日改訂。

2015 年 9 月 29 日改訂