名称	下越病院　医療情報システム運用管理規程				総頁数	8
作成日	2009.06.01	更新日	2017.3.13	作成部署・委員会	情報システム管理委員会	

下越病院管理会議

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

（1）理念

①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。

（2）対象情報

①当院において、対象とする情報の範囲については、1．2）管理体制に規程する委員会の審議を経て 、病院長がこれを定める。

（3）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

①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こと。

2）管理体制

（1）システム管理者、運用責任者、個人情報保護責任者等

①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。

②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。

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。

④システム管理者は病院長が指名する。

⑤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委員会を置く。

⑥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、情報システム委員会の審議を経て、病院長がこれを定める。

（2）マニュアル・契約書等の文書の管理体制

①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。

（3）監査体制と監査責任者

①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。

②監査責任者は病院長が指名する。

③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。

④監査の内容については、情報システム委員会の審議を経て、病院長がこれを定める。

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。

（4）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

①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。

②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。

（5）事故対策時の責任体制

①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。

（6）システム利用者への教育・訓練等周知体制

①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。

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

（1）システム管理者や機器管理者、運用責任者の責務

①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。

②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。

③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。

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。

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規程し、不正な利用を防止する。

⑥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。

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については各職場責任者を受付窓口とする。

（2）監査責任者の責務

①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。

（3）利用者の責務

①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。

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。

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。

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。

⑤利用者は、参照した情報を、目的外に利用しない。

⑥利用者は、患者のプライバシーを侵害しない。

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。

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。

⑨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

（1）来訪者の記録・識別、入退の制限等の入退管理規程

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を残す。

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）情報保存装置、アクセス機器の設置区画の管理・監査規程

①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。

（3）情報へのアクセス権限の決定方針

①1．2）管理体制に規程する委員会の審議を経て、病院長がこれを定める。

（4）個人情報を含む記録媒体の管理（保管・授受等）規程

①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。

（5）個人情報を含む媒体の廃棄の規程

①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。

（6）リスクに対する予防、発生時の対応方法

①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、速やかに運用責任者に報告し利用者に周知する。

（7）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

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。

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。

（8）技術的安全対策規程

①利用者識別と認証の方法

a　ユーザ ID とパスワードを組み合わせて認証を行う。

b　ユーザ ID の管理は人事担当者が行う。

②IC カード等セキュリティ・デバイス配布の方法

a　各職場責任者が管理する。

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

a　ユーザマスタの保守は人事担当者が行う。

b　メンテナンスプログラムを使用できる PC を特定する。

④アクセスログ取得と監査の手順

a　電子カルテの機能によるログ記録と操作履歴の表示。

b　利用者ログの証拠性確保のため、記録する時刻について精度の高いものを使用する必要がある。

⑤時刻同期の方法

a　NTP サーバからの時刻同期を行う。

⑥ウイルス等不正ソフト対策

a　ウィルス対策ソフトによりウイルス対策を行う。

b　利用者が勝手にソフトをインストールできないような設定を PC に施す。

⑦ネットワークからの不正アクセス対策

a　電子カルテネットワークは閉鎖ネットワークで、外部と接点をもたせない。

b　各種端末および通信機器には静的に IP アドレスを付与する。

c　ネットワークに流れるハードウェアアドレス情報(ARP パケット)の監視を行い、不正端末のアクセス検知と遮断を行う。

⑧パスワードの管理

a　電子カルテのログオンパスワードは、パスワード変更から 3 ヵ月で強制変更日を設定する。

（9）無線 LAN に関する事項

①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。

②利用者以外に無線 LAN の利用を特定されないようにすること

a　ネットワーク識別名(SSID)設定によりアクセス制限を行う。

b　ネットワーク識別名(SSID)を隠蔽設定する。

③不正な情報の取得を防止すること

a　無線 LAN の暗号化方式に WPA/AES を採用し、通信の暗号化を行う。

④無線 LAN のセキュリティ対策については、総務省発行の「安心して無線 LAN を使用するために」を参

考にして対策を実施する。

5）業務委託（システムの運用・保守・改造）の安全管理措置

（1）業務委託契約における安全管理・守秘条項

①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。

（2）再委託の場合の安全管理措置事項

①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。

（3）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

①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。

a　保守要員専用のアカウントの作成及び運用管理

b　保守作業等の情報システムに直接アクセスする作業の際には、作業者・作業内容作業結果の確認(原則として日単位)。

c　清掃等、直接情報システムにアクセスしない作業の場合の定期的なチェック。

d　保守契約における個人情報保護の徹底。

e　保守作業の安全性についてログによる確認。

6）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定し、それ以外の情報および情報機器の持ち出しを禁止する。

②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。

（2）持ち出した情報及び情報機器の運用管理規程

①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。

②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。

（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。

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おく。

③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。

④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。

（4）盗難、紛失時の対応策

①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。

②届け出を受け付けたシステム管理者は、その情報および情報機器の重要度に従って対応する。

（5）利用者への周知徹底方法

①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。

②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）医療系ネットワークとネット系ネットワーク間のファイル転送規程

（1）医療情報の2次利用データおよびその他利用者が作成した文書データを、医療系とネット系の両ネットワーク間で双方向にファイル転送する方法

①ファイルの転送には専用の転送ツールを使用する。

②ファイル転送ツールの使用には、ユーザ ID とパスワードによる認証を必要とする。

③ファイル転送ツールの機能

a　利用者、操作日時、転送したファイル名を操作履歴として記録する

b　転送したデータを特定の場所に任意の期間保存する。

（2）想定する転送ファイル

①医療系→ネット系

a　学会等発表資料(データの収集・分析は医療系の PC で行い、個人を特定できる情報が含まれない形になったものとする。)

b　統計資料(経営資料、診療分析資料、医事統計資料等)

c　利用者がオフィスソフトで作成した文書(基準、マニュアル、議事録、その他)

d　電子カルテメーカーへの問い合わせデータ(個人を特定する必要がある場合は、個人を特定できる情報として患者 ID のみの表示可とする)

②ネット系→医療系

a　利用者がオフィスソフトで作成した文書(基準、マニュアル、議事録、その他)

（3）ファイル転送ツールは、医局と医局以外(一般)で分けて運用する。

①共通事項

a　ファイル転送ツールの使用者は、転送するファイルに個人を特定できる情報がふくまれていない事を確認する。

②医局運用

a　ユーザ ID は、全医師に用意する。

③一般運用

a　ユーザ ID は職責者に用意するものとし、委員会の委員長・事務局長等で業務上必要なものに関しては、管理部に決裁を受けるものとする。

（4）ファイル転送ツールの利用者管理

①ファイル転送ツール専用でユーザ管理を行い、他のシステムのユーザマスタと共有しない。

②利用者の決裁は情報システム委員会で行う。

③ユーザマスタ保守は診療情報管理課が行う。

（5）転送ファイルの監査

①医局で就業時間外に行われた転送処理については、翌就業時間内に診療情報管理課でファイルの内容点検を行う。

②システム管理者は、定期的にファイル転送ツールの操作履歴、及び転送したファイルの内容を確認し、不正な転送がされていないか確認する。

8）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。

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。

（2）リスク対策の検討文書の管理規程

①リスク対策の検討文書を作成し維持・管理する。

（3）契約文書の管理と契約状態の維持管理規定

①外部の機関と医療情報を交換する場合、相手の医療機関等、通信事業者、運用委託業者などとの間で、責任分界点や責任の所在を契約書等で明確にする。

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。

（4）リモートメンテナンスの基本方針

①定期的に監査を行って確認する。

9）災害等の非常時の対応

（1）医療情報システムの事業継続計画(BCP)

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、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

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した場合、別途定める非常連絡網の連絡先に連絡する。

（3）システムの縮退運用管理

①システムの縮退運用時や非常時の運用に関して運用管理規程を作成し、利用者に周知の上、常に利用可能な状態におく。

a　システムが縮退運用を行っている際の運用ルール

b　正常復帰後に、代替手段で運用した間のデータ整合性を図る規約

10）教育と訓練

（1）マニュアルの整備

①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。

（2）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

①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。

（3）従業者に対する人的安全管理措置

①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。

11）監査

（1）監査の内容

①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。

②監査責任者は病院長が指名する。

③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。

④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。

⑤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）用語の定義

（1）電子保存システムとは、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（以下「保存義務のある情報」という。）を紙、フィルム媒体に代えて、原本として電子保存するためのシステムをいう。

（2）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である。

（3）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。

（4）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ていることである。

2）真正性確保

（1）作成者の識別及び認証

①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。

②パスワードの最低文字数は英数字混在で 8 文字以上、有効期間は最長 2 ヶ月とし、強制変更日を設定する。

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。

④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。

⑤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。

⑥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。

（2）情報の確定手順と、作成責任者の識別情報の記録

①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。

②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（自動確定は実施しない）。

（3）更新履歴の保存

①確定操作された情報は、履歴を残さないで改変、消去ができない。

（4）機器・ソフトウェアの品質管理、動作状況の内部監査規程

①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。

3）見読性確保

（1）情報の所在管理

①システム管理者は定期的に情報の所在確認を行う。

（2）見読化手段の管理

①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。

（3）見読目的に応じた応答時間とスループット

①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。

（4）システム障害対策

①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。

a　データベースおよびその他重要な機能を担うサーバを冗長構成とする

b　バックアップツールを使用して定期的にデータのバックアップを行う

4）保存性確保

（1）ソフトウェア・機器・媒体の管理

①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。

②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。

③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。

④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、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

①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。

（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

①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。

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。

（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

①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。

5）相互運用性確保

（1）システムの改修に当たってのデータ互換性を確保する。

（2）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。

改定履歴

版数	更新日	備考
第1版	2006/06/1	新規作成
第2版	2009/12/11	更新
第3版	2015/09/24	更新
第4版	2015/10/5	更新
第5版	2015/12/7	更新
第6版	2017/3/13	更新