

医療情報システム運用管理規程

***** 第 1.1 版 *****

南魚沼市民病院・南魚沼市立ゆきぐに大和病院

医療情報システム運用管理規程

1 目的

この規程は、南魚沼市民病院およびゆきぐに大和病院において、法令に保存義務が規定されている診療録および診療諸記録をはじめ医療事務情報ならびに、各部署における業務情報等の業務執行情報（以下「診療情報」という）の電子媒体による通信・保存のために使用される機器、ソフトウェアおよび運用に必要な仕組み全般（以下「情報システム」という）について、その取扱いおよび管理に関する事項を定め、診療情報の真正性を保障し適正な保存および利用を図るとともに、患者のプライバシー保護に寄与することを目的とする。

2 適用範囲

- (1) 対象者は医療情報システムを扱うすべての利用者である。
- (2) 対象システムは電子カルテシステム・オーダーエントリーシステム・画像配信システムおよびこれらに接続されるすべての各部門システムである。
- (3) 対象情報は、すべての診療に関する情報および従業員の履歴等の個人情報である。

3 情報システムに関する理念

- (1) 情報システムの管理者および利用者は、診療情報の電子媒体による通信・保存が、自己責任の原則に基づいて行われることを認識し、診療情報の真正性、見読性、保存性を確保し、かつ、患者の診療時にまたは管理運営上必要とされる時に、信頼性のある情報を迅速に提供できるよう当院全体として環境を整え、適正な運営に努めるものとする。
- (2) 情報システムの管理者および利用者は、診療情報の利用に当たっては、患者のプライバシーが侵害されることのないよう細心の注意を払うものとする。

4 情報システムが保存する情報の範囲

- (1) 当院において電子保存する診療情報の範囲については、2015年3月1日より稼働した全システムによってサーバーに記録されている診療情報とする。
- (2) ただし、保険請求レセプト情報については、5年を経過した後は情報システム委員会の決定を経て消去破棄することができる。

5 管理組織

- (1) 南魚沼市民病院内に医療情報システム運用責任者（以下、「運用責任者」という）および個人情報保護管理者を置き、病院事業管理者をもってこれに充てる。
- (2) 南魚沼市民病院内に情報システム管理者（以下「システム管理者」という）を置き、情報システム室長をもってこれに充てる。
- (3) 情報システムの適正な運用を図るため、情報システム監査責任者（以下「監査責任者」と

いう)を置き、事務部長をもってこれに充てる。

- (4) システムの管理運用に緊急対応が必要な場合を想定して、システム管理者のもとに数人の職員によるレスキューチーム（障害復旧対処組織・非専従）を設置するものとする。

→[A10 医療情報システム運用管理体制図](#)

→C40_障害対応レスキューチーム

6 情報システム委員会の設置

- (1) 情報システムに関する取扱いおよび管理に関し必要な事項を審議するため、院内に情報システム委員会(以下「委員会」という)を置く。
- (2) 委員会の委員は、前条に規定するそれぞれの管理者もしくはそれを補佐する者、ならびに運営管理会議が指定する者をもって構成し、情報システム委員会委員長(以下、「委員長」という)と事務局長を置く。
- (3) 委員会は、委員長が招集し、委員会を主宰する。
- (4) 委員会は、委員の半数以上の出席をもって成立する。
- (5) 委員長は、必要に応じて関係者を指名し、委員会に参画させることができる。
- (6) 委員会を円滑に運営するため、事務局を置く。

→[A20 情報システム委員会運営規約](#)

7 システム管理者

- (1) システム管理者の業務は、次に掲げるとおりとする。
 - ① 電子通信・保存に用いる機器およびソフトウェアの導入に当たっては、システムの機能を確認し、これらの機能が、法令に規定されている診療情報の電子媒体による通信・保存に関する通達等に適合するかどうか審査すること。
 - ② システムの機能要件が支障なく運用される環境を整備するとともに、診療情報の通信・保存の安全性を確保し、常に利用可能な状態にすること。
 - ③ 機器・ソフトウェアの品質維持のため、保守点検を行うこと。
 - ④ 情報の応答時間の劣化がないように維持につとめ、必要な対策をとること。
 - ⑤ 機器やソフトウェアに変更等があった場合においても、電子保存された情報の真正性を確保し、また継続的に使用できるよう配慮し、その対策を講じること。
 - ⑥ 情報システムを利用する職員等(以下「利用者」という)の登録を管理し、そのアクセス権限を規定し、不正な利用を防止すること。
 - ⑦ 情報システムを正しく利用させるため、利用者に対し、研修を実施すること。
 - ⑧ システム管理者は、患者またはシステム利用者からの情報システムについての要望や苦情を受け付ける窓口を設け、その対応に努めること。

8 利用者

- (1) 利用者の遵守事項は、次に掲げるとおりとする。
 - ① パスワードは「本規程 15 パスワード管理 (4) 利用者の責務」に準じて管理する。
 - ② 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、ユーザー認証番号、パスワードによって、情報システムに利用者自身を認識させること。
 - ③ 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こと。
 - ④ 代行入力の場合、入力権限を持つもの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こと。

- ⑤一つの診療記録を複数者で共同して記録する場合は、各人がログインすること。
- ⑥情報システムへのアクセス終了に際しては、必ずログオフ操作を行い、他者が自己のパスワードで入力操作することがないようにすること。
- ⑦与えられたアクセス権限を越えた操作を行わないこと。
- ⑧参照した情報を、目的外に利用しないこと。
- ⑨患者のプライバシーを侵害しないこと。
- ⑩情報システムの異常を発見した場合、速やかに情報システム室に連絡し、その指示に従うこと。
- ⑪不正アクセスを発見した場合、速やかに情報システム室に連絡し、その指示に従うこと。
- ⑫患者情報等のデータを、デスクトップ・マイドキュメント等のハードディスクドライブに保存してはならない。
- ⑬利用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こと。

9 情報システムの機能要件

- (1) 情報システムには、次に掲げる機能を備えるものとする。
 - ①情報にアクセスしようとする者の識別と認証。
 - ②情報の機密度に応じた利用者のアクセス権限の設定および不正なアクセスの排除。
 - ③利用者が入力した情報についての確定操作。
 - ④利用者が確定操作を行った情報(以下「確定情報」という)の正確な通信・保存。
 - ⑤確定情報の通信・保存に際し、その日時および実施者等の関連情報を記録すること。
 - ⑥管理上または診療上の必要がある場合、確定情報の速やかな出力。
 - ⑦複数の機器や媒体に記録されている情報の所在の一元的な管理。
 - ⑧情報の利用範囲、更新履歴、機密度等に応じた管理区分の設定と管理情報の整理。
 - ⑨記録された情報の複製(バックアップ)の作成。

10 サーバー室の管理

- (1) 情報システムの記録媒体を含むサーバー等主要機器は独立したサーバー室に設置するとともに、サーバー室の出入口は常時施錠し、情報システム室がその入退室を管理するものとする。

11 記録媒体の管理

- (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とともに、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ものとする。
- (2) 個人情報を含む記録媒体の保管・バックアップの作業に当たる者は、手順に従い行い、その作業記録を残し、責任者の承認を得ることとする。
- (3) 個人情報を記した媒体の破棄に当たっては、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、結果を記録に残すものとする。

12 ソフトウェアの管理

- (1) 情報システム室は、情報システムで使用されるソフトウェアについて、使用の前に検査を行い、情報の安全性に支障がないことを確認するものとする。

- (2) 情報システム室は、定期的にウイルスチェックを行い、感染の防止・駆除に努めるものとする。

13 ネットワークの管理

- (1) 情報システム室は、定期的に利用履歴やネットワーク負荷等を検査し、通信環境の効率的な運用を維持するとともに、不正に利用された形跡がないかを確認するものとする。
- (2) 情報システム室は、ネットワークの不正な利用を発見した場合には、直ちにその原因を追究し対策を実施する。

14 医療情報システム端末等の管理

- (1) 各部署に設置されているパソコン及びこれと接続されている電子機器の管理は、各部署の長が行う。
- (2) 部署のパソコンに異常を発見した場合は情報システム室に直ちに連絡をとり、対策を実施する。
- (3) 接続されている電子機器の異常については、情報システム室と相談しつつ、対策を実施する。

15 パスワード管理

- (1) ID・パスワードの管理は、システム管理者が担当する。
- (2) IDと初期パスワードの付与対象者は、職員、アルバイト、委託職員等当院より許可を受けて情報システムが使用できるパソコンを使用する者とする。なお、「一職員一ID」を原則とする。
- (3) 庶務課長は、入職・退職等異動情報があった場合、システム管理者に連絡し、システム管理者はユーザーID・初期パスワードの付与、または停止を行うものとする。
 - ①ユーザーID・初期パスワードはシステム管理者が付与する。
 - ②システム管理者はIDと初期パスワード付与した際に、本規程の内容をパソコン利用者に説明する。
 - ③利用者は初期パスワードを変更後利用することとする。
 - ④初期設定時やアプリケーションが正常に動作しない場合等、どうしても必要な場合を除き、IDの付与において、Administrator等の管理者権限を与えてはならない。
- (4) 利用者の責務
 - ①パスワードは容易に推測されないように設定し、その秘密を保たなければならない。
 - ②パスワードが当該利用者以外に知られた場合、またはその疑いのある場合は、速やかに変更させなければならない。
 - ③パスワードは8文字以上が望ましい。システムとしては4文字以上を設定しない場合、使用できない技術的措置を講じることとする。
 - ④パスワードは2か月に一度定期的に変更することとする。パスワードの技術的有効期限は180日とし、それ以内に変更を行わない場合使用できない技術的措置を講じることとする。

16 電子記憶媒体の利用

- (1) 医療情報システム端末での電子記憶媒体の利用

- ①情報システムより、個人情報抽出する場合は、その担当部署を情報システム室に一元化する。
 - ②システム管理者より許可された医療情報システム端末以外では、電子記憶媒体の使用は、原則禁止とする。
 - ③匿名化されていない個人情報を保存する場合、利用者は委員長の許可を得なければならない。
 - ④業務上、電子記憶媒体に個人情報を複写し、永続的に使用する場合は、利用者は委員長に許可を得ることとする。
 - ⑤利用者は、利用目的が終了した際は速やかに消去し、私的保有をしてはならない。
- (2) 電子記憶媒体利用の記録
- ①前項の③および④の際は、利用者は「医療情報利用申込書」を起票し、システム管理者に提出する。
 - ②匿名化されない個人情報利用の申請があった場合は、システム管理者は「医療情報利用申込書」に委員長の許可があるか確認しなければならない。
 - ③システム管理者は利用者から「医療情報利用申込書」を受領し、保管する。

17 事故対策

- (1) システム管理者は、システムに障害が発生した場合の回復手順を定め、非常時においても参照できるように保管し、レスキューチーム員に徹底するものとする。
- (2) 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、運用規定の見直しを行う。また、漏えい発生の場合の対応手順を定め、発生時に対しては速やかに情報システム室に報告し対応を実施する。
情報システム室は、速やかに病院事業管理者、院長、副院長、事務部長ならびに関係幹部に報告することとする。
- (3) システムダウン時の対応は、別途定める。
 - [C00_システム障害対応規定](#)
 - [C10_システム障害対応マニュアル](#)
 - [C20_システム障害対応基準表](#)

18 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扱いおよびプライバシー保護に関する研修を行うものとする。

19 監査

- (1) 病院事業管理者は、監査責任者に毎年 1 回、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なければならない。
- (2) 監査の内容については、監査責任者の監査計画を経て、病院事業管理者がこれを承認する。
- (3) 病院事業管理者は、必要に応じて臨時の監査を監査責任者に命ずることができる。

20 委託管理における安全管理

- (1) 業務を当院外の所属者に委託する場合は守秘義務を含む業務委託契約を結ぶこと。また、各担当者は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。

- (2) 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、作業内容につき報告を求めて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。
- (3) 委託先事業者が再委託を行うか明確にし、再委託を行う場合は委託先と同等の個人情報保護に関する対策および契約がなされていることを条件とすること。なお、再委託を行う場合、委託先事業者は当院の許可を得なければならない。

21 スキャナ読み取り書類の運用

- (1) スキャナにより読み取った電子情報と、元の文書等から得られる情報との同一性を担保する情報作成管理者を置き、情報システム室員 1 名をもってこれに充てる。
- (2) スキャナの対象となる文書、読み取り作業に関しては、スキャンセンターで実施する。
- (3) 以上及びその他に関する事項は、別途「スキャンによる電子化管理要項」に定めるものとする。
→[D10_スキャンによる電子化管理要項](#)

22 遠隔保守に関する安全管理

- (1) 遠隔保守は、I SDNまたはBフレッツの通信網を使用して契約した必要最低限の事業所と行う。
- (2) 外部接続については、遠隔サポートベンダーと接続するルータ、サポート機器(サーバ、モダリティ等)間にファイアウォールを設置することにより、不正な通信を未然に防止して運用しなければならない。
- (3) ベンダーからルータの接続に第三者が入り込むことがないように、I SDNではIDおよびパスワードの認証の前に、電話番号での認証によって接続した上で運用しなければならない。
- (4) Bフレッツについては、IP-VPNを採用し、固定IPによる接続先の特定と暗号化による機密性を確保して運用しなければならない。
- (5) 上記2種類の保守に関しては、外部接続ルータのネットワークと院内ネットワークは別体系とし、ファイアウォールを設置して運用しなければならない。
- (6) 通信状況の管理、監視は、ネットワーク監視サーバーを設置して常時監視し、遠隔保守管理の安全を確保していかなければならない。
遠隔保守に関わる事業所とは、守秘義務の記された契約書または覚書を別途取り交わした上で保守管理の運用を委託しなければならない。

23 本規程の改廃

本規程の改廃は、情報システム委員会が行い、運営管理会議の承認により発効する。

24 施行

本規程は、2015年3月1日から施行する。

以上

改 訂 履 歴

版数	改訂年月日	改訂内容
1.0	2015年2月23日	新規制定
1.1	2015年11月1日	ゆきぐに大和・南魚沼市民病院の対応内容に修正。システム障害時の対応基準等を追加。

※ 版数は新規制定を第 1.0 版とし、改訂が発生した際は第 1.1 版とする。

※ 改訂があった場合は、必ず改訂内容を記載すること。