新潟中央病院　医療情報システム運用管理規程

第1章　総則

（主旨）

第1条　この規程は、医療法人仁愛会 新潟中央病院（以下「当院」という。）において、病院情報システム（以下「情報システム」という。）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、適正な管理を図るために必要な事項を定めることを目的とする。

（法令等の遵守）

第2条　システムの利用にあたっては、「診療録及び診療諸記録の電子媒体による保存について」（平成11年4月22日付健政発517号厚生省健康政策局長、医薬発第587号医薬安全局長、保発第82号保険局長）、「個人情報の保護に関する法律（平成15年5月30日法律第57号、平成17年4月1日全面施行）」、「新潟中央病院個人情報保護規定」に定めるもののほか、この規程の定めるところによる。

（定義）

第3条　この規程において、次の各号に掲げる用語の定義は、当該各号に定めるところによる。

（1）システム・・・当院において、診療録に関する情報の電子計算機による処理及び電子媒体による保存のために使用される機器、ソフトウェア及び運用に必要な仕組み全般。

（2）利用者・・・第6条に規定する情報システム管理者が、次の各号に掲げる利用資格者のうち、利用を許可した者とする。

①当院の職員（非常勤、臨時職員及びパートタイマーを含む）

②委託職員でその職務により、システムを使用するもの

③その他情報システム管理者が必要と認めた者

（システム構成）

第4条　システムは、次の各号に掲げるシステムにより構成される。

（1）電子カルテ・オーダリング・看護支援システム

（2）看護勤務システム

（3）薬剤部門システム

（4）栄養管理システム

（5）医事会計・病歴システム

（6）文書作成システム

（7）インシデントレポートシステム

（8）健診システム

（9）検査システム

（10）放射線画像管理システム（PACS）

（11）リハビリシステム

（対象情報）
第5条　この規程で対象とする情報は、当院での診療に関する全ての情報とする。

第2章　管理体制
（情報システム管理者）
第6条　病院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、院長、副院長をもってこれに充てる。

（運用責任者）
第7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運用を担当する責任者（以下「運用責任者」という。）を置き、事務長、総務課長をもってこれに充てる。

（部門システムの監視責任者）
第8条　部門システムの監視責任者（以下「部門システム監視責任者」という。）を置き、各部門長をもってこれに充てる。

（電子カルテ委員会の設置）
第9条　1. 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、電子カルテ委員会を置く。
2. 電子カルテ委員会の運営については、全部門より最低1名の代表者が出席する。

（監査責任者）
第10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。理事長をもってこれに充てる。

（事故対策）
第11条　1. システム管理者は、緊急時及び災害時の連絡、復旧体制並びに回復手順を定め、非常時においても参照できるような媒体に保存し保管させること。
2. システム管理者は、利用者に対して、事故発生時に速やかに報告することを周知させること。
3. システム管理者は、業務上において情報漏えい等のリスクが予想されるものに対し、規程の見直しを行うこと。

（教育及び訓練）
第12条　運用責任者は、システムを適正に利用させるため、利用者の教育及び訓練を行うこと。

第3章　管理者及び利用者の責務
（システム管理者の責務）
第13条　システム管理者は、次の各号に掲げる責務を負う。
（1）紙を情報交換の中心にすえた業務方法からコンピュータ等の各種情報メディア機器を利用した情報交換に業務方法を変更し、さらに効率的に運用するために情報管理をする組織を設ける。
（2）情報の共有化を図るとともに、共有化によって起こる各種情報の漏洩防止のためにそのセキュリティ権限付

与を設定し常に管理する。
（3）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定し、不正な利用を防止する。
（4）情報システムを円滑に運営し、情報システム全体の管理状況を把握する。
（5）情報システムが常に業務の効率性と円滑化のために情報収集し、合理的運営を指針するために適切に関係委員会に諮問する。
（6）関係委員会の委員長を選任あるいは承認し、答申あるいは関係委員会の協議内容について報告を受ける。
（7）事故対策として、緊急時及び災害時の連絡、復旧体制並びに回復手順を定め、非常においても参照できるような媒体に保存し保管させる。

（運用責任者の責務）
第14条　運用管理者は、次の各号に掲げる責務を負う。
（1）情報システムを安全で合理的に運用し、運用上に問題が生じた場合は、速やかにシステム管理者に報告する。
（2）情報システムの有効活用を図り、機器の配置及び利用について決定する。
（3）情報システムと外部システムとのデータの連携に関して統括し、システム管理者の承認を得る。
（4）患者又は利用者からの、情報システムについての苦情を取りまとめ、対策案を策定する。
（5）利用者への周知のため、情報システムの取扱いについて手順書等を整備し、利用者に周知の上、常に利用可能な状態にしておく。
（6）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。

（部門システム監視責任者の責務）
第15条　部門システム監視責任者は、次の各号に掲げる責務を負う。
（1）部門の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）部門の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。
（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）部門の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。
（6）個別に接続された機器へのコンピュータ・ウイルス及び不正アクセスに対する対策を講じる。

（監査責任者の責務）
第16条　監査責任者は、別に定める規定により情報システムの監査を実施し、監査結果をシステム管理者に報告する責務を負う。

（利用者の責務）
第17条　利用者は、次の各号に掲げる責務を負う。
（1）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）情報システムの情報の参照や入力に際して、ID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）ID及びパスワードを他人に教えてはならない。また、他人が容易に知ることができる方法でID及びパスワードを

管理してはならない。
(4)利用者が正当なID及びパスワードの管理を行わないために生じた事故や障害に対しては、その利用者が相応の責任を負う。
(5)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。
(6)作業終了あるいは離席する際はログアウト操作を行う。
(7)与えられたアクセス権限を越えた操作を行ってはならない。
(8)参照した情報を目的外に利用してはならない。
(9)患者のプライバシーを侵害してはならない。
(10)システムの異常を発見した場合、速やかに運用責任者に連絡し、その指示に従うこと。
(11)不正アクセスを発見した場合、速やかに運用責任者に連絡し、その指示に従うこと。

第4章　一般管理における運用管理事項

(入退室管理)

第18条　システム管理者は、個人情報が保管されている機器の設置場所および記録媒体の保存場所は常時施錠管理し、入室管理すること。

(情報システムへのアクセス管理)

第19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、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。

(個人情報の記録媒体の管理)

第20条　運用管理者は、保管及びバックアップの状況を確認すること。

(個人情報を含む媒体の廃棄等処分)

第21条　システム管理者は、個人情報を含む媒体の廃棄等処分に当たり、安全かつ確実に行われるための適切な措置を講じること。

(リスクに対する予防、発生時の対応)

第22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、運用管理規程の見直しを行うこと。また、利用者は、事故発生時に速やかに運用責任者に報告すること。

(情報システムの安全に関する技術的対策と運用的対策の分担を定めた文書の管理)

第23条　利用者識別と認証、アクセス権限管理、アクセスログ取得と監査、時刻同期、ウイルス等不正ソフト対策は運用管理者が検討し導入する事。

(無線LANに関する事項)

第24条　1．システム管理者は、利用者以外に無線LANの利用を特定されないよう、ステルスモード、ANY接続拒否等の対策を施すこと。

2. システム管理者は、SSID等によるアクセス制限を行い、不正アクセスの対策を施すこと。
3. システム管理者は、WPA2／AES等により、通信を暗号化して情報を保護し、不正な情報の取得を防止すること。

第5章　情報及び情報機器の持ち出しについて
（情報及び情報機器の持ち出し禁止）
第25条　情報及び情報システムは、院外に持ち出してはならない。ただし、特段の事情により、システム管理者の許可を得た場合は、この限りではない。

（持ち出した情報及び情報機器の安全管理措置）
第26条　情報及び情報機器の持ち出しを許可された者は、情報の暗号化や情報機器のパスワード入力による起動等を施し、盗難、紛失、情報の漏えい等の事故がないよう、最大限の注意をもって管理すること。

第6章　外部の機関と医療情報を交換する場合
（外部接続におけるシステム管理者の事前承認）
第27条　外部の機関と医療情報を交換する場合、あらかじめシステム管理者の承認を得ること。

（脅威に対する対策）
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ネットワークを構築する場合、セキュアな回線の利用やデータの暗号化等により、盗聴、侵入、改ざん、妨害等の脅威を防止するための必要な対策を講じること。

（安全性が確保されていないネットワークでの保守作業禁止）
第29条　システム管理者は、安全性が確保されていないネットワークを経由して行う情報システムの保守作業等を許可してはならない。

第7章　災害等の非常時の対策
（災害等の非常時の運用）
第30条　システム管理者は、すみやかにシステムの被災状況を確認し、状況に応じ各システムメーカーと連携を取り、速やかな復旧を目指す。

第8章　教育と訓練
（運用手順書等の整備）
第31条　運用責任者は、情報システムの取扱いについて運用手順書、操作手順書等を整備し、利用者に周知すること。

（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）
第32条　運用責任者は、情報システムの利用者に対し、情報システムの取扱い及びプライバシー保護に関する教育情報を適宜発信すること。

第9章監査

（監査の内容）

第33条　監査の内容は、電子カルテ委員会の審議を経て、システム管理者がこれを定めること。

（監査の実施及び結果報告）

第34条　監査責任者は、年1回以上の頻度で情報システムの監査を実施し、監査結果をシステム管理者に報告すること。

（改善事項に対する対応）

第35条　システム管理者は、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。状況に応じ、電子カルテ委員会を開催すること。

（適時監査）

第36条　システム管理者は、必要な場合、適時監査を監査責任者に命ずることができる。

第10章　真正性確保

（作成者の識別及び認証）

第37条　1. 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定し、不正な利用を防止すること。

2. 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。

3. 利用者は、情報の参照や入力に際して、認証番号やパスワード等によりシステムに自身を認識させること。

4. 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こと。

（情報の確定手順と、作成責任者の識別情報の記録）

第38条　1. 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。

2. 代行入力の場合は、入力権限を持つ利用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こと。

（更新履歴の保存）

第39条　システム管理者は、技術的に更新履歴を保管させ、必要に応じて更新前の情報を参照する機能を持たせること。

（代行操作の承認記録）

第40条　システム管理者は、代行者を依頼する可能性のある担当者に、確定の任務を徹底すること。

（一つの診療録等を複数の医療従事者が共同して作成する場合の管理）

第41条　利用者は、一つの診療記録を複数者で共同して作成する場合に、各人がログインすること。

（機器・ソフトウェアの品質管理）
第42条　システム管理者は、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。

第11章　見読性確保
（情報の所在管理）
第43条　運用管理者は、定期的に情報の所在確認を行うこと。

（見読化手段の管理）
第44条　システム管理者は、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こと。

（見読目的に応じた応答時間とスループット）
第45条　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、必要な対策をとること。

（システム障害対策）
第46条　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。
2. 運用責任者は、データバックアップ作業が適切に行われている事を確認すること。

第12章　保存性確保
（ソフトウェア・機器・媒体の管理）
第47条　1. システム管理者は、システムで使用されるソフトウェアをあらかじめ審査し、情報の安全性に支障がないことを確認すること。
2. システム管理者は、システムの主要機器を施錠管理された場所に設置すること。
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こと。
4. システム管理者は、システムの主要機器の設置場所に無水消火装置、漏電防止装置、無停電電源装置等の保安設備を備えること。

（不適切な保管・取扱いによる情報の滅失、破壊の防止策）
第48条　システム管理者は、新規の業務担当者において操作前に教育を行うこと。

（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）
第49条　1. 運用責任者は、記録媒体や設備の劣化による読み取りエラーを防止するため、記録媒体に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させること。
2. 運用責任者は、品質の劣化が予想される記録媒体がある場合、あらかじめ別の媒体に複写させること。

（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）
第50条　システム管理者は、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成すること。

第13章　相互運用性確保

（システムの改修・更新に当たっての、データ互換性の確保策）

第51条　1. システム管理者は、標準的な規約（例えば、XML、HL7、DICOM等）に従った形式での情報の入出力を義務づけること。

2. システム管理者は、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と。

第14章　スキャナ読み取り書類の運用

（スキャナ読み取りの対象にする文書の規定）

第52条　運用責任者は、スキャナ読み取りの対象にする文書を選定する場合、電子カルテ委員会にはかり、決定させること。

（適切な精度のスキャナの使用）

第53条　運用責任者は、スキャナ読み取り電子情報と原本との同一性を担保できるよう、適切な精度のスキャナを導入し、適切な設定で運用させること。

（スキャンするタイミング）

第54条　利用者は、スキャナ読み取りの必要な書類が発生した場合、遅滞なくスキャナ取り込みを行うこと。

第15章　その他

（利用の制限及び禁止）

第55条　システム管理者は、利用者がこの規程に違反し、又は違反するおそれがあると認めるときは、電子カルテ委員会の承認を経て、システムの利用を制限し、又は禁止することができる。

（庶務）

第56条　この規程に基づく庶務は、電子カルテ委員会において処理すること。

（雑則）

第57条　この規程の施行に関し必要な事項がある場合は、電子カルテ委員会の審議を経て、システム管理者がこれを定めること。

附則

この規程は、平成26年3月3日から施行する。

平成27年9月1日改定。