医療情報システム安全管理規程

1.（目的）

本規程は、医療法人財団 中島記念会 大森山王病院（以下、「当院」）における医事管理システムや医療用画像管理システム等の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（以下「医療情報システム」）について、その取扱い及び安全管理に関する事項を定め、患者の個人情報保護と診療の継続性を確保し、適正保存するとともに、適正に利用することを目的とする。

2.（利用に関する理念）

・医療情報システム管理者及び利用者は、電子媒体による保存（以下、「電子保存」）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。
・医療情報システム管理者及び利用者は、電子保存された情報の真正性、見読性、保存性を確保し、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。
・医療情報システムの管理者及び利用者は、患者のプライバシーが侵害されることのないよう注意しなければならない。
・個人情報保護規定に則り、電子保存の三原則（真正性・見読性・保存性）を確保し、データの正確性を担保する。

3.（管理体制）

・当院に以下の責任者を置く。
最高情報責任者（CIO）： 病院長。システム運用全般の最終責任を負う。
医療情報システム安全管理責任者： 実務上の管理・指導やアクセス権限の承認を行う。

4.（医療情報システム管理者の責務）

医療情報システム管理者は以下の責務を負う。
・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、医療情報システムの機能を確認し、これらの機能が厚生労働省の定める「医療情報システムの安全管理に関するガイドライン」に示される各項目に適合するよう留意すること。
・医療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こと。
・電子保存された情報の安全性を確保し、常に利用可能な状態に置くこと。
・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。
・医療情報システム利用者を登録・管理し、そのアクセス権限を設定し、不正な利用を防止すること。
・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。

5.（医療情報システム利用者の責務）

医療情報システム利用者は以下の責務を負う。
・自身の認証番号やパスワード等を管理し、これを他者に利用させないこと。
・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、利用者自身を認識させること。
・医療情報システムへの入力に際して、確定操作を行って、入力情報に対する責任を明示すること。
・与えられたアクセス権限を越えた操作を行わないこと。
・参照した情報を、目的外に利用しないこと。
・患者のプライバシーを侵害しないこと。
・医療情報システムの異常を発見した場合、速やかに医療情報システム安全管理責任者に連絡し、その指示に従うこと。

6.（システム要件）

定義
・個人情報保護規定に準拠し、電子保存の三原則が確保された状態で、データの正確性が担保されていること。
真正性
・正当な人が記録・確認を行った情報について、第三者にとって作成の責任の所在が明確であり、かつ、故意又は過失による虚偽入力・書換え・消去・混同が防止されていること。
見読性
・電子媒体に保存された内容を、要求に基づき、必要に応じて肉眼で読み取れる状態にすること。
保存性
・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、見読性が確保された状態で保存されること。
データの正確性
・利用目的の達成に必要な範囲内において、個人データを正確かつ最新の内容に保つとともに、利用する必要がなくなったときは、当該個人データを遅滞なく消去するよう努めなければならない。

医療情報システムは、次の機能を備えるものとする。
・情報にアクセスしようとする者の識別と認証機能
・情報の機密度に応じた利用者のアクセス権限の設定と不正なアクセスを排除する機能
・利用者の情報へのアクセス開始及び終了（システムへのログイン・ログアウト）の記録を保存する機能
・利用者が入力した情報について確定操作を行うことができる機能
・利用者が確定操作を行った情報を正確に保存する機能
・利用者が確定操作を行った情報の記録及びその更新に際し、その日時並びに実施者をこれらの情報に関連付けて記録する機能
・管理上又は診断上の必要がある場合、記録されている情報を速やかに抽出する機能
・情報の利用範囲、更新履歴、機密度等に応じた管理区分を設定できる機能
・記録された情報の複製（バックアップ）を作成する機能

7.（技術的安全管理措置）
利用者認証とアクセス制御
・システム利用には、個別の利用者 ID とパスワードを用いて他に利用させない。
・パスワードは、他人に推測されにくい複雑なものを次の条件で設定している。
（1）13 桁以上である（定期変更の必要なし）。
（2）ランダムな文字列である。
（3）英字、数字、大文字、小文字、記号の全てが混在している。
（4）他で使用しているパスワードを再利用していない。
（5）単語や個人情報（名前、生年月日、電話番号など）を使用しない。
（6）同じ文字列の繰り返しやキーボードやアルファベット配列など安易な並びを避ける。
（7）ID と同じまたは一部同じ文字列を避ける。
・ ID とパスワードを他と共有してはならない。漏洩が判明した時点で変更を行う。
・ 職員の職種や役割に応じ、参照・入力・削除等のアクセス権限を最小限に制限する。
・ 入退職管理し、遅滞なく不要なアカウントを削除・無効化する。
・ アクセスログを管理し不正アクセスを監視する。

（サイバーセキュリティ対策）
・ 全ての端末にウイルス対策ソフトを導入し、定義ファイルを常に最新の状態に保つ。
・ OS やソフトウェアの脆弱性情報を収集し、速やかにセキュリティパッチ（最新ファームウェア、修正プログラム等）を適用する。
・ 外部ネットワークとの接続点にはファイアウォール等を設置し、不正アクセスを遮断する。
・ 管理者は、全ての機器をネットワーク制御し経営資源としての情報及びネットワークを監視する。
・ 管理者から許可を得ていないシステムや端末の接続及び導入をしない。
・ バックグラウンドで動作している不要なソフトウェアやサービスを停止する。

8.（物理的安全管理措置）
端末および設備の管理
・ サーバー等の基幹設備は、施錠可能な専用室またはラックに設置し、許可なき者の立ち入りを禁じる。
・ サーバー等の基幹設備は、湿度・温度管理可能な環境で災害等にも対応可能な設備・装置を備える。
・ 電子カルテ端末は、離席時にスクリーンロックをかける。
・ 患者の目に触れる場所に端末を設置する場合、覗き見防止フィルタの装着等の措置を講じる。
・ 在宅医療部門で使用する許可された情報及び情報端末以外の院外持ち出してはならない。
・ サーバー、端末 PC、ネットワーク機器は台帳管理を行う。
・ 端末は、許可されていない外部記録端末や情報機器との接続を制限し、許可のないデータ複写をしてはならない。
・ 医療情報システムは、許可されていない職員や外部の者が操作できないよう管理する。
・ 電子保存された個人情報をプリントアウトした場合には、紙媒体の診療記録と同等に厳重な取り扱いをする。
・ 医療情報システム管理者は、盗難紛失を防ぐため、防犯カメラを設置し、施錠できる部屋に機器を設置する。施錠できない部屋に関しては機器を固定する。
・機器や個人データの盗難、紛失時は「個人情報保護規定」「漏洩・紛失・毀損事故発生時の対応」（別表 2）に準じた対応を行う。

9.（バックアップ管理）
・ データの消失に備え、定期的にバックアップを作成する。
・ ランサムウェア対策として、バックアップデータの一部はネットワークから隔離した状態（オフライン）で保管する。

10.（個人情報の廃棄）
・個人情報を廃棄する場合は、個人を特定できないようにしなければならない。
・個人情報を記録したコンピュータを廃棄する場合は、物理的に破壊する。
・個人情報を記録したメディア（HD、FD、 CD 、 MO 、DVD等）の取扱いには最新の注意を払い、廃棄する場合は、個人情報を読み取られないよう、物理的に破壊する。
・個人情報の廃棄作業は原則として当院の職員が行う。ただし、必要があるときは適切な廃棄物処理業者に廃棄を委託する。

11.（委託先の監督）
・ システムの保守等を外部業者に委託する場合、機密保持契約を締結し、当該業者の安全管理体制が適切であることを定期的に確認する。
・ 業者から医療情報セキュリティ開示書（MDS/SDS）の提示を受ける（契約していない場合不要）。
・ リモートメンテナンスを契約する際は、利用機器及びネットワークを把握し監視する。
・ 当院の個人情報保護規定に準拠し、委託終了後は、保有する個人情報を返却または委託先で廃棄する。
・ 機密保持契約に基づき従業員を監督・教育し、雇用終了後についても遵守するよう誓約する。

12.（緊急時対応）
・ システム障害やサイバー攻撃を検知した場合、直ちに医療情報システム安全管理責任者に報告し、被害拡大防止のためネットワーク遮断等の緊急措置を講じる。
・ 重大な漏洩、滅失、毀損が発生した場合は、個人情報保護委員会および厚生労働省、医療情報システム保守業者、管轄警察、関係機関へ速やかに報告する（「個人情報保護規定」、「漏洩・滅失・毀損事故発生時の対応」（別表 2）、「医療情報システム等の障害発生時の対応フローチャート」に準ずる）。
・ 関係事業者と協力しバックアップから必要なデータやシステムを把握し復旧手順を確認する。

13.（事業継続計画）
・ システムダウン時に備え、紙カルテ等による代替診療手順を定め、年 1 回以上の対策訓練を行う。
・ 事業継続計画（別表 3）を参照。

14.（教育）
・ 全職員に対し、年 1 回以上の情報セキュリティ研修を実施する。

15.（監査）
・ 医療情報システム安全管理責任者は、本規程の遵守状況を確認するため、定期的に利用ログの確認および内部監査を実施する。
・ 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」及び「医療機関におけるサイバーセキュリティ対策チェックリスト」それに付随する項目に準拠し、本規定を見直し改訂する。

16.本規程は、2009 年 7 月より施行する。
・2015 年 9 月、一部改訂
・2022 年 4 月、一部改訂
・2022 年 11 月、一部改訂
・2024 年 4 月、一部改訂
・2025 年 8 月、一部改訂