

電子保存に関する運用管理規程

Ver.1.1

こせき歯科・諫早クリニック

施行 令和 7 年 6 月 20 日

改定 令和 8 年 9 月 1 日

1. (目的)

この規程は、当院において、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。)の電子媒体による保存(以下「電子保存」という。)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「電子保存システム」という。)について、その取扱い及び管理に関する事項を定め、保存義務のある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)

本規程の対象システムは、株式会社ヨシダデンタルシステムの電子カルテシステム ProfitRipi-eKarte (プロフィット・リピ・イーカルテ) 及び同電子カルテシステムと共に使用されるレントゲン写真、口腔内画像、CT 画像その他の診療記録のうちデジタル化が可能な情報の管理システムとする。

3. (管理体制)

(1) 電子保存システムの運用責任者、個人情報保護責任者及び電子保存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。)を置き、院長をもってこれに充てるものとする。

(2) 院長は必要な場合、システム管理者及び個人情報保護責任者を別に指名することができるものとする。

(3) 院長は、電子保存システムに関する監査を担当する監査責任者を指名するものとする。監査責任者の責務は、本規程に定めるものの他、別に定める。ただし、院長は、監査責任者の代わりに、第三者に電子保存システムに関する監査を依頼することもできる。

(4) 契約書、マニュアル等の文書の管理については、別途規程を定めるものとする。

(5) 患者及び電子保存システムを使用する者であってシステム管理者以外の者(以下「利用者」という。)からの、情報システムについての苦情・質問を受け付ける窓口を設けるものとする。

4. (システム管理者の責務)

システム管理者は以下の責務を負うものとする。

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、システムの機能を確認し、これらの機能が「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。

- ② 電子保存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。
- ③ 保存義務のある情報として電子保存された情報（以下「電子保存された情報」という。）の安全性を確保し、常に利用可能な状態に置くこと。
- ④ 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実施すること。
- ⑤ 障害時の対応体制が最新のものであるように管理し、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。
- ⑥ スキャナ読み取りに係る運用管理規程を設け、業務において同規程に則った運用がなされていることを確認すること。
- ⑦ 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。
- ⑧ 無線 LAN を使用する場合は、不正アクセス対策を実施し、不正な情報の取得を防止するために通信を暗号化すること。
- ⑨ 外部のサービス事業の利用に当たっては、必要なガイドラインへの適合性を、サービス事業者からの文書等により確認し、文書の保存を行うこと。
- ⑩ 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文書化し、利用者に周知の上、常に利用可能な状態におくこと。
- ⑪ 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ものとする。
- ⑫ 保守会社における保守作業に関し、その作業者及び作業内容につき報告を求め適切であることを確認し、必要と認めた場合は適時監査を行うものとする。

5. （利用者の責務）

利用者は以下の責務を負うものとする。

- 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こと。
- ② 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、システムに利用者自身を認識させること
- ③ 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。

- ④ 与えられたアクセス権限を越えた操作を行わないこと。
- ⑤ 利用者は、離席する際は、ログアウトすること。
- ⑥ 参照した情報を、目的外に利用しないこと。
- ⑦ 患者のプライバシーを侵害しないこと。
- ⑧ 電子保存システムの異常を発見した場合及び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、その指示に従うこと。
- ⑨ 在職中のみならず、退職後においても業務中に知り得た個人情報に関する守秘義務を負うこと。

6. (技術的と運用的対策の分担を定めた文書の管理規程)

(1) システム管理者は、各システムについて、その設計時及び運用開始時に、技術的対策と運用による対策をリスト化した基準適合リストを作成し、同リストを必要時には第三者への説明に使える状態で保存するものとする。

(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従っていることを確認するものとする。

7. (機器及び記録媒体の管理)

(1) 電子保存システムの記録媒体を含む主要機器は、システム管理者によって入退室管理された施設できる場所に設置し、定期的に設置機器の点検を行うものとする。設置場所には、火災、災害等にも対応可能な設備・装置を備えるものとする。

(2) 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ものとする。

(3) 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ものとする。

(4) 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、手順に従って行い、その作業の記録を残し、システム管理者の承認を得るものとする。

(5) 記録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、結果を記録に残すものとする。

8. (ソフトウェアの管理)

(1) システム管理者は、電子保存システムで使用するソフトウェアを、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ものとする。また、定期的にソフトウェアに異常がないかを検査するものとする。

(2) システム管理者は、定期的にソフトウェアのウィルスチェックを行い、感染の防止に努めるものとする。

9. (情報及び情報機器の院外持ち出し等)

(1) システム管理者は、情報及び情報機器の持ち出しに関しリスク分析を行い、情報及び情報機器の持ち出しの可否を決定し、それ以外の情報及び情報機器の持ち出しを禁止するものとする。

(2) システム管理者は、持ち出し対象となる情報若しくは情報機器は別表としてまとめ、利用者に公開するものとする。

(3) システム管理者は、情報が格納された可搬媒体及び情報機器の所在について台帳に記録し、その内容を定期的にチェックし、所在状況を把握するものとする。

(4) 個人保有又は個人管理下の情報機器の業務利用は原則として禁止するが、やむを得ない場合は、システム管理者による安全管理措置を施すものとする。

(5) 情報及び情報機器を院外に持ち出す場合は、持ち出す利用者の氏名、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、承認を得るものとする。

(6) 持ち出した情報を格納した情報機器について、起動パスワード等を設定し、ウィルス対策ソフトをインストールしておくものとする。

(7) 公衆無線 LAN は原則として禁止するものとするが、公衆無線 LAN しか使用できない環境にある場合は、「医療情報システムの安全管理に関するガイドライン」で定める基準に則り使用するものとする。

(8) 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（あるいは承認されていないサービスが利用できる）情報機器で取り扱うこと、持ち出した情報機器に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すること、持ち出した情報機器で承認されていないサービスを利用することは禁止する。

(9) 持ち出した情報及び情報機器の盗難、紛失時には、直ちにシステム管理者に届け出るものとする。

(10) 利用者が、情報機器、記録媒体を院内へ持ち込み、個人情報、診療内容のデータ化、複写等を行うこと及び入力した情報を院外へ持ち出すことは禁止する。

10. (外部の機関との医療情報交換)

(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及び運用的対策を講じるものとする。システム管理者は、技術的対策が適切に実施され問題がないかを、定期的に監査を行って確認するものとする。

(2) 外部の機関と医療情報を交換する場合は、相手の医療機関等、電気通信事業者、運用委託業者等との間で、責任分界点や責任の所在を契約書等で明確にするものとする。

(3) 外部の保守会社からリモートメンテナンスを受ける場合は、相手の保守会社等、電気通信事業者、運用委託業者等との間で、責任分界点や責任の所在を契約書等で明確にするものとする。

(4) 外部からアクセスを許容する機器については、別途定める規程に従ったものに限定するものとする。

11. (マニュアルの整備)

システム管理者は、電子保存システムの取扱い並びに情報及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ものとする。

12. (教育と訓練)

システム管理者は職員に対して、定期的に情報の安全性とプライバシー保護、電子保存システムの取扱い並びに情報及び情報機器の持ち出しに関する研修を行い、研修時のテキスト、出席者リストを残すものとする。

13. (運用管理規程の公開)

システム管理者は、本規程を院内の電子保存システム端末から容易に閲覧できるように配慮するとともに、ホームページ等で公開するものとする。

14. (その他)

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、院長がこれを定める。

15. この規定は 2025 年 6 月 20 日より施行する。

16. (情報の破棄)

電子カルテシステムに保存された情報及び関連する媒体の破棄は、法令及び院内規定に基づき、保存期間を満了した後に適切に実施するものとする。

(1) 情報種別ごとの破棄の手順

・電子データ

システム管理者の承認を得てデータを完全消去またはシステム機能により削除する。

・紙媒体

シュレッダー等で判読不明な状態で破棄する。

・バックアップ媒体

データを完全消去または物理破壊を実施する。

(2) 破棄を行う条件

①法令及び院内規定に定める保存期間が満了したとき。

②その他、システム管理者が不要と判断したとき。

(3) 情報を破棄可能な従業者

①システム管理者

②システム管理者から承認を受けた委託事業者

(4) 不要となった個人情報を含む媒体の破棄

①個人情報を含む電子媒体及び紙媒体は、個人情報が漏洩しないよう復元又は判読できない状態で破棄すること。

②個人情報を含む媒体の破棄を実施した場合は、必要に応じて廃棄記録を作成し保存すること。

17. (災害、サイバー攻撃等の非常時の対応)

(1) 非常時の判断基準

以下のいずれかに該当する場合

- ① システム障害等により電子カルテシステムが利用できない状態となった場合
- ② サイバー攻撃が疑われる場合
- ③ 情報漏洩の恐れがある場合
- ④ 災害により通常業務が困難な場合
- ⑤ その他システム管理者が非常時と判断した場合

(2) 非常時の判断の手順

- ① システムに関する異常や障害を認知した職員は、直ちにシステム管理者へ報告すること。
- ② 報告を受けたシステム管理者は障害状況を速やかに確認し、非常時に該当するか判断すること。

(3) 非常時の判断者

システム管理者 小関 優作

(4) 正常復帰時の判断手順

システム管理者は、通常運用への復帰前に以下の事項を確認すること。

- ① 電子カルテシステムへの正常な接続が可能であること
- ② 患者情報の閲覧及び診療記録の入力が正常に行えること
- ③ 電子カルテ内の患者情報及び診療記録についての整合性
- ④ バックアップデータ及びシステムログに異常がないこと

障害原因を特定し、再発防止措置を策定すること

18. (代行入力)

(1). 電子カルテへの診療情報の入力、原則として当該診療行為を実施した医師その他の医療従事者本人が行うものとする。

(2). 本人以外の者による電子カルテへの代行入力は、原則として認めない。

(3). やむを得ない事情により本人以外の者が入力を行う必要が生じた場合は、入力者及び指示者を明確にするとともに、記録の真正性及び責任の所在を確保しなければならない。

(4). 代行入力は、診療又は業務上必要な事項について、指示者の意思決定及び指示内容を正確に電子カルテシステムへ反映することを目的とするものであり、代行入力者が自己の判断により診療内容、医学的判断、処方、検査等の内容を追加、変更又は削除してはならない。

(5). 代行入力した内容は、必ず当日に医師が確認し確定作業を行うこと。

(6). 代行入力を行う場合、代行入力者は自身の認証番号及びパスワードを使用して電子カルテシステムにログインしなければならない。認証番号、パスワードその他の認証情報を他の職員と共有、又は他の職員の認証情報を使用してはならない。

(7). 緊急時その他やむを得ない事情により、通常の実行入力及び確認手順によることが困難な場合は、診療上の安全を確保するため必要な範囲で代行入力を行うことができる。この場合においても、事後速やかに指示者又は作成責任者が入力内容を確認し、必要な確定操作を行うものとする。

(8). 代行入力を行う職員は、電子カルテシステムの操作方法、代行入力の対象業務、情報セキュリティ、個人情報保護及び本規程に定める代行入力の手順について、所定の教育及び研修を受けなければならない。

(9). システム管理者は、代行入力に係る利用者権限を適切に設定するとともに、代行入力の利用状況、確定状況及び操作履歴について、必要に応じて点検又は監査を行うものとする。

(10). 代行入力においては、入力者と作成責任者を明確に区別し、入力行為の責任と診療記録の作成責任が適切に記録されるよう運用しなければならない。

(11). システム管理者は、代行入力を認める業務及び代行入力を行うことができる職種を指定すること。

(12). 代行入力を認める業務及び職種については別表に定め、必要に応じて見直すものとする。

19. この規定は 2026 年 9 月 1 日より施行する。