管理文書

医療情報システム運用管理規程

初版

森本医院

２０２５年10月２日

目次

医療情報システム運用管理規程

１．目的

この規程は、当院において、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) 対象システムは、電子カルテシステムである。

2) 対象システムの扱う情報については、そのシステムごとに別途定義と安全管理上の重要度の分類を行い、リスク分析を行い表に記入し保管すること。

リスク分析については、「小規模医療機関等向けガイダンス」に記載されている以下の付録を参照すること。

「中小企業の情報セキュリティ対策ガイドライン」（独立行政法人情報処理推進機構：IPA）

https://www.ipa.go.jp/security/keihatsu/sme/guideline/

３．標準規格

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ー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。

４．運用責任者、個人情報保護責任者、システム管理者

１）当院に運用責任者、個人情報保護責任者およびシステム管理者を置き、院長をもってそれに充てること。

２）院長は必要な場合、システム管理者を別に指名すること。

５．マニュアル・契約書等の文書管理

・契約書、マニュアル等の文書の管理については、別途規程を定めること。[文書管理規程]

・システム管理者は、情報システムに関する全体構成図（ネットワーク構成図・システム構成図等）、及びシステム責任者一覧（設置事業者等含む）を作成し、常に最新の状態を維持すること。

６．監査体制と監査責任者、監査実施

・情報システムの監査を定期的に行い、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。

７．患者及びシステム利用者からの苦情・質問の受付体制

１）患者及び利用者からの、情報システムについての苦情・質問を受け付ける窓口を設けること。

２）苦情・質問受け付け後は、その内容を検討し、速やかに必要な措置を講じること。

８．事故対策

システム管理者は、緊急時及び、障害時、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。

事業継続計画（BCP）策定 については、以下厚生労働省の HP に掲載されている資料を参照すること。

「医療情報システムの安全管理に関するガイドライン 第 6.0 版（令和 5 年 5 月）サイバー攻撃を想定した事業継続計画（BCP）策定の確認表等 」

https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html

９．システム利用者への教育・訓練など周知体制

１）システム管理者は、情報システムの取扱いについて必要に応じ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こと。

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扱い及びプライバシー保護に関する研修を行うこと。

１０．システム管理者や運用責任者、監査責任者の責務

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こと。

２）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。

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こと。

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こと。

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定し、不正な利用を防止すること。

６）情報システムを正しく利用させるため、作業手順書の整備を行い利用者の教育と訓練を行うこと。

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を受け付ける窓口を設けること。

８）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。

９）情報システムで用いる機器及びソフトウェアに対し、マルウェア対策ソフトやセキュリティアップデートなどのセキュリティ対策を実施すること

１１．利用者の責務

１）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、パスワード等

によって、システムに自身を認識させる。

２）利用者は、自身のパスワードを管理し、これを他者に利用させない。

３）利用者は、システム管理者によって設定された初期パスワードの変更を行うこと。
パスワードは、以下のいずれかの条件を満たす形で設定を行うこと。

a. 英数字、記号を混在させた 13 文字以上の推定困難な文字列

b. 英数字、記号を混在させた 8 文字以上の推定困難な文字列を定期的に変更 （最長でも２ヶ月以内）

４）利用者が、正当なパスワード等の管理を行わないために生じた事故や障害に対しては、その利用者が責任を負う。

５）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。

６）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。

７）利用者は、情報システム及び参照した情報を、目的外に利用しない。

８）利用者は、患者等のプライバシーを侵害しない。

９）利用者は、法令上の守秘義務の有無に関わらず、アクセスにより知り得た情報を目的外に利用し、又は正当な理由なしに漏らしてはならない。異動、退職等により職務を離れた場合においても同様である。

１０） 利用者は、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。

１１） 利用者は、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。

１２） 利用者は、離席する際は、窃視防止策を実施する（ログアウトまたはスクリーンロック等）。尚、不特定多数の者が出入する部署においては、必要に応じて偏光フィルム等による窃視防止措置を講ずる。

１３） 不正ソフトウェアの混入、サイバー攻撃を受けた場合は、ネットワークから端末を切り離すとともに、システム管理者へ連絡し、指示を仰ぎ、その指示に従う。

１２．個人情報の保存場所

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は、スタッフの常駐または施錠できる部屋に設置すること。また、個人情報が保存されている機器等の重要な機器に盗難防止用チェーン等を設置すること。

１３．情報システムへのアクセス制限の決定方針及び、記録、点検等のアクセス管理

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、以下の内容に沿って、アクセス管理を行い、定期的に管理状況を運用責任者に報告をする。

１）情報区分とアクセス権限に基づくアクセスできる診療録等の範囲を定め、アクセス管理を行う。

２）ＩＤ、パスワード等により診療録データへのアクセスにおける識別と認証を行う。

３） ＩＤには原則として管理者権限は付与しない（ユーザー権限とする）。ただし、サーバー管理のために必要な場合は、システム管理者の承認の上、管理者権限を付与する。
４） Administrator 等の OS のデフォルト ID は使用せず、個別 ID とする。
５） システム管理者は、情報システム、データへの使用状況を監視するため、以下の事項を含むアクセスログを取得する。異常なアクセスがあったときは警告を発生し、ネットワークを切断する。
・利用者ＩＤ
・端末ＩＤ
・操作の日時
・データへのアクセス結果（誰が、いつ、誰の情報に、どのようなアクセスをしたか）
６） システム管理者は、取得したアクセスログを定期的に検証し、問題がある場合は、速やかに措置を講じる。
７） 取得したアクセスログは、情報システムの重要度に合わせ定期的に検証し、問題のないことを確認する。問題がある場合は、速やかに適切な措置を講じる。
８） アクセスログは、重要度に合わせ定めた方法・場所・期間に従い保管する。
９） アクセスログを廃棄する場合は、電子媒体の廃棄方法に準じて実施する。
１０） アクセスログは、特定の担当者以外アクセスできない仕組みとする。

１４．個人情報を含む記録媒体の管理（保管・授受等）
１） 個人情報を記録した可搬型記録媒体（CD-ROM,DVD,USB メモリ,ポータブル型 SSD 等）は、施錠できるキャビネットに保管し、その所在を台帳に記録し、管理する。
２） オフラインバックアップを記録した媒体は、個人情報を記録した可搬型記録媒体として扱い管理する。
３） 個人情報を可搬型記録媒体で授受する場合は、授受の記録を残す。
４） 特に許可した場合を除き、データのバックアップ業務以外には外部記憶媒体への個人情報の複写を禁止する。
５） 媒体使用時は、必ずコンピュータウイルス等の不正なソフトウェアの混入がないか確認する。
６） 媒体毎に、保存可能容量（サイズ）、期間、バックアップの頻度や方法等を明確にすること。

１５．個人情報を含む媒体の廃棄
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、結果を記録に残すこと。
１） 紙媒体の廃棄は、原則シュレッダーによる粉砕処理とする。大量に廃棄する場合などは、外部業者に委託することができるが、その場合は、廃棄証明書を受領するものとする。
２） 電子媒体の廃棄は、原則粉砕処理とする。
３） ＰＣのハードディスク、SSD 等については、米国国防総省 NSA 規格相当もしくはそれ以上の回

復困難な方法でのデータの上書処理により既存データを書き換え、その後データを消去する。なお、このデータの消去処理を外部業者に委託することができるが、その場合は、消去証明書を受領するものとする。尚、レンタル・リース切れによるＰＣの返却等により処分する場合も、本規定に則り、ＰＣ上の不要データの完全消去を行うこととする。

１６．リスクに対する予防、発生時の対応方法

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、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こと。

１７．技術的対策と運用的対策の策定

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こと。

２）システムの保守時には、必要に応じて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こと。

３）システム改造時は、必要に応じて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こと。

４）個人情報を扱うクラウドサービスを使用する場合は、「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」に示される「サービス仕様適合開示書」もしくはそれを具体化した「製造業者/サービス事業者による医療情報セキュリティ開示書（ JIRA/JAHIS）」、サービス・レベル合意書（SLA）等で技術的対策内容を確認すること。

１８．IoT 機器の利用に関する事項

１）IoT 機器の利用において、サイバーセキュリティに関して対策を行うこと。

２）製造販売事業者提供の文書を運用実施手順書に含めること。

３）購入後に発見された脆弱性対策に実施においても同様とすること。

４）患者への機器貸し出しに関して、リスク等の注意事項、不具合時の連絡等の情報を提供すること。

５）機器の管理台帳により、使用終了機器・不具合未対応機器の再利用を防止すること。

６）機器・システムの状態や通信状態を収集・把握し、ログを適切に記録すること。

７）Io 機器により医療情報を取り扱う場合は、製造販売業者から提供を受けた当該医療機器のサイバーセキュリティに関する情報を基にリスク分析を行い、リスク対策表を作成すること。

１９．無線 LAN の管理

無線 LAN を利用する際は、以下の措置を実施する。

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）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に設定する（ステルスモード、ANY 接続拒否、暗号化等）。暗号化には WPA2/AES 等を採用する。
３）不正アクセスの対策を施す（MAC アドレスによるアクセス制限を行う）。
４）不正な情報の取得を防止するため、通信を暗号化し情報を保護する。
５）電波を発する機器（携帯ゲーム機等）によって電波干渉が起こり得るため、無線 LAN 利用規則等を院内関係者および利用可能性のある患者へ説明する。
６）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。

２０．委託契約における安全管理・守秘条項

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こと。

２１．再委託の場合の安全管理措置事項

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こと。

２２．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

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こと。必要と認めた場合は、適時監査を行うこと。

保守作業において医療情報を用いる場合には、漏洩等が生じないために、医療機関内で作業を完結させる、あるいは、やむを得ず持ち出す場合は暗号化処理を施すなど、必要な対策を講じること。

２３．持ち出し対象となる情報および情報機器の規定

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こと。
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、利用者に公開すること。
[持出情報機器一覧]
３）個人保有又は個人管理下の情報機器の業務利用（BYOD）は、原則利用禁止とする。
BYOD を認める場合、管理者は下記を遵守すること。
・利用者に対し、端末や OS 等に応じて推奨されている適切な方法により、アプリケーションをインストールするよう指導すること。
・アプリケーション等の脆弱性に関する情報を収集し、利用者が脆弱性の明らかになったアプリケーションを使用していないか、定期的に確認すること。
・利用者に対し、OS の設定変更を禁止すること。

２４．持ち出した情報および情報機器の運用管理規定

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、承認を得ること。[情報機器持出申請書]

２）システム管理者は、情報が格納された可搬媒体および情報機器の所在について台帳に記録すること。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こと。[持出情報機器一覧]

２５．持ち出した情報および情報機器の安全管理規定

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る等、適切なパスワードの設定・運用を行うこと。

２）持ち出す情報機器について、コンピュータウイルス対策ソフトをインストールしておくこと。

３）公衆無線 LAN を使用しないこと。公衆無線 LAN しか使用できない環境にある場合には「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こと。

４）持ち出した情報を、別途定められている以外のソフトウェアがインストールされた情報機器で取り扱わないこと。[インストール許可ソフトウェア一覧]

５）持ち出した情報機器には、別途定められている以外のソフトウェアをインストールしないこと。[インストール許可ソフトウェア一覧]

２６．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こと。

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したがって、対応すること。

２７．利用者への周知徹底

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、利用者に以下のことを周知させること。

- 持ち出しの都度、事前にシステム管理者に許可申請が必要であること。
- 持ち出す情報は必要最低限とし、暗号化などのセキュリティ対策を行うこと。
- 院外への持ち出し時は、常に身辺に置いて目を離さないようにすること。
- 紛失や盗難等が発生した場合は、ただちにシステム管理者に連絡すること。
- 院外で使用し持ち帰った電子記憶媒体または院外から持ち込んだ電子記憶媒体を院内ＰＣに接続する場合は、当該電子記憶媒体についてコンピュータウイルスチェックを行うこと。
- 原則公衆無線 LAN を使用しないこと。公衆無線 LAN しか使用できない環境にある場合には「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こと。
- 申請した目的以外に使用しないこと。

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い、その記

録を残すこと。

２８．安全を技術的、運用的面から確認する規定

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、地域医療連携基盤運用機関および連携機関と密に連携を行い、安全な方法で医療情報を交換可能なように、技術的および運用的対策を講じること。

２）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こと。

２９．情報処理事業者との通常運用時、事故処理時それぞれで責任分界点を定めた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こと。

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こと。

３０．リモートメンテナンスの基本方針

１）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、相手の保守会社等、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こと。

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こと。

３１．従業者による医療機関等の外部からアクセスする場合の運用管理規定

外部からアクセスを許容する機器については、以下を実施すること。

１）外部からアクセスする利用者は、事前に許可されたものに限定する。

２）外部からアクセスを許容する機器は、事前に許可されたものに限定する。

３）紛失等があった場合は、ただちにシステム管理者に連絡し、パスワードの変更や抹消を行い、アクセスできない措置をとること。

４）セキュリティが保たれていることをメーカーからのチェックリストにて確認し、技術的な安全対策が行われていることを確認する。

５）その機器が許可された際の状態を保持していることを定期的に確認すること。

３２．医療サービス体制に支障が発生する非常時の規定

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、別途定める手順にしたがって運用を行うこと。

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こと。

３３．システムの縮退運用管理規定、非常時の機能と運用規定

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こと。

３４．サイバー攻撃対策のためのバックアップ取得

１）電子カルテの診療録データは特に重要であるため、別途定める「オフラインバックアップ手順」に従い、定期的にオフラインバックアップを取得する。[オフラインバックアップ手順]

２）バックアップは、3世代分の記録媒体を用意し、交換してバックアップを行う。

３）バックアップ取得後は、必ず手順に従い物理的に記録媒体を取り外し、個人情報記録媒体として保管を行う。

４）バックアップからの復元は、システム保守会社に連絡し、復旧作業を実施する。

３５．報告先と内容一覧

災害、不正ソフトウェアの混入などによるサイバー攻撃を受けた（疑い含む）場合、サイバー攻撃により障害が発生し、個人情報の漏洩や医療提供体制に支障が生じる又はそのおそれがある事案であると判断した等の場合には、別途定める一覧の連絡先に連絡すること。

３６．マニュアルの整備

システム管理者は、情報システムの取扱いについて必要に応じ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こと。

３７．定期または不定期なシステムの取り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

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及びプライバシー保護に関する研修を行い、その記録を残すこと。また、研修時のテキスト、出席者リストを残すこと。

３８．従事者に対する人的安全管理措置

当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。

３９．運用管理規程の見直し

運用管理責任者は、適切な医療情報システムの運用を維持するために、運用管理規程の見直しを定期的に実施すること。

４０．入力者及び確定者の識別及び認証

１）システム管理者は、電子保存システムの入力者及び確定者の登録を管理し、そのアクセス権限

を規定し、不正な利用を防止する。

２）電子保存システムにおいて保存されている（される）情報の確定者は、各記録について法令に定められた作成責任者とする。

４１．情報の確定手順と、作成責任者の識別情報の記録

利用者は、電子保存システムへの情報入力・更新に際して、確定操作（システムにて定められた入力情報が正しいことを確認する作業）を行ない、入力情報に対する責任を明示する。

確定した情報の保存期間は、法令で定められた期間などをもとに定めること。

※カルテは法令で定められている「完結の日から 5 年間」（保険医療機関及び保険医療担当規則第９条）を最低期間とする。

４２．代行入力の承認記録

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こと。

４３．機器・ソフトウェアの品質管理、動作状況の内部監査規程

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こと。

４４．情報の所在管理

システム管理者は定期的に情報の所在確認を行うこと。

４５．見読化手段の管理

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。

４６．見読目的に応じた応答時間とスループット

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。

４７．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。

２）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。

４８．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こと。

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常に目の届く範囲もしくは入退室管理された場所に設置すること。[入退管理表]
３）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こと。
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ること。
５）設置機器は定期的に点検を行うこと。

４９．不適切な保管・取り扱いによる情報の滅失、破壊の防止策

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こと。

５０．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こと。
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こと。

５１．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

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こと。

５２．相互運用性確保

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。

５３．スキャナ読み取り書類の運用

紙及びフィルム媒体をスキャンして電子保存する場合、原本は別途保管し、診断等の利用を行わない目的で利用可能な参照用画像として適切な解像度・フォーマット形式で保存すること。

５４．外部保存を受託する機関での保存確認と患者への説明
１）外部保存を委託する場合は、システム管理者は、外部保存委託先における保存性対策が適切であることを少なくとも以下の事項を確認する。
a. 医療情報等の安全管理に係る基本方針・取扱規程等の整備状況
b. 医療情報等の安全管理に係る実施体制の整備状況
c. 不正ソフトウェア等のサイバー攻撃による被害を防止するために必要なバックアップの取得及び管理の状況
d. 実績等に基づく個人データ安全管理に関する信用度
e. 財務諸表等に基づく経営の健全性
f. プライバシーマーク認定又は ISMS 認証の取得
g. 「政府情報システムにおけるクラウドサービスの利用に係る基本方針」の「セキュリティクラウド認証等」に示す下記のいずれかの認証等により、適切な外部保存に求められる技術

及び運用管理能力の有無。

・政府情報システムのためのセキュリティ評価制度（ISMAP）

・JASA クラウドセキュリティ推進協議会 CS ゴールドマーク

・米国 FedRAMP

・AICPA SOC2（日本公認会計士協会 IT7 号）

・AICPA SOC3（SysTrust/WebTrust）（日本公認会計士協会 IT2 号）

上記認証等が確認できない場合、下記のいずれかの資格を有する者による外部監査結果により、上記と同等の能力の有無を確認すること

・システム監査技術者

・Certified Information Systems Auditor ISACA 認定

h. 医療情報を保存する機器が設置されている場所(地域、国)

i. 受託事業者に対する国外法の適用可能

また、監査者は必要に応じて外部保存委託先の設備を監査する。

2）運用責任者は、外部保存していることの患者への周知（例、掲示内容）が計られていることを適宜確認する。

3）医療機関等が自ら暗号化を行い、暗号鍵を事業者に預託する場合、暗号鍵の使用は非常時に限定し、通常時の利用は禁止する。暗号鍵の使用には、院長またはシステム管理責任者の承認を必要とする等の仕組みを構築すること。

５５．その他

その他、本規程の実施に関し必要な事項がある場合は、院長がこれを定める。

５６．本規程は　2025 年 10 月　2 日より施行する。

医療機関名称：森本医院

医療機関住所：福岡市西区丸川 1 丁目 1539-1

院　長　名： 森本 健