医療法人徳隣会　院内情報システム（オンライン診療を含む）

承認	作成

運用管理規程

1. 総則

1.1. 目的

この規程は、医療法人徳隣会（以下「当法人」という。）の情報セキュリティ基本方針に従い、院内情報システム（以下、「情報システム」という）の安全かつ合理的な運用を図り、併せて法令に保存が義務付けられている診療録（診療記録を含む）の電子媒体による運用（電子保存システム）・オンライン診療の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。

1.2. 対象情報

１）対象システム

情報システムとは、当法人で運用する電子カルテシステム及び電子カルテシステムと接続する部門システム並びに接続機器など診療情報を取り扱うシステムをいう。

２）適用対象

管理対象となる情報は、情報システムで取り扱う電子情報だけでなく、情報システムへ入力する前の紙媒体の情報や、従業者の履歴書等全ての個人情報を適用対象とする。

３）取り扱い情報

対象システムの扱う情報については、下記情報システムが取り扱う情報とする。

・電子カルテシステムおよびレセプトコンピュータシステム

・オンライン診療で使用するシステム

1.3. 標準規格

システム管理者は、システム変更・改定時の対象とするため、フォローすべき法令及び標準規格の変更状況を確認し維持する。主な法令は以下の通りである。

医師法
医療法
薬事法
個人情報の保護に関する法律
JIS Q 15001：2006 個人情報保護マネジメントシステム－要求事項
保健医療福祉分野のプライバシーマーク認定指針
医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン
医療情報システムの安全管理に関するガイドライン
診療情報の提供等に関する指針
看護記録および診療情報の取り扱いに関する指針

2. 用語の説明

以下、本書で使用する用語を説明する。

Ｎｏ	用語	説明
1	ユーザ ID	利用者を識別するために用いられる符号。
2	電子証明書	データの暗号化や認証などの目的に使う公開鍵が正当なものであることを証明するために、認証局によって発行される電子データ。
3	クライアント証明書	利用者が使用する機器が正当なものである（成りすましでない）ことを公開鍵暗号技術により検証するため、利用者の端末にインストールする電子証明書。
4	ウイルス	電子メールやホームページ閲覧などによって PC に侵入し、PC 内のファイルを消去したり、PC を起動できなくするなどの被害をもたらす悪意をもったプログラムの一種。
5	ウイルス対策ソフト	PC にインストールし、ウイルスを検知・除去してウイルス感染から PC を守るためのソフトウェア。
6	LAN	Local Area Network の略称。
7	無線 LAN	無線通信を利用してデータの送受信を行う LAN システム。
8	WPA/AES	Wi-Fi Protected Access/ Advanced Encryption Standard の略称で、無線 LAN の暗号方式の一種。
9	SSID	Service Set Identifier の略称で、無線 LAN 通信規格で定められているアクセスポイントの識別子を意味する。同じ空間に複数のアクセスポイントがあった場合、混線を避けるために使われる。
10	MAC アドレス	Media Access Control address の略称で、PC などのネットワーク機器等に割り当てられた、全世界で唯一固有の識別子であり、LAN 経由のデータの送受信で使われる。
11	PKI	Public-Key Infrastructure の略称で、公開鍵と秘密鍵のキーペアからなる公開鍵暗号方式という技術を利用し、インターネット上で安全に情報のやりとりを行うセキュリティのインフラ（基盤）を意味する。
12	Winny	Peer to Peer 技術を応用したファイル共有ソフトの一種であり、PC 内に格納されている電子データ（電子ファイル）がインターネット上に漏洩してしまう恐れがある。

3. 管理体制

3.1. 管理者、責任者の任命

１）当院に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、院長をもってこれに充てる。

２）院長は必要な場合、運用責任者及び個人情報保護管理者を内部の者から別に指名することができる。

３）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管理者（以下「システム管理者」という。）を置き、院長が指名した医療情報部長をもってこれに充てる。

４）情報システムを監査するため、情報システム監査責任者（以下、「監査責任者」という）を置き、院長が内部の者から指名する。

５）各部門システムを円滑に運営管理するため、各部門に情報システム部門管理者（以下、「部門管理者」を置き、システム管理者が推挙し、院長が任命する。

3.2. 情報システム管理委員会の設置

１）情報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、院長のもとに情報システム管理委員会を設置する。

２）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、情報システム管理委員会の審議を経て、院長がこれを定める。

3.3. 文書管理体制

各種規定、様式、記録、契約書、マニュアル等の文書の管理については、情報システム運用責任者が、作成日、作成者を明らかにした一覧表を作成の上、ファイリングを行う。

3.4. 監査体制

院長は、情報システムを円滑に運用するため、公平、かつ、客観的な、立場にある情報システム監査責任者（以下「監査責任者」という。）を内部の者から指名し、監査の実施及び報告を行う責任及び権限を他の責任にかかわりなく与え、業務を行わせる。

3.5. 苦情・質問受付体制

１）当法人は、個人情報の取扱い及び情報システムの運用に関して、本人及びシステム利用者からの苦情及び質問を受け付けて、適切、かつ、迅速な対応を行う手順を確立し、かつ、維持する。

２）当法人は、上記の目的を達成するために、患者及びシステム利用者からの、苦情・質

問を受け付ける窓口を設ける。

3）個人情報に関する苦情窓口担当者ならびに各担当者は、本人より直接または間接的に苦情を受けた際に、速やかに対応しなければならない。

3.6. 事故対策体制

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文書化し、利用者に周知の上、常に利用可能な状態におく。

3.7. 教育・訓練体制

1）情報システム管理者は、情報システムの取扱い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。

2）情報システム管理者は、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。

4. 管理者及び利用者の責務

4.1. 運用責任者の責務

1）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。

2）患者又は利用者からの、情報システムについての苦情を受け付ける窓口を設ける。

3）監査責任者に監査を実施させ、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る。

4.2. システム管理者の責務

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。

2）診療情報の安全性を確保し、適切な設定を行い、常に利用可能な状態に置いておく。

3）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。

4）情報システムの利用者の登録を、人事異動等による利用者の担当業務の変更等に併せて管理し、そのアクセス権限を規定し、不正な利用を防止する。

5）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。

6）情報システムの安全管理の見直し及び改善の基礎として、運用責任者に情報システムの運用状況を報告する。

4.3. 監査責任者の責務

1）監査責任者は、監査計画を立案し、監査を指揮し、監査報告書を作成し、運用責任者に報告する。
2）監査責任者は、情報システムの監査を円滑に実施するため、情報システムに関する監査を担当する監査員を置くことができる。
3）監査員の選定及び監査の実施においては、監査の客観性及び公平性を確保する。
4）監査員は自らの所属する部門を監査しない。

4.4. 情報システム部門管理者の責務

1）情報システム部門管理者（以下、「部門管理者」という）は、自部門のシステムの運用に管理に責任を持つ。
2）部門管理者は、自部門のマスタを管理する。
3）自部門のマスタに変更・追加が生じた場合には、速やかに書面をもってシステム管理者に提出する。
4）マスタの変更の際に、過去の情報に対する内容の変更が起こらない機能を備えること。

4.5. 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、ユーザＩＤとパスワードによって、システムに自身を認識させる。
2）利用者は、自身のユーザＩＤとパスワードを管理し、これを他者に利用させない。
3）利用者が、正当なユーザＩＤと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、その利用者が責任を負う。
4）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。
5）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。
6）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。
7）利用者は、患者等のプライバシーを尊重し、職務上知ることが必要な情報以外の情報にアクセスしてはならない。
8）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。
9）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。
１０）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。

１１）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。

１２）ウイルスに感染又はその恐れを発見した場合は、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。

5. 一般管理における運用管理事項

5.1. 利用者の登録・認証

１）利用者のユーザ認証は、ユーザＩＤとパスワードに加えてクライアント証明書を使用した二要素認証を用いる。

２）ユーザＩＤの付与は、個人単位とし共有することはない。

３）システム管理者は、利用する情報システムの利用者等の申請を受け、審査し、ユーザ登録を実施する。

４）システム管理者は、職員等の採用時、異動時、退職時に合わせ、速やかにユーザの登録、変更、削除の措置を取る。

５）ユーザ登録時は、システム管理者の登録処理による初期値のパスワードとし、その後速やかに、利用者が個々のパスワードへ変更する手順とし、システム管理者であってもパスワードを推定できない仕組みとする。

６）パスワードの有効期限は、原則２ヶ月以内とし、利用者が更新する。システム管理者は、２ヶ月以上パスワードを更新しない利用者に対し、警告を与え、速やかに更新させるものとする。

７）利用者が、パスワードを紛失し、情報システムの利用ができなくなった場合は、システム管理者へパスワードの初期化依頼を提出する。

８）システム管理者は、利用者からのパスワード紛失の申請書を受け、ユーザ登録の確認後、パスワードの初期化を行ない、利用者へ知らせることとする。この場合、利用者は、速やかにパスワードを変更することとする。

９）OS の利用者ＩＤには原則として管理者権限は付与しない（ユーザ権限とする)。

10）システム管理者は、クライアント証明書を適切に管理し、利用者が利用する端末にクライアント証明書をインストールする。

5.2. 部外者の立ち入り

部外者が執務室等に立ち入る場合は、同伴者等の管理を実施する。

5.3. 端末管理

１）盗難の恐れがある端末（ノート PC 等）は、盗難防止用ワイヤーロックで固定するか、

使用しない際は鍵のかかる保管庫に保管管理すること。

２）離席時など、特定の時間使用しなかった場合は、なりすましによる使用を防ぐため、パスワード付きスクリーンロック又は、自動ログオフ機能を設定すること。

３）端末の使用に際しては、画面を廊下側に向けない、窃視防止フィルムを貼るなどの、窃視防止に努めること。

４）私有のＰＣを持込み、院内ＬＡＮに接続することは、禁止とする。

５）システム保守のため委託先等の外部者が院内へ PC を持ち込み院内ＬＡＮへ接続する場合は、システム管理者に申請し、許可を得てから行うこととする。

６）全端末の時刻情報はサーバ時刻と同期させる。

5.4. ネットワーク管理

１）院内ＬＡＮへの接続は、システム管理者の判断・責任により行う。

5.5. インターネットの利用・管理

インターネットの利用を許可されたネットワークにおける利用・管理については以下に定める。

１）インターネット利用は、業務上必要な場合に限られ、私的利用は禁止とする。

２）業務遂行上必要のないインターネットサイトからデータ・ソフトウェア等のダウンロード、インストール等の行為は、原則禁止とする。

３）システム管理者は、ホームページを含む不正アクセスや改ざんの防止のため、インターネットに係る各サーバ、ルータ等に適切な管理策等の措置を講じる。

４）システム管理者は、ホームページの利用状況を監視し、不正アクセスやホームページの改ざんの有無を確認し、問題がある場合は、適切な措置（予防・是正）を講じる。

５）当院の情報を、ホームページを用いてインターネットへ公開、又は公開情報を変更・削除する場合は、システム管理者へ申請する。

６）システム管理者は、内容の確認後に、登録・変更を実施する。

5.6. 電子メールの利用・管理

当院では、業務上特に電子メールは用いず、電子メールアカウントを職員に対して付与していないため、管理対象外とする。

5.7. ウイルス対策ソフトの導入と運用

１）悪意のあるソフトウェア等から保護するため、全てのサーバ、端末にウイルス対策ソフトを導入し、パターンファイルは常に最新のものを使用する。

２）定期的にソフトウェア等のウイルスチェックを行ない、感染の有無を確認する。

3）ウイルス対策ソフトは、常に稼動させておくこととする。
4）業務上許されたデータ取得分については、ウイルスチェックを行い、問題のないことを確認後に使用する。
5）電子メールサーバは、すべての着信メールについてウイルスチェックを行ない、感染の有無を確認する。
6）ネットワークに接続するサーバと端末は、配信型のウイルス対策ソフトの利用を可能とし、パターンファイルの更新は自動更新で行うこと。
7）ネットワークに接続していないＰＣは、ＰＣの利用者が常に更新情報の入手に努め、最新パターンファイルを入手し更新する。
8）インターネットに接続していない院内 LAN は、最新のパターンファイルを、インターネットに接続したウイルスサーバにより取得し、院内情報システムのウイルスサーバに手動で更新・配信する。

5.8. セキュリティパッチの適用

1）院内情報システムのサーバ及び端末には、ベンダーからの保証がない限り、原則として修正プログラムは適用しない。
2）インターネットへの接続を許可された端末については、オペレーティングシステムやパッケージソフト等のパッチなどの修正プログラムがメーカーより発行された場合、必要であれば既存システムの影響を考慮して適切に実施し、その記録を残す。

5.9. 媒体管理

1）個人情報を記録した可搬型記録媒体（ポータブル HDD,CD-ROM,DVD,USB メモリ等）は、施錠できるキャビネットに保管し、管理する。
2）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。
5）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。
6）媒体使用時は、必ず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。

5.10. 廃棄

個人情報を記した媒体（紙媒体、情報機器を含む）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。

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のハードディスク等については、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。

4）特に重要な情報を廃棄する場合は、必要に応じて立ち会うものとする。

5.11. 文書管理

当法人は、以下の技術的と運用的対策の分担を定めた文書の管理を実施する。

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。

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したがっていることを確認する。

3）システム改造時は、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。

5.12. 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（少なくとも SSID や 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 利用規則を院内関係者に説明をする。

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。

5.13. 電子署名・タイムスタンプ

1）法令で署名または記名・押印が義務付けられた文書等において、記名・押印を電子署名に代える場合、以下の条件を満たす電子署名を行う。

(1) 厚生労働省の定める準拠性監査基準を満たす保健医療福祉分野 PKI 認証局もしくは認定特定認証事業者等の発行する電子証明書を用いて電子署名を施す。

(2) 電子署名を含む文書全体にタイムスタンプを付与する。

(3) 上記タイムスタンプを付与する時点で有効な電子証明書を用いる。

2）システム管理者は、電子的に受領した文書に電子署名が有る場合の、署名検証手順を定める。具体的には、電子署名が有効である間に、電子署名の検証に必要となる情報（関連する電子証明書や失効情報等）を収集し、署名対象文書と署名値とともにその全体に対してタイムスタンプを付与する等の対策を実施する。

6. サーバ管理における運用管理事項

6.1. 電子カルテシステムについて

1）医療情報管理のための各種ガイドラインに合致したクラウド環境にサーバ機能を設けているため、サーバ管理に関する運用は院内では発生しない。

2）バックアップについてもクラウド環境に自動保存されるため、院内での運用は発生しない。

6.2. その他システムについて

6.2.1. サーバの導入

1）システム管理者は、情報システムの開発・保守により情報システム機器・ソフトウェア等を導入・取替える場合には、システム要件を明確にするとともに、システムのセキュリティ要件を明確にし、文書化する。

2）システム管理者は、情報システムのリプレース時のデータ移行や関連するデータ交換等、以下の事項の十分な確認を実施する。

・アクセス制御に関する要件の確認

・データ入力権限、入力エラーとする要件、エラー時の対処方法についての必要性の確認

・データ変更・削除権限、処理順序の制限、障害時の回復処理及び手順等の要件の確認

・データ出力の方法、装置等に対する要件の確認

・情報システムの重要度に応じた要件の確認

・既存システムへの影響（サーバ、ネットワーク等）の有無の確認

6.2.2. 保安・環境維持措置

1）運用責任者は、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（以下、「サーバ室等」という）における火災、その他の災害、盗難に備えて、非常電源装置などによる必要な保安措置を講じなければならない。

2）電子的な情報を保存している媒体や機器が置かれている場所（サーバ室等）の温度、湿度等の環境を適切に保持する。

6.2.3. サーバの管理及び環境設定

1）システム管理者は、導入・取替えサーバをサーバ室等のセキュリティが保たれた管理領域に設置する。

2）運用側の情報システムへの影響を考慮し、開発側と運用側との情報システムは、分離する。

6.2.4. 入退室管理

1）サーバ室等は、スタッフの常駐または施錠できる部屋に設置する。

6.2.5. サーバの運用

1）システム管理者は、サーバへのアクセス状況・稼動状況を定期的（月１回以上）に確認し、問題がある場合は、速やかに措置を講じる。

2）システム管理者は、個々のサーバ及び端末機のクロックを定期的（月１回以上）に確認するとともに、誤差が生じている場合は標準時間に設定し直す。

6.2.6. 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（ユーザ権限とする)。ただし、サーバ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 のディフォルト 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等の機能を有すること。

・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（月１回以上）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）アクセスログは、特定の担当者以外アクセスできない仕組みとする。また、アクセスログへのアクセス確認を別人が実施すること。

6.2.7. データのバックアップ

1）情報システムの重要度に応じて、システムファイル及びデータのバックアップを定期的に取得する。
2）バックアップの作業に当たる者は、その作業の記録を残し、部門管理者の承認を得る。
3）バックアップ媒体は、施錠できるキャビネット、耐火金庫等に保管し、管理する。
4）バックアップ媒体は１年間に１回新品に交換する。媒体に品質の劣化が予想される場合や、劣化原因と思われる障害が発生した場合は、直ちに新品に交換を行う。
5）部門管理者は、記録媒体及び機器のログを確認し、記録媒体の劣化や機器の不具合を確認する。エラー・警告のログが発見された場合は、直ちに新品の記録媒体に記録を複写すること。
6）情報がき損した時に、バックアップされたデータを用いてき損前の状態に戻せることを確認し、リストア手順を規定する。

6.3. リスク対応（障害対策）

システム管理者は、院内情報システムに係る障害が発生した場合には、事態の掌握・収拾及び被害を最小限に止め、復旧作業の軽減、時間の短縮等を図るため、次の措置を講じなければならない。

1）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する。
2）利用者に対し事故発生時には、速やかに報告することを周知させる。
3）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、運用ルール等の見直しを実施する。
4）基幹システム以外の部門システムで障害が発生した場合は、当該部門の部門管理者に報告し、部門管理者は、担当 SE と連携して復旧対策を講じるとともに、障害内容をシステム管理者に報告する。
5）部門管理者は、障害内容が部門間インターフェイスの要因であると判断した場合は、関係部門に報告するとともに、システム管理者に報告し、復旧対策の指示を待つこと。その際は、状況に応じて伝票での運用に切り替え、通常業務の稼働に努めること。

7. 業務委託の安全管理措置

7.1. 業務委託における安全管理

業務を当院外の所属者に委託する場合は、以下の措置を実施する。

1）守秘事項を含む業務委託契約を結ぶ。契約の署名者は、その部門の長とする。

2）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（委託先が、許可無く個人情報を含むデータを組織外に持ち出すことは禁止する)。

3）業務委託の契約書には、次に示す事項を規定し、十分な個人情報の保護水準を担保する。

a) 委託者及び受託者の責任の明確化
b) 個人情報の安全管理に関する事項
c) 再委託に関する事項（再委託する事業者にも委託先と同等の義務を課すこと）
d) 個人情報の取扱状況に関する委託者への報告の内容及び頻度
e) 契約内容が遵守されていることを委託者が確認できる事項
f) 契約内容が遵守されなかった場合の措置
g) 事件・事故が発生した場合の報告・連絡に関する事項
h) 一連の委託業務終了後に関する事項（終了報告、確実にデータを消去する等）
i) 保守要員のアカウント情報の管理に関する事項（適切に管理することを求める）

7.2. 再委託の安全管理措置

委託先事業者が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及び契約がなされていることを条件とする。さらに、当院との業務委託の契約書に再委託での安全管理に関する事項を加える。

7.3. 保守作業報告確認

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、作業報告確認のため、システム管理者は、保守会社における保守作業に関し、以下のような確認を実施する。また、必要と認めた場合は適時監査を行う。

1）保守要員用のアカウントの確認（保守要員個人の専用アカウントを使用すること)。

2）保守作業等の情報システムに直接アクセスする作業の際には、作業者・作業内容作業結果の確認（原則として日単位)。

3）清掃等、直接情報システムにアクセスしない作業の場合の定期的なチェック。

4）保守契約における個人情報保護の徹底。

5）保守作業の安全性についてログによる確認。

8. 情報および情報機器の持ち出しについて

8.1. 持ち出し対象となる情報および情報機器

1）リスク分析を実施し、情報および情報機器の持ち出しに関する方針を定める。

2）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。

3）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。

8.2. 持ち出した情報および情報機器の管理

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。

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。

8.3. 持ち出した情報および情報機器への安全管理措置

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、また定期的に変更する。

2）持ち出す情報機器について、ウイルス対策ソフトをインストールしておく。

3）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情報機器で取り扱わない。

4）持ち出した情報機器には、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しない。

5）持ち出した情報を、例えばファイル交換ソフト（Winny 等）がインストールされた情報機器で取り扱わないこと。

6）持ち出した情報機器をネットワークに接続したり、他の外部媒体を接続する場合は、コンピュータウイルス対策ソフトの導入やパーソナルファイアウォールを用いる等して、情報端末が情報漏えい、改ざん等の対象にならないような対策を施す。

8.4. 盗難、紛失時の対応

1）情報に対して暗号化、アクセスパスワードを設定する等、容易に内容を読み取られないようにすること。

2）持ち出した情報および情報機器の盗難、紛失時には、速やかにシステム管理者に届け出る。

3）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従って対

応する。

8.5. 従業員への周知

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。

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う。また、研修時のテキスト、出席者リストを残す。

9. 外部の機関と医療情報を交換する場合の措置

9.1. 安全を技術的、運用的面から確認する規程

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および運用的対策を講じる。

2）システム管理者は、外部のシステムと連携する場合、連携のための設定が正確に行われるように十分な確認を実施する。

3）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。

9.2. リスク対策の検討文書の管理

リスク対策の検討文書を作成し維持・管理する。

9.3. 契約文書の管理と契約状態の維持管理

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、運用委託業者などとの間で、責任分界点や責任の所在を契約書等で明確にする。また、患者あるいは家族から個人情報を含む医療情報の連携に対する同意書を取得する。

2）上記の契約状態や同意書取得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。

9.4. リモートメンテナンス時の安全管理

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。

2）適切なアクセスポイントの設定、プロトコルの限定、アクセス権限管理等を行って不必要なログインを防止する。

3）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。

9.5. モバイル端末等のアクセス管理

1）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定に従ったものに限定する。

規定には、以下の内容を定める。

・医療機関等の内部のシステムに不正な侵入等を防止する技術的対策
・外部からアクセスを許容する機器及びその状態
・外部からアクセスを許容した機器が、その許容状態を保持しているのかを確認する手順

2）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。

10. 災害等の非常時の対策

10.1. 医療情報システムの BCP

1）災害、サイバー攻撃などにより一部医療行為の停止など医療サービス提供体制に支障が発生する非常時の場合、別途定める事業継続計画(BCP)にしたがって運用を行う。
2）医療サービスを提供し続けるための BCP の一環として“非常時”と判断する仕組み、正常復帰時の手順を別途定める。すなわち、判断するための基準、手順、判断者、をあらかじめ決めておく。
3）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、手順に従ってシステム管理者が判断する。

10.2. システムの縮退運用管理

システムの縮退運用時や非常時の運用に関しては BCP 内に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。

- システムが縮退運用を行っている際の運用ルール
- 正常復帰後に、代替手段で運用した間のデータ整合性を図る手順
- 「非常時のユーザアカウントや非常時用機能」の管理手順

10.3. 報告先と内容一覧

1）災害、サイバー攻撃などにより一部医療行為の停止など医療サービス提供体制に支障が発生した場合、別途定める一覧の連絡先に連絡する。
2）サイバー攻撃で広範な地域での一部医療行為の停止など医療サービス提供体制に支障が発生する場合は、関連当局への報告を行う。

11. 教育と訓練

11.1. 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。

11.2. 研修の内容

１）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。また、研修時のテキスト、出席者リストを残す。

２）特に電子保存システムへの情報入力・更新に際しては、確定操作を行う前に十分に内容の確認を行うことを徹底する。

11.3. 人的安全管理措置

１）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。

２）法令上の守秘義務のある者以外を採用する場合の措置は、雇用及び契約時に守秘・非開示契約を締結する。

12. 監査

１）当法人は、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。

２）監査責任者は院長が指名する。

３）当院は、医療情報システムの運用管理規程が、「医療情報システムの運用管理に関するガイドライン」への準拠状況及び情報システムの運用状況を毎年 3 月に監査する。

４）運用責任者は、監査責任者から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。

５）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。

６）監査の内容については、監査責任者が定める。

７）運用責任者は必要な場合、臨時の監査を監査責任者に命ずることができる。

13. 是正処置及び予防処置

当法人は、患者、システム利用者等からの苦情、緊急事態の発生、監査報告、外部審査機関等からの指摘で、システムの機能、運用状況等に問題がある場合には、問題に対する是正処置及び予防処置を確実に実施するための責任及び権限を定める手順を確立し、実施し、かつ、維持する。その手順には、次の事項を含める。

a)　問題の内容を確認する。

b)　問題の原因を特定し、是正処置及び予防処置を立案する。

c)　期限を定め、立案された処置を実施する。

d)　実施された是正処置及び予防処置の結果を記録する。

e)　実施された是正処置及び予防処置の有効性を確認する。

14. 運用責任者による見直し

1）運用責任者は、適切な医療情報システムの運用を維持するために、年に１回、情報システム管理委員会において運用ルールを見直す。運用管理規程の見直しにおいては、次の事項を考慮する。

ａ）監査及びシステム管理者の運用状況に関する報告
ｂ）苦情を含む外部からの意見
ｃ）前回までの見直しの結果に対するフォローアップ
ｄ）安全管理ガイドライン等の標準規格や法令等の規範の改正状況
ｅ）社会の情勢等の変化、国民の認識の変化、技術の進歩などの諸環境の変化
ｆ）情報システムの運用状況の変化
ｇ）内外から寄せられた改善のための提案

2）運用責任者は、情報システム管理委員会の議事録をもって院長に報告する。

15. 電子保存３原則の確保

15.1. 用語の定義

1）電子保存システムとは、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。）を紙、フィルム媒体に代えて、原本として電子保存するためのシステムをいう。

2）真正性とは、正当な人が記録し確認された情報に関し第三者から見て作成の責任と所在が明確であり、かつ、故意又は過失による、虚偽入力、書き換え、消去、及び混同が防止されていることである。

3）見読性とは、電子媒体に保存された内容を必要に応じて肉眼で見読可能な状態に容易にできることである。

4）保存性とは、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、見読可能にできる状態で保存されていることである。

15.2. 真正性の確保

15.2.1. 利用者の識別及び認証

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。

2）パスワードの有効期間等を４．１に基づき実施する。

3）電子保存システムにおいて保存されている情報の作成責任者は、特に定めがない限り担当医師である。

4）作成責任者は、必要に応じ常時確認できる状態におく。

15.2.2. 情報の入力確定手順及び利用責任者の識別情報の記録

１）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（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。

２）複数の医療従事者にて共同による診療記録を作成する場合や、代行入力の際には、入力に際し、利用者の各人の ID で個々にログインする（代行入力の適用範囲を事前に明確にしておく)。また、速やかに作成責任者が最終の確定操作を行ない、入力情報に対する責任を明示する（自動確定は実施しない)。

３）作成責任者が行った操作に関して、５．２．６の５）に従い操作記録を残し、定期的に確認する。

４）確定操作された情報は、別途定める保存期間内は履歴を残して保存する。

15.2.3. 機器・ソフトウェアの管理

１）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。ハードウェア・ソフトウェアに対し、保守点検が実施できる体制を整備する。

２）装置（モダリティ等の情報発生装置）の管理責任者や操作者を運用手順書等に明記し、それ以外の人の操作を防止する。

３）当該装置による記録は、いつ・誰が行ったかをシステム機能と運用の組み合わせにより明確にする（実施記録)。

４）システム仕様書等を維持管理し、システムがどのような機器、ソフトウェアで構成され、どのような場面、用途で利用されるのかを明らかにしておく（必要に応じ、ソフトウェアの改訂履歴をベンダー等に求める)。

15.2.4. 代行操作の承認記録

技術的に更新履歴を保管し必要に応じて更新前の情報を参照する。

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と同時に適宜履歴の監査を行う。

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。

15.3. 見読性の確保

15.3.1. 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。

15.3.2. 見読化手段の管理

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。

15.3.3. 見読性に応じた応答時間とスループット

システム管理者は、応答時間の大幅な遅延がないようにシステムの維持に努める。

15.3.4. システム障害対策

システム管理者は、障害時の対応体制を整え、最新の状態を維持するとともに、データバックアップ作業が適切に実施されていることを定期的に確認する。

15.4. 保存性の確保

15.4.1. ソフトウェア・機器・電子媒体の管理

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し、情報の安全性に支障がないことを確認する。
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入退室管理された場所に設置する。
3）システム管理者は、必要に応じ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。
4）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、設置機器は定期的に点検を行う。

15.4.2. 不適切な保管・取扱いによる情報の滅失、破壊の防止策

システム管理者は、新規に配属された業務担当者に操作前の教育を実施する。

15.4.3. 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電子媒体は、障害を防ぐため、情報の保管期間、記録媒体の種別により、定めた期間内に複製を作成する。
3）保存するデータを読み取れることの確認を定期的に実施する。

15.4.4. 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

1）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移行計画を作成する。

２）システム管理者は、電子保存システムに対して必要なバグフィックスやウイルス対策の必要性をベンダーに定期的に確認し、必要に応じて対策する。

15.5. 相互運用性確保

１）システム管理者は、情報機器やソフトウェアを変更した場合に、電子保存した情報が継続的に使用できるよう維持する。

２）原則として、電子保存システムにおいて外字は使用しないこと。ただし、外字の使用を避けられない場合は、外字部分を外字であることが分かるようにして印字し（コメントを入力など)、手書きの運用を行う。

15.6. 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システムをスキャナシステムと呼ぶ。

15.6.1. スキャナ読取の対象文書

スキャナシステムにより電子保存する対象文書は以下の通り。

１）患者や他院・他施設から持ち込まれた文書等（例：紹介状、救急活動記録表等）

２）患者や医師の署名・記載が必要な文書等（例：同意書、問診票、救急活動記録表等）

３）やむ得ない事情で生じる紙媒体文書等（例：システムダウン時の診療記録等）

15.6.2. 管理監督

１）スキャナ設置部署においては、スキャナシステムを円滑に運用するため、スキャナ読み取り電子情報と原本との同一性を担保する情報作成管理者（以下、「作成管理者」という）を置く。

２）作成管理者の指名は、システム管理者が指名する。

３）作成管理者は、スキャン業務について職員を指導し、監督する責任を有し、適正な手続きで確実に実施される措置を講じる。

15.6.3. 電子署名・タイムスタンプ

スキャナで読み取った情報は、紙原本は別途保存とし、電子情報は参照情報とするため、スキャン文書全体に電子署名・タイムスタンプは付与しない。

16. その他

本規程は 2014 年 2 月より施行する。

以上

改　訂　履　歴

版数	改訂年月日	改訂内容
1.0	2014 年 2 月 1 日	新規制定
2.0	2022 年 11 月 1 日	15.2.4 代行操作の承認記録を追記
3.0	2023 年 11 月 30 日	オンライン診療システムを追記

※ 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。

※参考情報

9.3 契約文書の管理と契約状態の維持管理　で記載した、外部の機関と医療情報を交換する場合に取得する患者同意書の例を次頁に添付します。ご利用の際は、最適な内容に適宜修正の上、ご利用ください。

同意書(例)

つつみクリニック朝倉における個人情報の取り扱いについて

当院では、利用者様への在宅医療サービス提供のため、医療・看護・介護従事者等の在宅医療提供関係者間で密接に連携して、日々業務を行っております。その際、利用者様等の個人情報を以下のように取り扱う必要があります。内容をご確認いただき、同意の上、申し込みいただきますよう、お願い申し上げます。

１．利用目的について

別紙「当院における個人情報の利用目的」をご参照ください。特定された利用目的以外の個人情報の取扱い（目的外利用）は行いません。特定された目的以外で個人情報を利用する場合は、あらかじめご本人様に利用目的を通知し、同意を得るものといたします。ただし、緊急時や当事業所が在宅医療サービスの遂行上必要性が高いと判断した場合は、利用後に改めて説明させていただきます。

２．個人情報の取扱いについて

個人情報保護に関する法律等を遵守し、情報の漏えい、紛失、改ざんや不正アクセスに対する安全対策を実施し、適正に管理いたします。

３．業務委託について

在宅医療サービスを提供するに当たり、検査業務、給食業務、介護業務、情報保管管理、情報システム管理、廃棄物処理等の業務を外部に委託する場合があります。個人情報が不適切に扱われないように契約を取り交わし、管理しています。

４．利用者様等の権利

当院が保有する利用者様等の個人情報は、ご本人による開示請求・訂正・削除・利用停止等を求めることが可能です。詳しくは、相談窓口または下記の個人情報保護管理者までお願いいたします。

相談窓口：つつみクリニック朝倉
TEL ０９４６－２１-６４１１
個人情報保護管理者：三木原　恵美

（西暦）　年　月　日

私は、前記事項について説明を受け、いずれも同意します。

＜利用者（患者）＞

氏 名

住 所

＜家族＞

氏 名

住 所

別紙

当院における個人情報の利用目的

当院は、個人情報を下記の目的に利用し、その取り扱いには細心の注意を払っています。個人情報の取り扱いについてお気づきの点は、相談窓口または個人情報保護管理者までお申し出ください。

1. クリニック内での利用
   ① 利用者（患者）に提供する在宅医療サービス（計画・報告・連絡・相談等）
   ② 医療保険・介護保険請求等の事務
   ③ 会計・経理等の事務
   ④ 医療事故等の報告・連絡・相談
   ⑤ 利用者（患者）への看護サービスの質向上（ケア会議・研修等）
   ⑥ その他、利用者（患者）に係る事業所の管理運営業務

2. 他の事業所等への情報提供
   ① 連携医療機関、他の病院、診療所、助産院、薬局、クリニック、介護事業者等との連携
   ② 利用者（患者）に居宅サービスを提供するほかの居宅サービス事業者や居宅介護支援事業所との連携（ただし、サービス担当者会議等への情報提供はご利用者に文書で同意を得ます)、照会への回答
   ③ その他業務委託
   ④ 家族等介護者への心身の状況説明
   ⑤ 医療保険・介護保険等事務の委託
   ⑥ 審査支払機関へのレセプト提出、審査支払機関又は保険者からの照会への回答
   ⑦ 損害賠償保険などに係る保険会社等への相談又は届出等

3. その他上記以外の利用目的
   ① 医療・看護サービスや業務の維持・改善のための基礎資料