医療情報システム安全管理規程

株式会社Warm relationship

第1条（目的）

本規程は、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」（最新版。以下「本ガイドライン」という。）に基づき、当社が取り扱う医療情報および医療情報システムの安全管理に関し必要な事項を定め、利用者の個人情報の保護と医療・介護サービスの継続的な提供を確保することを目的とする。

第2条（適用範囲）

1. 本規程は、当社の役員および全従業者（正職員、パート職員、派遣職員、実習生、業務委託先の従事者を含む。以下「職員等」という。）に適用する。
2. 本規程の対象とする情報は、利用者の診療情報、看護記録、訪問看護計画書・報告書、指示書、ケアプラン、保険資格情報、その他利用者に関して知り得た個人情報および医療情報の一切とする。
3. 本規程の対象とする情報システムは、次のとおりとする。

区分	サービス	提供事業者	主な用途
記録・請求システム	カイポケ（カイポケレセプト、カイポケ訪問看護 for iPad、カイポケケア連携 等）	株式会社エス・エム・エス	訪問看護記録、給付費請求、提供票等の授受
記録・書面作成システム	ミルナス	株式会社オプティス	訪問看護計画書・報告書・記録書Ⅱの作成、生成AIによる文案作成
情報連携ツール	メディカルケアステーション（MCS）	日本エンブレース株式会社	連携機関との利用者情報の共有
情報連携ツール	Chatwork（ビジネスプラン）	株式会社kubell	連携機関との情報連携、職員間の業務連絡
業務基盤・文書管理	Google Workspace／Google Cloud	グーグル合同会社	文書作成・保管、内製ツールの稼働基盤

区分	サービス	提供事業者	主な用途
オンライン資格確認	オンライン資格確認等システム	社会保険診療報酬支払基金・国民健康保険中央会	資格確認、診療情報等の取得
情報機器	当社が貸与するパソコン・タブレット・スマートフォン	—	上記システムの利用

第3条（安全管理体制）

1. 当社は、本ガイドラインの区分に従い、次のとおり責任者を置く。

区分	職名	主な役割
経営管理者	代表取締役	安全管理に関する最終責任、方針決定、必要な経営資源の配分
企画管理者	【管理者名】 坂本　翔太	規程の策定・運用、リスク評価、職員教育、事故発生時の指揮」
システム運用担当者	【担当者名】 坂本　翔太	機器・アカウント・ログの管理、技術的対策の実施、委託先との調整

2. 各責任者は、相互に連携し、少なくとも年1回、安全管理体制の運用状況を確認する。

3. 非常時の対応　災害、通信障害、サイバー攻撃、外部サービスの停止等により医療情報システムが利用できない場合においても、訪問看護および居宅介護支援の提供を継続できるよう、次の代替手段を定める。

停止したもの	代替手段
カイポケ・ミルナス	紙の記録用紙により記録し、復旧後に入力する。請求期限が迫る場合は国保連等に相談のうえ対応する

停止したもの	代替手段
MCS・Chatwork	電話および携帯電話のショートメッセージにより連絡する。連携機関の緊急連絡先一覧を事業所内に備え置く
Google Workspace／Google Cloud	事業所内に備え置く紙の様式および控えにより業務を継続する
オンライン資格確認等システム	被保険者証等の提示または利用者への聴取により確認する

4. 企画管理者は、前項の連絡先一覧および紙の様式を年1回以上更新し、職員等に周知する。

第4条（組織的安全管理措置）

1. 医療情報を取り扱う業務の範囲および担当者を明確にし、台帳等により管理する。
2. 医療情報の漏えい、滅失、毀損その他の事故またはそのおそれを認知した職員等は、直ちに企画管理者に報告する。企画管理者は経営管理者に報告のうえ、被害の拡大防止、原因調査、関係機関への報告および利用者への説明等、必要な対応を行う。
3. 事故の発生状況および対応内容は記録として保存し、再発防止策を検討する。

第5条（人的安全管理措置）

1. 職員等は、採用時および退職時に、業務上知り得た医療情報を正当な理由なく開示・漏えいしない旨の誓約書を提出する。この義務は退職後も継続する。
2. 当社は、職員等に対し、年1回以上、医療情報の取扱いおよび情報セキュリティに関する研修を実施し、実施記録を保存する。
3. 職員等は、離席時の画面ロック、私物端末への業務情報の保存禁止、業務用アカウントの共用禁止など、日常の取扱いルールを遵守する。
4. 訪問記録機能により職員の使用する端末の位置情報が取得されることを、あらかじめ職員等に説明する。

第6条（物理的安全管理措置）

1. 医療情報を記録した書類および電子媒体は、施錠可能な保管庫等に保管し、事業所外への持出しは業務上必要な範囲に限る。
2. 情報機器は、事業所内の管理された場所に設置し、第三者が容易に操作できない状態を保つ。
3. 覗き見のおそれがある場所で情報機器を使用する場合は、覗き見防止フィルターを使用する。

4. 医療情報を含む書類および電子媒体を廃棄する場合は、細断、溶解、データの復元不可能な消去等の方法により行う。
5. 外部サービスのサーバ設備に係る物理的安全管理は、当該サービス提供事業者およびそのクラウド基盤事業者の責任範囲とし、当社は第9条により当該対策の状況を確認する。

第7条（技術的安全管理措置）

1. 利用者認証　医療情報システムへのアクセスには、職員ごとに付与したIDおよびパスワード等による認証を必須とする。IDの共用および貸与は禁止する。
2. アクセス権限　職種および業務内容に応じて、必要最小限の範囲でアクセス権限を設定する。異動・退職時は速やかに権限を変更または削除する。
3. パスワードおよび多要素認証
    - パスワードは英数字を混在させ、十分な長さを確保し、他のサービスと同一のものを使用しない。
    - 多要素認証が利用可能なサービスについては、全職員がこれを設定することを必須とする。
    - 定期的なパスワード変更は一律には求めず、漏えいのおそれがある場合その他必要と認めるときに変更する。
    - システム運用担当者は、サービスごとの管理者機能により職員ごとの多要素認証の設定状況を年1回以上確認し、未設定者に設定させる。
4. ログの取扱い
    - アクセス記録を利用者側で確認できるサービスについては、必要に応じてその内容を確認する。
    - 利用者側でアクセスログを確認する機能を備えないサービスについては、当該事業者が記録を取得していることを第9条により確認したうえで利用し、不正利用が疑われる場合は当該事業者に調査を依頼する。この場合、調査が有償となることがあることを了解のうえ利用する。
    - 前号のサービスについては、ログに代わる管理手段として、第12条に定める参加者台帳および年1回以上の利用状況点検により、共有範囲の妥当性を確認する。
5. 不正プログラム対策　業務に用いる端末にウイルス対策ソフトを導入し、OSおよびソフトウェアを常に最新の状態に保つ。各サービスが指定する動作環境（対応OS、ブラウザ、PDF閲覧ソフト等）を満たし、いずれもサポート期間内の最新版を使用する。
6. 通信の安全性　医療情報を伝送する場合は、TLS1.2以上により暗号化された通信経路を用いる。公衆無線LANを用いた医療情報の送受信は行わない。
7. バックアップおよび保存性の確保
    - 外部サービスに登録した情報は、当該サービスの規約により一定期間の経過後に事業者の判断で削除されることがある。当社は、法令上保存を要する記録について、当社の責任においてバックアップを取得し、保存期間を満たすよう管理する。
    - 記録・請求システムに登録した情報については、年1回以上、必要な範囲を出力または複製して保管する。
    - 情報連携ツール上のやり取りのうち、看護・介護の提供に必要な事項は、第12条により記録システムへ転記することをもって保全する。

第8条（モバイル端末およびリモートアクセスの管理）

1. 訪問先で使用する端末は、当社が貸与または承認したものに限る。個人所有の情報機器を業務に用いる場合は、企画管理者の事前承認を要し、承認を受けた端末を台帳に登録する。
2. 利用する外部サービスに端末を技術的に制限する機能がない場合、前項の制限は運用によって担保するものとし、企画管理者は年1回以上、職員等が使用している端末の状況を確認する。
3. 貸与端末には、起動パスワードおよび画面ロックを設定する。
4. 端末上のアプリケーションに登録した情報の漏えいおよび不正利用について、サービス提供事業者が責任を負わない旨を定めている場合があることを踏まえ、端末およびアカウントの管理は当社の責任において厳格に行う。
5. 端末の紛失または盗難が発生した場合、発見者は直ちに企画管理者およびシステム運用担当者に連絡する。システム運用担当者は、直ちに当該職員のアカウントのパスワードを変更し、必要に応じてアカウントを無効化する。
6. 業務に必要のない端末への医療情報の保存および複製は行わない。

第9条（外部サービス・委託先の管理）

1. 外部サービスを利用する場合は、事前に次の資料により、本ガイドラインおよび「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」への適合状況を確認し、保存する。
    - サービス事業者による医療情報セキュリティ開示書（SDSチェックリスト）、対応表またはホワイトペーパー
    - 利用規約その他の責任分界を示す文書
    - データの保管場所に関する説明
2. 確認の結果、当該事業者が「医療機関等において判断・実施すべき事項」としている項目については、本規程および関連規程により当社の責任で措置を講じる。
3. 現に利用している外部サービスに関する確認結果は、次のとおりとする。

（1）カイポケ（株式会社エス・エム・エス）

確認事項	内容
適用される規約	カイポケ利用規約、エス・エム・エス経営支援サービス共通規約、個人情報の取扱いについて
登録情報の保存	登録日より5年経過後、会員の同意なしに削除されることがある。バックアップは会員（当社）の責任

確認事項	内容
ケア連携の送信情報	送信日より5年経過時等に削除されることがある。復旧について事業者は責任を負わない
送信情報の閲覧・開示	会員の同意、令状・行政機関の要求、法令上の義務、生命身体等の保護、緊急のメンテナンスの場合に事業者が閲覧・開示することがある
提供票等の送付	個人情報を保護する形で送付する場合は、当社側でセキュリティ設定を有効にして送付する必要がある
位置情報	訪問記録機能において、利用端末の位置情報が取得される
動作環境	サポート期間内のWindows OS、Google Chrome最新版、Adobe Acrobat Reader最新版
責任分界	タブレットアプリの内部情報の漏えい・不正利用について事業者は責任を負わない。ケア連携で会員間または会員と第三者間に生じたトラブルに事業者は関与しない
当社が補完する事項	定期的なバックアップ（第7条7）、送付時のセキュリティ設定（連携規程）、端末・アカウント管理（第8条）、位置情報取得の職員への説明（第5条4）

（2）ミルナス（株式会社オプティス）

確認事項	内容
適用される規約	ミルナス利用規約、プライバシーポリシー
利害関係	提供事業者の代表者は当社の代表者と同一である。適合状況の確認は、当社の代表者以外の者（企画管理者）が行い、確認記録を保存する
データの保存	法令等で定められた保存義務期間の範囲内で事業者のサーバー上に保管される。保存義務

確認事項	内容
	期間が経過したデータ、および事業者が保存の必要がないと判断したデータは削除される
バックアップ	事業者はバックアップの義務を負わない。契約期間中に当社の責任で必要なデータを出力・保存する
解約後の取扱い	解約日以降、当社はデータへのアクセス・閲覧・編集・出力ができなくなる。参照が必要な場合は再契約を要する
認証	事業者IDおよびユーザーIDによる認証。パスワードは初回ログイン後速やかに変更する（一定期間変更がない場合はアカウントが一時停止される）
事業者によるデータアクセス	ユーザーサポート、障害調査、動作確認その他の技術的対応の目的に限り、事業者の担当者が介護利用者等データにアクセスすることがある。事業者はアクセスの実施日時・担当者・対象範囲を記録し、一定期間保存する
生成AIの利用	書面案等作成機能において、登録した介護利用者等データおよびプロンプトが、Anthropic PBC（米国カリフォルニア州）の提供する生成AI APIにより処理されることがある。事業者は、提供元との契約により、安全管理措置、目的外利用の禁止、再提供の制限等について国内と概ね同水準の措置を義務付け、その履行状況を確認するとしている。提供されたデータはAIの性能向上を目的とした学習には利用されない
出力物の正確性	事業者は、生成された文案・書面の正確性、完全性、適法性を保証しない。診療報酬請求の適法性・正確性も保証しない
再委託	事業者は、サービスの提供に必要な業務を第三者に委託することができる
責任分界	ID等の管理不十分、使用上の過誤、第三者による使用に起因する損害は当社が負う。事業者の賠償責任は故意または重過失の場合に限ら

確認事項	内容
	れ、直前6か月間の利用料金の合計額を上限とする
当社が補完する事項	出力された文案・書面の内容確認および修正（第11条2項）、生成AIの利用に関する利用者への説明と同意取得、定期的なデータ出力・保管（第7条7）、ID・パスワードの管理（第7条1・3）

（3）メディカルケアステーション（日本エンブレース株式会社）

確認事項	内容
ガイドライン適合資料	MCS運用管理規程、安全管理に関する情報提供、SDSチェックリストを入手し保管
認証	ISO/IEC 27001、ISO/IEC 27017、プライバシーマーク
参加者の限定	招待または管理者の承認を経た者のみが参加できる非公開型
患者・家族との分離	医療介護側と患者側でタイムラインが分離されている
通信の暗号化	TLS1.2以上
データ保管場所	国内。国外への業務委託およびデータの移管・保管なし
当社が補完する事項	事業者が「施設のMCS運用管理規程として定める必要がある事項」として示す事項の規程化、利用者・職員の同意取得、コミュニティ機能への利用者情報の投稿禁止

（4）Chatwork（株式会社kubell／ビジネスプラン）

確認事項	内容
ガイドライン適合資料	SDSチェックリスト Ver.5.0（安全管理ガイドライン第6.0版対応）を入手し保管

確認事項	内容
データ保管場所	AWS東京リージョン。Amazon S3により3つのデータセンターに冗長化して保管
通信の暗号化	TLS1.2以上。「TLS暗号設定ガイドライン」の高セキュリティ型に準じた設定
認証	ID・パスワードに加え、ワンタイムパスワードアプリまたはショートメッセージによる多要素認証
アクセス管理	ルーム参加者と権限の設定により実施
利用者向けアクセスログ	機能なし。事業者側で取得しており、インシデント時に調査を依頼できる（有償の場合あり）
不正プログラム対策	実行可能なファイル形式はアップロード不可
責任分界	利用規約 第4条・第25条・第26条
当社が補完する事項	取扱情報リストの作成（第4条2）、端末の限定（第8条）、代替連絡手段の確保（第3条3）、参加者台帳と定期点検（連携規程）

（5）Google Workspace／Google Cloud（グーグル合同会社）

確認事項	内容
ガイドライン適合資料	事業者が公開する3省2ガイドライン対応ホワイトペーパーおよび提供事業者ガイドラインの統制マッピングを入手し保管
認証	ISO/IEC 27001、ISO/IEC 27017、ISO/IEC 27018
契約形態	業務での利用は、当社が契約する組織アカウントに限る。個人アカウントの業務利用は禁止する
アクセス管理	組織の管理コンソールにより、アカウント、共有設定および外部共有の可否を管理する
当社が補完する事項	共有リンクの範囲設定、外部共有の制限、2段階認証プロセスの必須化、退職者アカウントの

確認事項	内容
	停止、内製ツールにおける個人情報の取扱範囲の限定

4. 医療情報の取扱いを外部に委託する場合は、契約書等において、安全管理措置の内容、責任分界、再委託の可否、事故発生時の報告義務を明確に定める。
5. 委託先およびサービス提供事業者の一覧を整備し、確認資料とあわせて管理する。

第10条（オンライン資格確認等システムの取扱い）

1. オンライン資格確認等システムにより取得した利用者の診療情報、薬剤情報および特定健診等情報は、訪問看護の実施に関する計画的な管理の目的に限り利用する。
2. 情報の取得にあたっては、利用者の同意を得たうえで行い、取得の事実を記録に残す。
3. 当該システムに接続する端末およびネットワークについては、第7条および第8条の措置を適用する。

第11条（生成AIを用いる機能の取扱い）

1. 医療情報システムの機能として生成AIを用いる場合は、当該機能により作成された文案および書面が、事実と異なる内容を含む可能性があることを前提として取り扱う。
2. 職員等は、生成AIにより作成された文案および書面について、記録および提出の前に必ず内容を確認し、必要な修正・補足を行う。確認を経ないまま利用者に交付し、または関係機関に提出してはならない。
3. 生成AIの処理にあたり利用者の情報が外国にある事業者に送信されることがある場合は、あらかじめ利用者本人または家族にその旨を説明し、同意を得る。説明の内容および同意の取得は記録に残す。
4. 生成AIの機能に入力する情報は、業務上必要な範囲に限る。

第12条（多職種連携における情報共有）

ICTを用いて関係機関と利用者の情報を共有する場合の取扱いは、別に定める「ICT連携ツール利用に関する取扱規程」による。

第13条（点検および見直し）

1. 企画管理者は、年1回以上、本規程の遵守状況を点検し、結果を経営管理者に報告する。点検には、次の事項を含める。
    - 職員ごとの多要素認証の設定状況
    - 端末の登録状況
    - 各サービスの参加者台帳・アカウント一覧と実際の利用者の突合
    - 記録のバックアップ取得状況

- 外部サービスの適合状況資料の更新有無

2. 経営管理者は、点検の結果、法令・ガイドラインの改正、システム構成の変更、事故の発生等を踏まえ、必要に応じて本規程を見直す。

第14条（違反時の措置）

本規程に違反した職員等に対しては、就業規則の定めるところにより処分を行うことがある。

制定日　令和　8年　6月　1日

株式会社Warm relationship 代表取締役　坂本　翔太