【 yui 合同会社　情報セキュリティ安全管理規定 】

① 情報セキュリティ安全管理規定の目的

この安全管理規定（以下、「本規定」という。）は、yui 合同会社（以下、「当法人」という）が提供するサービスで取り扱う個人情報を含む医療情報を安全に管理し、漏えい、き損、改ざん等の物理的、技術的、人的被害から守り、その機密性、完全性、可用性を確保し、当法人が提供するサービスの効率性及び信頼性を確立し、かつ、維持することを目的とする。

② 安全管理の基本事項

２−１　組織の体制。

（１）安全管理責任者
社長が安全管理責任者となり、安全管理に対する施策、権限を有する。

（２）運用担当者
サービスの保守・運用作業を行う運用担当者は、安全管理責任者および安全管理責任者が任命した従業員のみとする。

提供するサービス、医療情報システムの安全管理ににかかわる苦情・質問の受付窓口は当法人が電話およびメールにて対応する

２−２　適用範囲および管理対象

本規定の人的適用範囲は、役員、正職員、契約社員、派遣職員、パート･アルバイトを含む全ての従業者及び、委託契約を行っている委託先において、委託業務に携わる全ての従業者を範囲とする。

本規定は、当法人が提供するサービスを構成するすべての機器を管理対象とする。

本規定によらず、サービスを安全に運用管理するために必要な機器類を管理する場合は、本規定を遵守するものとする。

③ 物理的安全管理措置

３−１　医療情報処理システムを設置する建物

サービスで提供される医療情報処理システムおよび情報を保存するサーバーを設置する場所（以後、「管理施設」という。）は、当法人の専有する建物、あるいは当法人が全体を専有するフロア、あるいは十分に安全性が確保された外部事業者のデータセンター内に設置された医療情報処理システム専用のサーバラックとすること。

外部事業者のデータセンターを利用する場合には、医療情報処理システムを構成する全ての機器を十分な強度を持った専用のラックに納め、同じデータセンターを利用する他事業者からの不正なアクセスに対する保護対策を施すこと。

部屋を区切る壁面、天井、床部分においては、傍受、盗撮等の不正な行為を防止するため

の十分な厚みがあり、部屋に対する物理的な不正侵入を抑止できる環境が整備されていること。

３−２　管理施設の入退室管理

安全管理責任者より許可を受けた要員以外の管理施設入室を禁ずる。

管理施設内への個人的所有物の持ち込みは禁止する。

３−３　医療情報処理システムのセキュリティ

医療情報処理システムを構成する装置は、製造元又は供給元が指定する間隔及び仕様に従って保守点検を行うこと。

火災発生時の消火設備が医療情報処理装置に損傷を与えないよう配慮すること。また、機器を設置するサーバラックは、震災時に転倒することが無いよう確実に設置するとともに、十分な換気・空調を施すこと。

保守点検で障害不良等が発見された際は、当法人が管理する領域で対応作業を行うこととし、外部に持ち出すことが無いようにすること。ただし、必要により外部に持ち出しての作業が必要な場合には、装置内の電磁的記録を確実に消去した場合に限り持出しを許可するが、記憶装置等、障害により情報の消去が不可能となっている装置については補修ではなく物理的に破壊し廃棄すること。

医療情報処理システムにつながる端末は、離席時には画面の電源を切るか、パスワード付きスクリーンセーバを設定すること。

３−４　情報・機器・媒体の廃棄や再利用

個人情報（不要になった個人情報を含む）及び機密情報が格納された機器等を廃棄する場合は、安全管理責任者または安全管理責任者が選任した者が以下の方法で廃棄し、廃棄した記録を残しておくこと。

サーバ・PC 等を廃棄する場合、ハードディスクは確実な方法でデータを完全消去するか、物理的に破壊し廃棄すること

CD、USB 等の外部媒体は、物理的に破壊し、廃棄すること。

紙媒体は、シュレッダーで裁断し廃棄すること。

上記いずれにおいても、外部の事業者に廃棄を委託する場合には、廃棄方法を確認するとともに、確実に廃棄したことを証する証明等の証跡を取得すること。

３−５　医療情報処理システムを構成する装置及び事務所内機器の外部への持ち出し

医療情報処理システムを構成する装置は、装置内の電磁的記録を確実に消去した場合に限り持出しを許可するが、記憶装置等、障害により情報の消去が不可能となっている装置については補修ではなく物理的に破壊し廃棄すること。

事務所内機器は、持ち出しが許可されている機器以外の持ち出しは原則禁止とする。ただし、やむを得ず許可のない機器を持ち出す場合は、個人情報が格納されていないか、格納されていればＰＷの設定等安全確認を行った上、安全管理責任者の許可を得ること。

３−６　契約書等の文書

提供するサービスの内容等を規定した契約書等の文書は事務所内に施錠の上保管する

④　技術的安全管理措置

４−１　医療情報処理システムを構成する装置およびソフトウェアの保守・改修

保守・改修に伴うHomeClinicを構成する装置及びソフトウェアの変更がもたらす影響を考慮し、影響を最小限に抑える方策を検討すること。

医療情報処理システムを構成する装置及びソフトウェアの保守・改修作業については、業務の停止時間を最小限に留めるように計画を立てるとともに、必要な関係者への周知を行い、変更に伴う影響の監視を行うこと。

医療情報処理システムを構成する装置及びソフトウェアの保守・改修作業については、作業終了後に動作確認で使用した個人情報を含むデータを消去すること。

潜在的な技術的脆弱性が特定された場合には、リスク分析を行った上で必要な処置（パッチ適用、設定変更等）を決定すること。

メーカー等から提供されるセキュリティパッチは、原則自動適用とする。なお、サーバ等は、パッチを適用することによるアプリケーション等への不具合がない事を確認した上で適用するものとする。

保守・改修作業を外部事業者に委託する場合には、上記要件を満たしていることを確認すること。

保守・改修を行った際には、作業の妥当性を検証し内容を安全管理責任者に報告すること。

医療情報処理システムにかかわる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。

４−２　悪意あるコードからの保護

最新の脅威についての情報収集に努め、導入している悪意のあるコード対策ソフトウェアの対応範囲を確認し、対策漏れが無いことを確認すること。脅威の例としては、コンピュータウイルス（ワーム）、バックドア（トロイの木馬）、スパイウェア（キーロガー）、ボットプログラム（ダウンローダー）等がある。

悪意のあるコード対策ソフトウェアでは、リアルタイムスキャン（ディスク書き出し・読み込み）、定期的な自動スキャン、外部記憶媒体へのデータ書き出し・読み込み時におけるオンデマンドスキャンを設定すること。

４−３　外部事業者が提供するサービス

外部事業者により提供されるサービスを特定し、サービスレベルを確認するとともに、サービスの実施、運用、維持について定期的に検証すること。

サービス実施について事前、事後報告を義務づけ、報告内容を点検確認すること。

サービスを実施する人員は予め届け出を受けサービス実施時に確認するとともに、原則、職員が監督している状況で作業を実施すること。

サービス実施にともなう処理施設内への立ち入り手順に関しては、職員の入室、退室手順に準ずること。

４-３　ネットワークの管理

セキュリティゲートウェイ（ネットワーク境界に設置したファイアウォール、ルータ）では、接続先の限定、接続時間の限定等のアクセス制御を行うこと。

医療機関等との接続ネットワーク境界には侵入検知システム（IDS）及び侵入防止システム（IPS）などを導入し、ネットワーク上の不正なイベントの検出、あるいは不正なトラフィックの遮断を行うこと。

侵入検知システムが、緊急度の高い攻撃・不正アクセス行為を検知した際は、監視端末への出力や電子メール等を用いて直ちに管理者に通知する設定にしていること。

ネットワーク経由で直接、特権ユーザとしてログオンする行為を禁止すること。

VPN 接続を含むネットワーク接続のログ（認証ログ及び接続ログ）を記録し、毎月定期的に点検すること。なお、不正なアクセスの兆候を検出した場合は、システム管理者に通知するとともに、実態を把握するとともに、必要に応じ是正・予防処置を講じること。

無線 LAN の使用は原則禁止する。なお、業務上使用せざるを得ない場合は、安全管理責任者の承認を得た後にWPA2-AES 以上の暗号化を行った上で利用する。

４-４　媒体の取扱い

医療情報処理システムのデータを記録した可搬型の記憶媒体は、安全管理責任者の許可を受けない限りは持ち出してはならない。

情報交換、情報保管以外の目的で記憶媒体を用いないこと。またその場合、媒体内のデータにパスワードによるアクセス制限又は暗号化を施すこと。

媒体は、施錠可能なキャビネット等で保管するとともに、一覧表を作成し、所在管理を行うこと。なお、未使用の媒体は安全管理責任者が保管し、払い出し等を管理すること。

媒体を配送する際は、配送物と宛先に間違いがないかを十分確認した上で配送すること。

配送業者から媒体を受け取る時は、正規職員が直接受け取ること。

CD、DVD 等の光学メディア、MT（磁気テープ）等の媒体を廃棄する場合には、物理的に破壊し（高温による融解、裁断等）廃棄する。なお、媒体の破壊は当法人自身で行うが、破壊した媒体の処理は外部の専門事業者に依頼することが可能である。

ハードディスク等の固定記憶装置の扱いについては第９条（廃棄・再利用）に従う。

４-５　配送時のセキュリティ

物理的に情報を搬送する場合には、以下の対策を実施すること。
(1) 予め評価選定された配送業者に依頼し、配送伝票を 1 ヵ月以上保管する。
(2) 配送時の作業者については、発送元、受領先の双方で身分確認を行い第三者によるなりすましを防ぐこと
(3) 交換する記憶媒体の数と種類について、予め情報交換して受領時に欠損が無いことを

確認すること
(4) 不正な開封を検出することのできるコンテナ等を利用すること
（ただし、以下の対策を実施する事が困難な場合は、別の安全対策方法を示し安全管理責任者の許可が得られた場合は上記以外の方法で搬送する事ができる。）

電子的に情報を転送する際には以下の対策を実施すること。
(1) ファイル転送等による送受信を行う際は、送信者、受信者は相互に電子的に認証を行い相手の正当性を検証すること。
(2) 送受信する経路は適切な方法（VPN、SSL 等）で傍受のリスクから保護されていること。
(3) 送受信に失敗する時には、三回を上限として再送受信を試み、上限に達した際には送受信者間の全ての通信を停止し、障害の特定等の作業を実施すること。
(4) 電子メールに添付する場合は、必ず暗号化し、復号のためのパスワードは送信メールとは別の手段で確実に相手先に伝えること。

４-６　医療情報処理システムに対するセキュリティ

開発用コード又はコンパイラ等の開発ツール類および作業者個人のファイル、情報処理に不必要なファイル等は、運用システム上に置いてはならない。

業務に供するソフトウェア及びオペレーティングシステムソフトウェアについて、十分な試験を行った上で導入すること

運用システムに関わるライブラリプログラムの更新については監査に必要なログを取得すること。

システム運用情報（システム及びサービス設定ファイル等）の複製及び利用については監査証跡とするためにログを取得すること。

４-７　アクセスログの管理

サーバーへのアクセス状況等についてログを記録し、不正な行為・システム異常等の有無について毎月安全管理者が点検する。

４－８　バックアップ

バックアップを取得するサーバ等を特定し、原則、毎日バックアップし 3 世代以上の世代管理を行う。

バックアップ媒体は、アクセスが制限された室・キャビネット等で確実に保管する。

４－９　アクセス制御

情報処理に用いる情報処理機器、ソフトウェアおよびデータに関するアクセスポリシーを定め、アクセス権限者を明確にすること。

アクセス権限は、安全管理責任者に申請し、それに基づき適切にアクセス権限を付与し、その状況を記録すること。

アクセス権限者を定める際は、業務内容等を考慮し、作業者を最小限にするとともに、必要最小限の権限とするよう考慮すること。

作業者に与えられた権限外の情報や権限外の操作画面を表示しないよう権限管理を行うことが望ましい。

４－１０　ID の管理

作業者にはユニークな ID を付与し、ID の共有は原則不可とする。

やむを得ない理由で共有 ID を使用する場合は、同 ID を使ったものが特定できるよう別途作業日誌等により作業開始日時・終了日時等を記録すること。

作業者が変更もしくは退職した際には、直ちに当該 ID を利用停止すること。

不要な ID やアカウントが残っていないことを毎月定期的に確認すること。

情報処理装置及びソフトウェアを使用する前に、製造ベンダが設定したデフォルトのアカウント及びメンテナンス用のアカウント等、必要のないアカウントについては削除あるいはパスワード変更を行うこと。

４－１１　パスワードの管理

安全管理責任者および運用担当者が設定した初期パスワードは、使用する前に変更すること。

過去に利用したパスワードは再利用せず、付箋・張り紙等に記録し張り付けるなどをしてはならない。

類推しやすいパスワードの使用や類似のパスワードを繰り返し使用しないこと。

⑤ 人的安全管理措置

５－１　要員の管理

医療情報を操作する可能性のある要員の全てについて、雇用契約時あるいは医療情報を扱う職務に着任する際の条件として秘密保持契約あるいは守秘義務契約への署名を求めること。

派遣従業員については機密保持義務及び継続的な情報セキュリティ教育を課すことを条件に選定、派遣することを求めること。

医療情報を操作する可能性のある要員の全てに情報セキュリティに関する教育を行い、一定水準の理解を得たものだけを選定すること。派遣従業員に関しては、派遣元に対し、情報セキュリティに関する一定水準の知識、理解を持つ、あるいは持つことができる人員を選定、派遣することを求め、受入れ後に正規職員同等の教育を行うこと。

医療情報を操作する要員が退職する際には、貸与された情報資産の全てについて返却し、返却が完全であることを確認するための台帳及び返却確認手続きを予め規定しておくこと。

業務上知りえた医療情報について退職後も秘密として管理することを記した合意書への署名を求めること。派遣従業員については、派遣契約解除時に同等の合意書への署名を求めること。

⑥　情報セキュリティインシデント

６－１　情報セキュリティインシデントへの対応と再発防止

情報セキュリティインシデントが発生した場合、被害の拡大を防ぐとともに、情報セキュリティインシデントから復旧するための体制を整備する。

情報セキュリティインシデントが発生した際の対応手順を整備する。

情報セキュリティインシデントに備え、サービス提供のための緊急連絡先、連絡手段、連絡内容を含む緊急連絡網を整備する。

必要に応じ、情報セキュリティインシデントについて社外から報告を受けるための窓口を設置する。

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場合や、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された場合には、所管官庁への連絡等必要な対応を行うほか、そのための体制を整備すること。

情報セキュリティインシデントが発生した場合には、インシデントの原因を調査し再発防止策を策定する。

安全管理責任者は、運用担当者から情報セキュリティインシデントについての報告を受けた場合には、その内容を検討し、再発防止策を実施するために必要な措置を講ずる。

附則
この規程は、令和６年６月１日から施行する。