資料１

広島県救急搬送支援システムの利用規定について

令和７年12月２日

広島県健康福祉局健康危機管理課

1．国が示すガイドライン上の要件

広島県救急搬送支援システム（救急隊が入力する傷病者情報などの医療情報を医療機関職員が閲覧するクラウドサービス）の運用・利用にあたっては、国が定めるセキュリティガイドライン、

・医療情報システムの安全管理に関するガイドライン
・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

を満たすことが求められる。

シフトにより入れ替わる複数のスタッフが院内の複数の場所においてシステムにアクセスすることから、
ガイドラインで示される以下の要件を踏まえ利用規定を整理する（３頁参照）。

【ガイドライン上の要件】

○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（掲載先：厚生労働省ホームページ）
- 「多要素認証」の採用を強く推奨（特にクラウドサービスや院外アクセス時）。
- 個人単位での識別とアクセスログ管理が必須。
- 利用者が頻繁に入れ替わる医療現場を想定した場合でも、「誰が」「いつ」アクセスしたかを追跡できることが条件。

○医療情報を取り扱う情報システム・サービス提供事業者における安全管理ガイドライン第2.0版（掲載先：経済産業省ホームページ）
- ID管理の適正化（入退職・異動に伴う速やかなアカウント廃止・変更）。
- 認証情報の複雑性・使い回し防止。
- 端末やネットワークの制御（証明書※1やVPN※2など）を組み合わせること。

※1　端末固有の識別番号を通して端末管理が可能。証明書が登録された端末からのみクラウドサービスへのアクセスを許可できる。
※2　不特定事業者が接続されるネットワーク上に構築された、特定の事業者間のみを接続する仮想的な閉域網のこと。

2．広島県救急搬送支援システムの利用規定について

○救急搬送支援システムを利用する端末については、県が貸与する端末のほか、**運用上必要な端末の台数に貸与台数が満たない場合は、医療機関が別途調達・用意する端末での利用を許容する。**

○医療機関が別途調達・用意する端末については、**医療機関がIT資産管理台帳等において適切に管理する端末（個人が所有する端末ではなく、医療機関が所有し管理責任を負う端末）とする。**

○医療機関は、システムを利用する端末の機種、配置場所、配置理由、利用方法、主な利用者及び利用者の特定方法について、県及び県委託事業者（TXP Medical株式会社）に届けることとする（届出方法は、指定のWebフォーム若しくはExcel様式（今後変更の可能性有））。

○システムの利用にあたっては、**端末にパスコードロック（６文字以上）を設定し、システムへの二要素認証※3によるログイン※4及び利用者の特定を必要とする。**

・二要素認証

Authenticator（2段階認証用のワンタイムパスワードを生成するアプリケーション）をシステム利用端末にインストールし、**「ID・パスワード（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）＋2段階認証用のワンタイムパスワード」でログインを行う。**

※3　認証の３要素である「知識情報（ID、パスワード等）」、「所有情報（スマートフォン、ICカード等）」、「生体情報（指紋・顔認証等）」のうち、2つの独立した要素を組み合わせて認証を行う方式。Authenticatorによるワンタイムパスワードを送信して認証を行う方法は所有情報に含まれる。

※4　令和７年度においては、救急医療情報連携プラットフォームにのみ適用とし、民間救急システム（NSER mobile）については、国のガイドラインに基づき今後整理を行う。

・利用者の特定

指定された者以外の者の入室が制限されるような区画（当該区画への入場に当たって利用者の識別・認証が適切に実施されている）の中に端末が設置されている、または、MDM※5管理下にあり画面パスコードロックが定期的にかかる設定などにより操作可能な人が限られる端末において、シフトやログの記録等から一定の範囲内で利用者が特定できることとする。

※5　情報端末のシステム設定等を統合的・効率的に管理する手法。利用できる機能、導入できるソフトウェアやデータに制限を加えたり、紛失時に遠隔制御によってデータの消去や操作のロックが可能。

【指定された者以外の者の入室が制限されるような区画】

- 医事課や当直室等の閉鎖空間や、カウンター等で物理的に仕切られた空間（スタッフステーションや受付などの事務スペース等）
- 職員以外が自由に立ち入ることが出来ない空間（救急外来の処置室等）など

【利用者の特定】

- シフトや業務日誌、電子カルテ記録、システムへのアクセスログ記録、上記区画に設置された監視カメラなどにより利用者の特定が可能
- 利用にあたり個人を特定する認証を別途設けている　など