

付録 (参考) 外部機関と医療情報等を連携する場合に取り決めるべき内容

外部の機関と医療情報共有の連携等を行う場合に、連携する機関の間で取り決めるべき内容の参考として以下に記載する。

1. 組織的規約
 - 理念、目的
 - 管理と運営者の一覧、各役割と責任
 - 遵守すべき法令・ガイドライン等の確認
 - 医療機関等と情報処理事業者・クラウドサービス事業者・電気通信事業者等との責任分界点
 - セキュリティ事故・大規模災害等が発生した際の報告体制・内容
 - 免責事項、知的財産権に関する規程
 - 参加機関間の規約（参加機関の資格タイプ、参加機関の状況を管理する規約）、費用負担等に係る取決め等 等

2. 運用規則
 - 管理組織構成、日常的運営レベルでの管理方法
 - システム停止の管理（予定されたダウンタイムの通知方法、予定外のシステムダウンの原因と解決の通知等）、データ維持、保存、バックアップ、不具合の回復等

3. プライバシー管理
 - 患者共通ID（もし、あるならば）の管理方法
 - 患者情報等のアクセスと利用の一般則
 - 利用者とアクセス権限のある医療情報別の対応規約
 - 患者同意のルール
 - 非常時のガイド（ブレイクグラス（非常時のID等の運用）、システム停止時、等の条件） 等

4. システム構造
 - 全体構造、システム機能を構成する要素、制約事項、採用する標準等
 - 連携組織外部との接続性（連携外部の組織とデータ交換方法） 等

5. 技術的セキュリティ
 - リスク分析
 - 認証、利用者管理、利用者識別（パスワード規約、二要素認証等の識別方法）

可搬媒体のセキュリティ要件 等

6. 構成管理

ネットワーク構成、ハードウェアやソフトウェアの機能更新・構成変更等の管理方法、新機能要素の追加承認方法 等

7. 監査

監査者、監査頻度、監査結果を踏まえた対応

8. 規約の更新周期