対象となるシステムの要件

公募にあたっては、以下の要件を満たすことを確認するための資料の提出を求める。
※項目末尾の括弧内は、「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版システム運用編の参照先

1　機能に関する事項

① 厚労省が示すケアプランデータ連携標準仕様に準じて出力されたCSVファイルを、標準仕様で示すファイルの組み合わせで送受信することが可能であること
② （公社）国民健康保険中央会の「ケアプランデータ連携システム」と接続するAPIの開発に協力するとともに、データ連携が可能になった段階で連携することを宣誓すること

2　安全管理措置に関する事項

① 保守時の安全管理対策として、作業計画書の作成・管理等により、保守要員等による情報流出・漏洩や保守作業中におけるデータ破壊・障害の対策が実施されていること（10.1 保守時の安全管理対策）
② データを保存するサーバルーム等において、入退室管理、防犯カメラや自動新入監視装置等が設置され、データの物理的な盗難防止策が講じられていること（12.1 サーバルーム等の物理的要件）
③ 非常時に利用できるようにバックアップデータが適切に管理されていること（12.2 バックアップの管理 ）
④ オープンでないネットワーク、又はTLS クライアント認証（TLS1.3以上（ただし、事業所の環境等やむを得ない場合はTLS1.2以上）を利用していること。ただし、TLS1.2を利用する場合は、「TLS 暗号設定ガイドライン 3.0.1 版」に規定される「高セキュリティ型」に準じた適切な設定を行われていること。（13.ネットワークに関する安全管理措置）
⑤ サーバのストレージ、及びデータベースに保存されているデータについても全て暗号化して保存する等、保存される個人識別に係る情報の暗号化を行い適切に管理すること（13.3.2 情報に対する暗号化 ）
⑥ 信頼された証明書発行機関が発行した証明書を使ってネットワーク上の伝送データを全て暗号化していること（13.3.3 盗聴防止等）
⑦ 二要素認証を採用していること（14.1.1 利用者の識別・認証 ）
⑧ WEBアプリケーションの脆弱性を利用した攻撃を防ぐ為のWAF（Web ApplicationFirewall）を実装していること（18.1 サイバーセキュリティ対応）

（参考）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 システム運用編において連携先システムに求める安全管理措置

１．情報セキュリティの基本的な考え方
２．システム設計・運用に必要な規程類と文書体系
３．責任分界
４．リスクアセスメントを踏まえた安全管理対策の設計
５．システム設計の見直し（標準化対応、新規技術導入のための評価等）
６．安全管理を実現するための技術的対策の体系
７．情報管理（管理・持出し・破棄等）
８．利用機器・サービスに対する安全管理措置
９．ソフトウェア・サービスに対する要求事項
１０．医療情報システム・サービス事業者による保守対応等に対する安全管理措置
１１．システム運用管理（通常時・非常時等）
１２．物理的安全管理措置
１３．ネットワークに関する安全管理措置
１４．認証・認可に関する安全管理措置
１５．電子署名、タイムスタンプ
１６．紙媒体等で作成した医療情報の電子化
１７．証跡のレビュー・システム監査
１８．外部からの攻撃に対する安全管理措置

※ガイドラインから、連携するにあたり最低限必要な項目を抜粋（運用上の対応や、利用する事業者の責務等は除いた）