1.「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」に関する取り組み

(1) 基本的な考え方

HASTOS / POST.exサービスは、健診標準フォーマットの CSVファイルに変換することを目的とするサービスであり、健診機関・医療機関等から送信された健康情報・医療情報を保存（外部保存）並びに管理することはありません。
HASTOSサーバ（HASTOS / POST.exサービスを運用するための物理サーバ）では、健診機関・医療機関等から送信された全ての情報はバイナリファイルとして扱っており、ファイル内の情報の読み取りやデータベース化等は行っていません。また、ファイルは暗号化して扱うことを基本とし、必要とする場合に限って一時的に復号することとしていますので、オペレータ（システム管理者・操作者）がファイル内の個人データを覗き見ることができない仕組みになっています。
健診標準フォーマットの CSVファイルへの変換作業は完全に自動化しており、オペレータは介在しません。また、ファイルは変換等処理の終了後に自動的に削除し、削除した記録をデータベースに保存します。ファイルを操作した記録はプライベート型ブロックチェーンに格納し、健診機関・健診実施主体の双方から閲覧できる仕組みとなっています。

---

(2) 取り組み

医療機関等が医療情報安全管理ガイドラインに基づき「外部保存を受託する事業者の選定基準」として少なくとも確認する必要がある項目

HASTOS / POST.exサービスは、医療機関等から送信された健康情報・医療情報を外部保存するサービスではありません。

1）保存された情報を格納する情報機器等が、国内法の適用を受けることを確認すること

HASTOS / POST.exサービスは、日本医師会総合政策研究機構が契約する国内データセンター内に設置した物理サーバを使って運用しています。
セキュリティ上の理由から、物理サーバの設置場所は公開できません。

2）医療情報等の安全管理に係る基本方針・取扱規程等の整備状況
3）不正ソフトウェア等のサイバー攻撃による被害を防止するために必要なバックアップの取得及び管理の状況
4）医療情報等の安全管理に係る実施体制の整備状況

HASTOS / POST.exサービスは、厚生労働省の「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（令和5年5月）」を参照して開発・構築しており、ガイドラインに準拠して運用しています。

5）実績等に基づく個人データ安全管理に関する信用度

HASTOS / POST.exサービスは正式運用開始前ですので、実績等はありません。

6）財務諸表等に基づく経営の健全性

HASTOS / POST.exサービスは、日本医師会総合政策研究機構が設置する健診標準フォーマット管理事務局（以下、事務局）が運用します。

7）プライバシーマーク認定又はISMS認証を取得していること

HASTOS / POST.exサービスの保守・運用は、事務局から株式会社アルファインターナショナルに委託しています。株式会社アルファインターナショナルは、プライバシーマーク認定とISMS認証を取得しています。

プライバシーマーク認定とISMS認証を取得している事業者が運用することから、政府情報システムのためのセキュリティ評価制度（ISMAP）のサービスリストにあるクラウドサービスを利用していません。

医療機関等との共通理解を形成するために情報提供すべき項目

1）医療機関等との役割分担の明確化

HASTOS / POST.exサービスは、ファイルを単位とする変換処理・送受信処理が基本であり、その処理プロセスを完全自動化しています。
サービスを利用する医療機関等は、個人データを扱うことになるため、厚生労働省の「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（令和5年5月）」への準拠が必要になります。
医療機関等にて３省２ガイドラインに準拠した運用規定を定めて、経済産業省の「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」に例示されているとおり、HASTOS / POST.exサービスの利用者（操作者）へのセキュリティ教育等を実施すること、事務局が求めた場合に、医療機関等が運用規定を事務局に提示することを要請します。

2）医療情報システム等の安全管理に係る評価
3）リスクアセスメントの成果物
4）リスク対応の成果物
5）運用管理規程に含める事項
6）制度上の要求事項への対応の成果物

HASTOS / POST.exサービスは、医療機関等から送信された健康情報・医療情報を外部保存するサービスではありません。
HASTOS / POST.exサービスは、厚生労働省の「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（令和5年5月）」を参照して開発・構築しており、ガイドラインに準拠して運用しています。

HASTOSサーバにて健診標準フォーマットに変換したファイルは、ファイルを受信する機関（HASTOSの場合は健診実施主体、POST.ex Onlineの場合は医療機関等）が「受信完了」操作をするまで、暗号化したうえでデータベース内に一時的に格納しています。リスク低減のため、送受信ファイルを受信することなく長期間滞留することがないように業務運用していただくよう要請します。