評価区分：

「民間事業者による医療情報の外部保存及びASP・SaaSサービス」に対する評価について

2012年12月

一般社団法人　保健医療福祉情報安全管理適合性評価協会

１．概要

医療機関等が厚生労働省の発行した「医療情報システムの安全管理に関するガイドライン」に基づいて医療情報システムを構築する場合に民間事業者のサービスを利用して構築することがある。その際に医療機関等は民間事業者が提供するサービスが経済産業省の発行した「医療情報を受託管理する情報処理事業者向けガイドライン」あるいは総務省が発行した「ASP・SaaS 事業者が医療情報を取り扱う際の安全管理に関するガイドライン」に適合したサービスを採用する必要がある。

本評価区分の適合性評価はその際の参考とする為に医療機関等の立場で各ガイドラインへの適合性を評価するものである。本評価は次章に示す詳細区分を参考に評価項目を選択する。

２．詳細区分

Ａ：ファイル転送型サービス

処理は行わず、送信されたデータ保存のみを行う。

データに対する検索・加工処理・変換処理などのアプリケーション機能提供サービスがあれば、Bの「アプリケーション処理外部保存型サービス」とする。

Ｂ：アプリケーション処理外部保存型サービス

利用者から送信されたデータをASP・SaaS で処理を行うほか、送信されたデータ保存も行う。

提供サービスに「外部保存」を謳っていなくても、ASP・SaaS 事業者が自らの意思で「ある期間、データを保管する」場合は、本項に該当する。

Ｃ：トランザクション型サービス

利用者から送信されたデータをASP・SaaS で処理を行い、送信されたデータの保存は行わない。

３．評価の視点

１）協会は利用者代わって評価する立場
利用者に開示する情報が評価対象になる。

２）ISMS 又はP マークの第三者認証を取得が条件
当協会の確認は、ガイドラインの要求事項に対する対策内容と申請者内部の審査者が何をもって確認したか、適切なエビデンスであるかの確認。
対策内容の実施の現場確認自体の責任は申請者内の審査者側にあるとの整理。

３）医療機関とのSLA やサービス契約書事項の雛型文書が評価対象
「責任分界点の説明」と「利用者へのセキュリティ遵守事項説明」の利用者へ提供。
代理店を通す場合には誰が責任を持って行うのかの規定化が必須。

４）評価は原則書類審査
エビデンスの実在性が疑われる場合、あるいは審査者の審査の実行性が確認出来ない場合は立入調査もありえる。また、2 年後の更新評価でサービス利用者としての医療機関等の利用環境等への立ち入り、その実効性を評価する場合がある。

５）「HISPRO 評価」の標榜表現の評価
評価申請者であるサービス提供者が「HISPRO 評価」を標榜するならば、その文章を申請時添付する。HISPRO による評価範囲と齟齬がないか、記載が明確であることを評価する。

４．評価手順

１）評価申請書提出
２）チェックリストの申請者提示
３）評価対象範囲の打合せ、適用チェックリスト項目の選別
４）評価範囲の了解
５）見積もり
６）契約、手付金支払い(試行期間中は後払い可)
７）業務計画・評価者のアサイン
８）申請者によるチェックリスト記入
９）評価業務（問答集による評価内容確認）
10）評価の判定
11）結果の通知
12）残金(有れば)支払い
13）評価結果の公表

５．提出書類

１）評価申請書

２）サービス概要説明書

３）評価対象範囲説明書

４）記入済みチェックリスト

５）チェックリストでエビデンスとした書類

６）責任分界点の説明書

７）利用者へのセキュリティ遵守事項説明書

８）適合性していると評価された場合「HISPRO 評価」によりガイドライン適合性を標榜する場合の文章（HISPRO による評価範囲との齟齬がないことを確認する為）

以　上