評価区分：

民間事業者による医療情報に係るクラウドサービスの評価

1. 概要

医療機関等において医療情報等を電子的に扱う際には、医療としての責任を果たすために適切に管理する必要があり、善管注意義務を果たすためのガイドラインとして厚生労働省「医療情報システムの安全管理に関するガイドライン」が発出されている。

医療情報を電子的に外部に保存することについては、いわゆる「外部保存改正通知」での文書等を対象として保存可能としている。対象文書以外の情報についても IT サービスが発展してきた昨今では外部保存ないし外部のサービスを利用して、患者の診療等にあたっている事例が増加してきている。善管注意義務を果たす意味では、「医療情報システムの安全管理に関するガイドライン」に従い管理することが適切であると考えられる。

「医療情報システムの安全管理に関するガイドライン」の「第 8 章 診療録及び診療諸記録を外部に保存する際の基準」では、医療機関等が民間事業者等との契約に基づいて確保した安全な場所に保存する場合、“サービス形態によって、経済産業省の定めた「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」や総務省が定めた「ASP・SaaS における情報セキュリティ対策ガイドライン」及び「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」の要求事項も満たす必要がある。”とされている。これらの整備を前提に「外部保存改定通知」が発出されることを踏まえると、医療機関等において、これらのガイドライン(通称、3 省 4 ガイドライン)を遵守の上、IT サービスを検討・利用することが必要である。

その中で、今般、総務省が定めた「ASP・SaaS における情報セキュリティ対策ガイドライン」及び「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」について、クラウドサービスの利用の普及状況、技術の進展にも鑑み、改定が行われ、「クラウドサービス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（第 1 版)」となった。

保健医療福祉情報安全管理適合性評価協会(HISPRO)では、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を行ってきたところであるが、今般の改正に合わせて、医療情報に関する IT サービスに関するガイドラインへの準拠性を遵守するための負担について軽減し、かつユーザー視点で評価できるようチェックシートの改定を行った。

本評価区分では、改定したチェックシートによる評価実施することとし、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こととなる。本評価を受けることで、以下のようなメリットがある。

- ユーザーは、自身の医療機関等で IT サービスに対するガイドライン遵守状況の評価を行う必要がある。民間事業者等との契約に基づいて確保した安全な場所に保存する場合、受託事業者が民間事業者等に課せられた経済産業省や総務省のガイドラインを遵守していることを確認する必要がある。この場合、評価に関しては、ガイドラインに対する理解や、IT サービスに対する専門の知識が必要となり、負担となる。本チェックシートによる HISPRO の評価を受けることで、IT サービスでのガイドラインの対象となる箇所が明確となり、専門の知識を持った評価員によって評価が行われ、安心した IT サービスの選択、利用が可能となる。
- サービス提供事業者は、ガイドラインに対する遵守状況について、自身の評価に対して、第三者、かつユーザー視点での評価を得ることができるため、ユーザーからの信頼を得た形でのサービスの差別化ができる。

2. 評価対象

民間事業者において、ネットワーク等を用い医療情報を扱う IT サービス

３．評価の視点

1) ユーザーの視点で評価を実施するため、ユーザーに開示すべき情報を用いて評価する。開示すべき情報は、説明責任などの観点から書面として保持していることが一般的であり、その書面を提出してもらい、評価のエビデンスとする。
2) ISMS、P マーク等の第三者認証の取得をしていることを前提条件とする。サービス提供者自体の安全管理体制が構築され、その現場確認が第三者によって行われていることが必須となる。ISMS に関して、取得範囲に保存業務を行う部門が含まれていることを確認する必要がある。
3) サービス提供に際しての責任分解について、適切な理解をしているかを評価する。特に医療機関等との責任分界、第三者サービスを利用する場合はそのサービスとの責任分界、販売代理店等を通して提供する場合における責任分界等の内容を評価する。
4) サービス提供を行うに当たっての、サービス提供者自身の体制が整備されているかについて評価する。
5) 提供するサービス自体の概要や構成内容について、ユーザーに対して説明をきちんと行えるかを評価する。
6) 提供するサービスに対して、ガイドラインに記載された技術的対策が実施されているかを評価する。
7) エビデンスを基に評価を行うが、エビデンスが不正確である場合や、実効性が確認できない場合等は、立入調査を実施することもある。また、更新評価の際に立入調査を行い、実効性を評価する場合がある。
8) 提供するサービスの紹介として、サービス提供者が「HISPRO 評価」を標榜する場

合においては、その表現についても評価する。評価内容は、HISPRO による評価範囲と齟齬がないか、記載が正確であるかについて等である。

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) 残金支払い(残金がある場合)
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
   (※ルールの整備状況を見る場合、フォーマット等の存在をエビデンスとして扱う)
6) 責任分界点の説明書
7) ユーザーへのセキュリティ遵守事項説明書（重要事項説明書等）
8) 「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等（標榜する場合のみ)

システム概念例

(※)連携に関してはサービス提供形態の多様化により、
機能での分割(XXaaS)や、仮想化等の形態があり得る