PHRサービス自己チェックリスト

点検日： 2023/4/18
点検者： 代表取締役　阿部達也

【一般的事項】

	チェック			
1．取り扱いの情報	はい（対応済）	いいえ（対応未）	わからない（不明）	該当しない
1-1.　個人の生活に紐付く医療・介護・健康等情報（ライフログを含む）を取り扱っていますか	レ			
1-2.　以下の情報を取扱っていますか（扱っている項目にチェックをお願いします。複数選択可）				
a. 個人情報保護法で定義される個人情報	レ			
b. 個人情報保護法で定義される要配慮個人情報	レ			
c. 個人情報保護法で定義される匿名加工情報		レ		
d. 個人情報保護法で定義される仮名加工情報		レ		
e.「民間 PHR 事業者による健診等情報の取扱いに関する基本的指針」で定義される健診等情報	レ			
f.「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」で定義される医療情報	レ			
2．説明と同意				
2-1.　個人の福祉・健康を主目的とすることを明示していますか	レ			
2-2.　契約の目的、PHRサービスの目的・使用用途等について正しく理解できるような方法で情報提供した上で、同意を取得していますか	レ			
2-3.　個人情報の利用目的をできる限り特定していますか	レ			
2-4.　要配慮個人情報を取得する場合や、データ連携等により個人情報を第三者に提供する場合に同意を取得していますか	レ			
3．解約に関する権利				
3-1.　解約の権利を設ける場合にはその旨を明示していますか	レ			
該当する場合、解約後のデータの処理について明示していますか	レ			
4．ユーザビリティ/アクセシビリティ（利用し易さ・便利さについて）				
4-1.　PHRサービスの内容に応じたユーザビリティやアクセシビリティの確保について検討していますか（参照：JIS X 8341-3:2016*）	レ			
5．本人確認				
5-1.　本人確認を実施していますか	レ			
5-2.　実施している場合、どの方法を用いていますか（扱っている方法にチェックをお願いします。複数選択可）				
a. オンラインでの本人確認（eKYC：electronic KYC（Know Your Customer）の略で、KYCをオンライン上で実現するための仕組みを指す）	レ			
b. 対面または郵送による本人確認（KYC：Know Your Customerの略で、本人確認を行う手続きを指す）		レ		
c. 氏名、住所、生年月日、メールアドレス等の情報入力		レ		
d. その他		レ		

【有効性に関する事項】

6．リコメンドサービス	はい（対応済）	いいえ（対応未）	わからない（不明）	該当しない
6-1.　法令順守、リコメンドサービスに対するリスクアセスメントの実施及び開示				
6-1-1.　リコメンドサービスが医行為に該当しないか、医師法17条に抵触していないかを少なくとも社内で確認していますか	レ			
6-1-2.　リコメンドサービスに使用するアプリケーションが医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律（薬機法）上のプログラム医療機器に該当するかを少なくとも社内で確認していますか	レ			
リコメンドサービスに使用するアプリケーションがプログラム医療機器に該当する場合、医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律（薬機 法）に基づく承認等を得ていますか				レ
6-1-3.　疾病の診断・治療に関わるPHRサービスを提供していますか		レ		
該当する場合、医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律（薬機法）の規定を遵守していますか				レ
6-1-4.　同サービスに対するリスクアセスメントの方法を開示していますか		レ		
6-2.　リコメンドサービスに対するリスクマネジメントシステムの確立				
6-2-1.　リコメンドサービスに対するリスクマネジメントシステム（PDCAサイクルの設定や体制）を確立していますか		レ		
6-2-2.　リコメンドサービスのための組織体制や責任等に言及した情報を開示していますか		レ		
6-2-3.　リコメンドサービスのプロセスやリソース、指導内容の根拠を提示できていますか		レ		
6-2-4.　リコメンドサービスに対する定期的レビューをしていますか		レ		
7．管理・閲覧サービス				
7-1.　管理・閲覧サービスに対するリスクアセスメントの実施及び開示				
7-1-1.　管理・閲覧サービスに対するリスクアセスメントの方法を開示していますか		レ		
7-2.　管理・閲覧サービスに対するリスクマネジメントシステムの確立				
7-2-1.　管理・閲覧サービスに対するリスクマネジメントシステム（PDCAサイクルの設定や体制）を確立していますか	レ			
7-2-2.　管理・閲覧サービスのための組織体制や責任等に言及した情報を開示していますか	レ			
7-2-3.　管理・閲覧サービスに対する定期的レビューをしていますか	レ			
7-3.　管理・閲覧サービスに対する利用者側の利便性				
7-3-1.　利用者が自身のPHRデータを自由に閲覧できるようになっていますか	レ			
7-3-2.　利用者の求めに応じてPHRデータを削除できるようになっていますか	レ			
7-3-3.　健診等情報を取り扱う場合は、その情報をエクスポートできるようになっていますか		レ		
7-3-4.　PHRデータ標準交換規格を取り扱っていますか？		レ		
該当する場合は、その情報を標準交換規格でエクスポートできるようになっていますか。		レ		

【安全性（機密性）に関する事項】

8．第三者機関による監査	はい（対応済）	いいえ（対応未）	わからない（不明）	該当しない
8-1.　情報セキュリティ対策				
8-1-1.　情報セキュリティに係る第三者認証（プライバシーマーク認証、ISMS認証、セキュリティ管理に係る内部統制保証報告書等）を取得していますか	レ			
8-1-2.　取り扱う情報の要求レベルに応じて、「民間PHR事業者による健診等情報の取扱いに関する基本的指針」の「２．情報セキュリティ対策＞２．１.安全管理措置＞（２）本指針に基づく遵守すべき事項」に定義される各項目について対応していますか	レ			
8-2.　脆弱性診断等システムにおける安全性				
8-2-1.　バリデーションプロセス（顧客、監査など）の経験がありますか	レ			
9．運用体制や責任者				
9-1.　情報管理責任者とカスタマーサポート				
9-1-1.　PHRサービスについての文書化された取扱説明書、取扱い手順、またはそれに類するものはありますか	レ			
ある場合、その文書をサービス利用者に開示していますか	レ			
9-2.　運用体制				
9-2-1.　適切に開発、管理及びサポートを実施する専門分野に対する経験及び資格または能力がある十分なスタッフを明示していますか	レ			
9-2-2.　アクシデントが発生した際のユーザーへの報告方法が明確になっていますか	レ			
9-3.　クラウド事業者の選定				
9-3-1.　取り扱う情報の要求レベルに応じて、十分な情報セキュリティ対策を行っているクラウド事業者やサービスを選定していますか	レ			

【信頼性に関する事項】

10．サービスにおける信頼性	はい（対応済）	いいえ（対応未）	わからない（不明）	該当しない
10-1.　当該PHRサービスの運用やカスタマーサポートの体制を開示していますか	レ			
10-2.　当該PHRサービスの健康情報管理における実績を何らかの形で開示していますか	レ			
10-3.　運用ポリシーを公開していますか	レ			
10-4.　当該PHRサービスは、第三者へのデータ提供を行っていますか		レ		
10-5.　当該PHRサービスは、利用者によるデータポータビリティを確保していますか		レ		
11．運用や体制の開示				
11-1.　医師法、薬機法を含む各種法令、ガイドライン、通達等の遵守及び開示				
11-1-1.　当該事業者のPHRサービスに関わる個人情報保護法、医師法、薬機法を含む各種法令、これらの法令等に関するガイドライン、通達等の内容を理解し、遵守していますか	レ			
11-2.　不具合発生時の体制及び対応方法の開示				
11-2-1.　当該PHRサービスの不具合発生時の体制及び対応方法を提示していますか	レ			

*JIS X 8341-3:2016 達成基準 早見表（レベルA & AA）https://waic.jp/files/cheatsheet/waic_jis-x-8341-3_cheatsheet_201812.pdf