Hôpitaux Universitaires Genève		*Référence :* Réf.: Checklist mHealth v1.1	
PSSI : Checklist sécurité pour les applications pour terminaux mobiles		*N° de version : 1.1*	*Créé le 26.11.2019*
Responsable du document : Security Officer			

Contexte d'application : Cette checklist de sécurité support le processus de validation des applications mobiles destinées à recevoir une certification HUG

Toutes les réponses OUI / NON doivent impérativement être accompagnées d'un commentaire. Les checklists non signées par le fournisseur ne seront pas analysées.

Le fournisseur est invité à transmettre (avec demande de NDA si besoin) tous les documents utiles pour expliciter les réponses apportées.

Le niveau d'exigence minimale dépend de la nature de l'application et de la criticité des données selon 3 niveaux. Une application peut implémenter des exigences du niveau supérieur, mais par l'inverse. (merci de préciser le niveau A1, A2, A3 avec les cases a cocher)

- ☐ A1 : Application pour information, promotion de la santé, sans personnalisation (criticité faible) :
- ☐ A2 : Application personnalisée pour la prise en charge de maladies (saisie de données, conseils) (criticité modérée)
- ☐ A3 : Application avec analyse de données pour le bilan/diagnostic de patients, avec usage à destination des professionnels (criticité élevée)

Authentification	Oui / non	Explication / Commentaire	Niveau
1. L'application mobile dispose d'un mécanisme d'authentification		*Préciser la méthode d'authentification : code PIN, mot de passe, empreinte digitale…*	A2, A3
2. Ce mécanisme authentifie le téléphone, l'utilisateur ou les deux		*Préciser l'objet de l'authentification*	A2, A3
3. Cet authentifiant est vérifié localement dans l'application mobile			A2
4. Cet authentifiant est vérifié sur un serveur distant		*A préciser le protocole utilisé pour la validation de l'authentifiant et quelle sécurité est appliquée au stockage des authentifiants côté serveur*	A3
5. Cette authentification est gérée par les couches systèmes du terminal ou redéveloppée dans les couches applicatives			A2, A3
6. Pour les accès des professionnels aux données collectées sur les serveurs, l'authentification peut être déléguée à un annuaire tiers (ex : azure AD…)			A3
7. Cette authentification s'intègre avec des standards de Single-Sign-On comme SAML ou OAuth			A3
8. Un processus de blocage est mis en œuvre localement sur le mobile en cas de fourniture répétée d'un mauvais authentifiant			A2

9. Un processus de blocage est mis en œuvre côté serveur en cas de fourniture répétée d'un mauvais authentifiant			A3
10. Il est possible de forcer un logout automatique dans l'application backend (appel d'une url par exemple ou autre) lors de la sortie du client local sur le terminal			A3
Contrôle d'accès			
11. Toutes les pages de l'application mobile sont protégées par une authentification		*Préciser celles qui ne le sont pas*	A2, A3
12. Tous les services de traitement des données collectés sur les serveurs distants sont protégés par un mécanisme de permissions			A3
13. Ces mécanismes de permissions s'appuient-ils sur des rôles applicatifs			A3
14. Des tests unitaires ou d'intégration sont disponibles pour démontrer le bon fonctionnement du mécanisme de permissions			A3
Sécurité du stockage des données			
15. Les données utilisateurs sont stockées en local sur le mobile			A1, A2
16. Les données utilisateurs sont exclusivement stockées sur des serveurs informatiques chez un prestataire (Editeur, cloud, institution santé…)			A3
17. Toutes les données stockées en local sont chiffrées. Sinon liste des données non chiffrées à fournir			A2
18. Ce chiffrement repose sur des standards		*Préciser l'algorithme (DES, AES…), le mode (EBC….) et la taille des clés*	A2
19. La génération et le stockage des clés de chiffrements sont sécurisé		*Préciser la méthode de génération (dérivées d'informations du téléphone, dérivées de l'authentifiant utilisateur, générées aléatoirement) et de protection des clés (stockage dans une enceinte sécurisée du téléphone..)*	A2
Sécurité des communications			
20. Les échanges avec les serveurs distants sont tous sécurisés avec TLS 1.2 ou supérieur			A1, A2, A3

21. L'application mobile implémente la méthode du « certificate pinning » pour s'assurer qu'elle dialogue avec le bon serveur			A3
Validation des entrées			
22. Toutes les entrées utilisateurs sont strictement validées.			A2, A3
23. La validation est assurée sur le serveur et non en local sur le mobile.			A3
Protection contre la modification de l'application et la rétro-ingénierie			
24. L'application détecte et rejette l'usage d'un téléphone jailbreaké/rooté, d'un émulateur			A3
25. Le binaire est offusqué		*Préciser comment*	*A3*
26. L'application vérifie que son binaire n'a pas été modifié		*Préciser comment*	*A3*
Cycle de vie de l'application			
27. Des activités sécurité sont-elles menées pendant le cycle de développement de l'application (Analyse de menaces, Revue de code manuelle ou automatisée, Tests d'intrusion…)		*Décrire processus*	*A2, A3*
28. Le processus de contrôle qualité garantie que l'application publiée ne contient aucune information ou fonctionnalité de debug		*Décrire processus*	*A2, A3*
29. Un processus surveille les clones de cette application sur le store Apple/Google		*Décrire processus*	*A1, A2, A3*
30. En cas de vulnérabilité de l'application, un correctif est mis à disposition sur les stores Apple/Google dans un délai minimal.		*Décrire processus et le délai de réaction*	*A1, A2, A3*
31. Il est possible d'imposer une version minimum de l'application mobile pour garantir que les utilisateurs ne se servent que de la version à jour			A1, A2, A3
32. Le code source de l'application répond au besoin du "software escrow". Il peut être sauvegardé chez un tiers de confiance et contenir l'ensemble des versions et documentations associés au bon fonctionnement de l'application.			A1, A2, A3
Respect de la vie privé de l'utilisateur			

33. Les permissions (agenda, position, stockage, SMS….) requises par l'application sont soumises à l'acceptation de l'utilisateur		*Fournir liste des permissions et préciser pourquoi ces permissions sont-elles toutes nécessaires*	A1, A2, A3
Test de sécurité			
34. L'application mobile a fait objet d'un test de sécurité par un tiers			A1, A2, A3
35. L'application sur le serveur a fait objet d'un test de sécurité par un tiers			A3

Visas

FOURNISSEUR	**Signature**
Société : ……	
Nom et Prénom : ……	
Fonction : ……	
Date : .../.../….	

HUG	**Signature**
Departement / Service : ……	
Nom et Prénom : ……	
Fonction : ……	
Date : .../.../….	