http://esante.gouv.fr/services/referentiels/securite/hebergement-faq#7

Q25 - Que dois-je décrire dans mon dossier de demande d'agrément pour pouvoir héberger des applications prévoyant un accès direct du patient à l'application ?

Au regard du caractère sensible des données de santé à caractère personnel, l'accès de tout acteur aux données de santé doit être réalisé de façon sécurisée (article L 1110-4 du code de la santé publique qui dispose que le patient a droit au respect de sa vie privée et du secret des informations la concernant).

Le dossier de demande d'agrément doit décrire les modalités d'identification et d'authentification du patient.

1- Identification

Le dossier de demande d'agrément doit préciser les moyens mis en œuvre pour réaliser l'enrôlement du patient.
Les procédés suivis doivent notamment assurer l'attribution du bon identifiant au bon patient afin d'éviter les doublons et les risques de collisions entre des dossiers de différents patients.

Lorsque l'hébergeur n'est pas en lien direct avec le patient, il doit clairement définir les principes que s'engage à respecter son client afin de garantir l'identification du patient.

2- Authentification

Il est impératif **d'utiliser un moyen d'authentification forte** afin préserver la sécurité des accès.
Plusieurs moyens d'authentification forte peuvent être mis en œuvre par l'hébergeur ou son client.

A titre d'exemple, voici quelques moyens qui peuvent être retenus.
1- Utilisation d'un identifiant/passe associé à un mot de passe à usage unique (OTP = One Time Password) envoyé par mail ou SMS.

Le dossier de demande d'agrément doit préciser :

- Qui délivre le mot de passe au patient et par quel procédé (le mot de passe doit être personnalisé par le patient lors de la première connexion à l'application) ?
- Qui recueille les informations relatives au canal de transmission de l'OTP (adresse mail ou numéro de téléphone mobile) ?

2- Utilisation d'un certificat électronique de type carte à puce

Le dossier de demande d'agrément doit préciser :

- Les moyens de protection du certificat (code pin, biométrie, etc.).
- Qui délivre le certificat au patient et comment ?

Lorsque l'hébergeur n'est pas en lien direct avec le patient, il doit clairement définir les principes que s'engage à respecter son client afin de garantir l'authentification forte du patient.

Retour au Sommaire