Il y a plusieurs mesures possibles pour sécuriser les données des habitants :

-Imposer des mots de passes forts (majuscule, minuscule, chiffre et symbole en un mot de passe)

-Imposer l'authentification a 2 facteurs (A2F) qui est une vérification par mail ou SMS pour certaines connexions.

-Un système d'expiration de session pour les utilisateurs qui les déconnecte automatiquement au bout d'une certains durée

-Chiffrer les données sensibles stockées comme les mots de passe ou les données personnelles.

-Toute les communications doivent utiliser TLS/SSL

-Faire en sorte que le système de permissions accorde le moins de privilèges possibles pour chaque rôle, par exemple qu'un résident ne puisse voir que ses données.

-Limiter le nombre de requetes qui peuvent être faites pour prévenir une attaque.

-Système de logs (historique) permettant d'enregistrer des activités suspectes comme des tentatives de connexions échouées.

-Notifications en cas de connexion depuis un nouvel appareil

-Eduquer les utilisateurs et leur donner des conseils comme ne pas partager leur mots de passe.

-Forcer les mises a jour permettant de corriger des failles de sécurité