Débuter avec l'outil MhCare

1- Premiers pas avec MhCare

2- Récupérer son mot de passe MhCare sur l'application Web

3- Se connecter sur le site Web de MhCare

   - 1ère connexion de la journée sur « MhCare Web »

4- Configurer ses informations de facturation

5- Télécharger l'Application MhCare mobile

   - 1ère connexion de la journée sur « MhCare Mobile »

6- Éléments complémentaires

   - Communiquer autour du patient
   - Accéder à la documentation en ligne

Pour toutes questions relatives à **l'utilisation de l'outil**, des problèmes de **facturations** ou de **règlements**, notre hotline est à votre disposition :

- Par téléphone au **04 78 78 59 59** (tous les jours de 8H30 à 12H30 et de 13H à 17H, sauf le mercredi uniquement de 13H à 17H)
- Par mail à l'adresse suivante : **HADHotline@lyon.unicancer.fr**

Premier pas avec MhCare

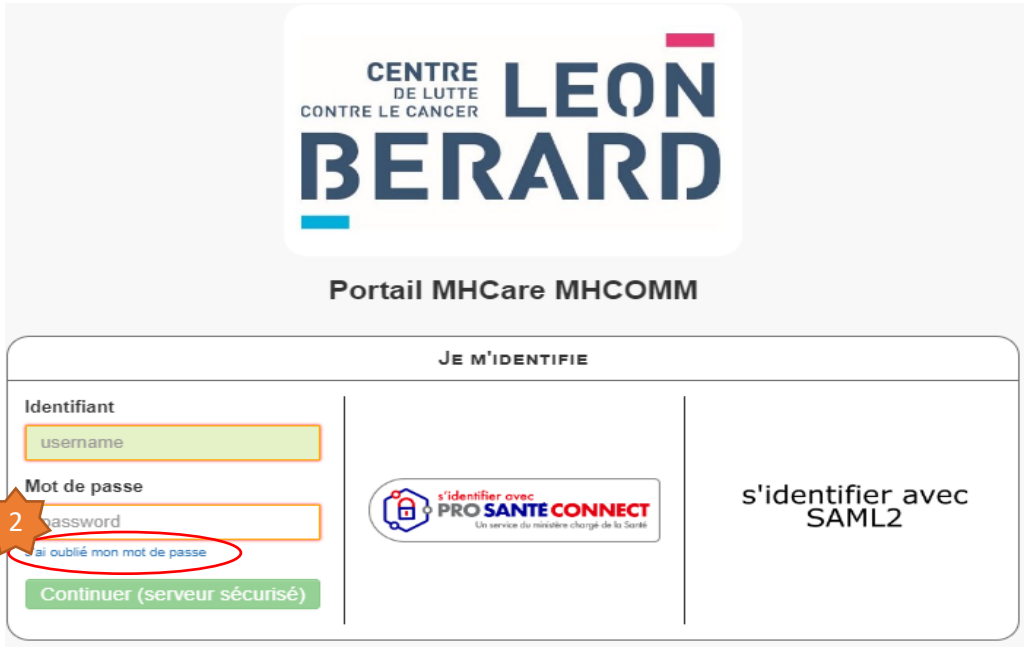
Ouvrir un navigateur (Edge / Chrome) et saisir dans la barre d'adresse le lien suivant :

https://domicile.centreleonberard.fr/

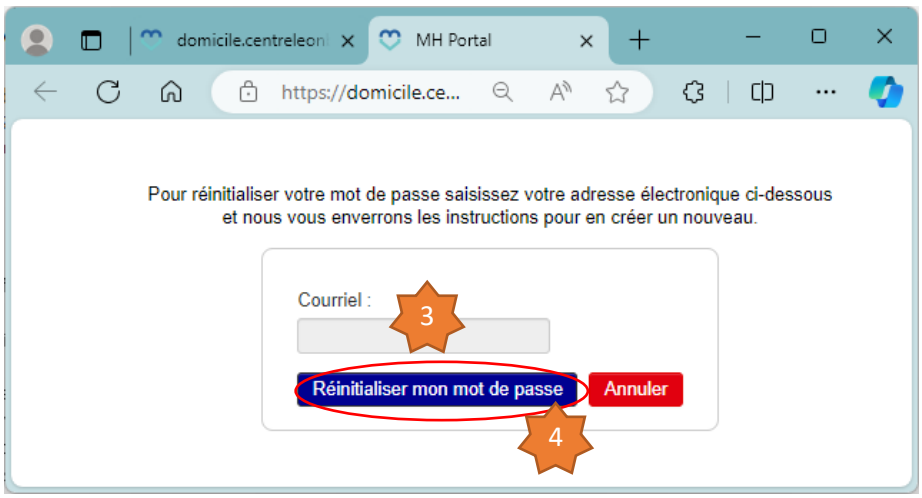
Étape 1 : Récupérer son mot de passe MhCare

1- Ouvrir un navigateur (Edge/Chrome/Firefox …) et saisissez dans la barre d'adresse le lien suivant : **https://domicile.centreleonberard.fr/,**
2- Cliquez sur le lien bleu « J'ai oublié mon mot de passe »
3- Dans l'écran suivant, saisissez votre **adresse mail** unique que vous avez communiquez au service HAD comme identifiant dont vous êtes seul propriétaire.
4- Puis cliquez sur le bouton Réinitialiser mon mot de passe

→ Un mail va vous être alors envoyé. Suivez les indications du mail pour vous générer votre mot de passe personnel



L'**Identifiant** MhCare est votre **adresse mail** que vous avez communiquez au service HAD comme identifiant personnel (pas de mail de cabinet).



Se connecter sur le site web de MhCare

2 types de connexion au site sont proposés :

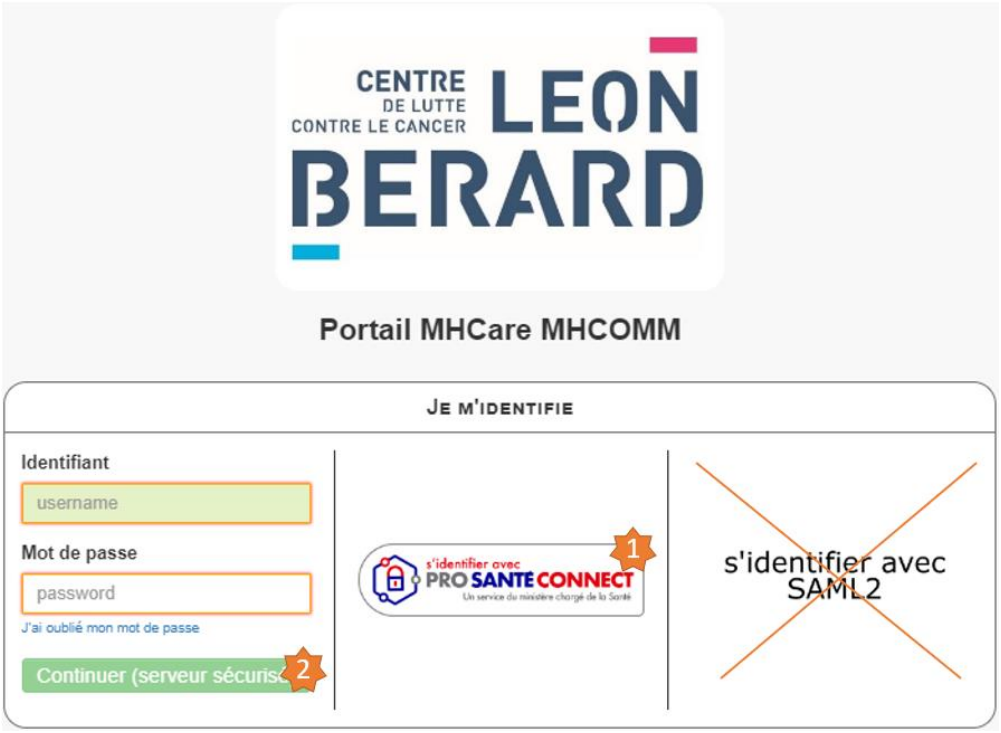
1- Par PRO SANTÉ CONNECT → https://esante.gouv.fr/produits-services/e-cps/guides/je-me-connecte
2- Ou via Identifiant / Mot de passe (unique et dont vous êtes seul propriétaire/utilisateur)

Identifiant :

Adresse mail MhCare personnelle (permet de vous identifier en tant que tiers physique unique)

Mot de passe :

Mot de passe créé à l'étape 1

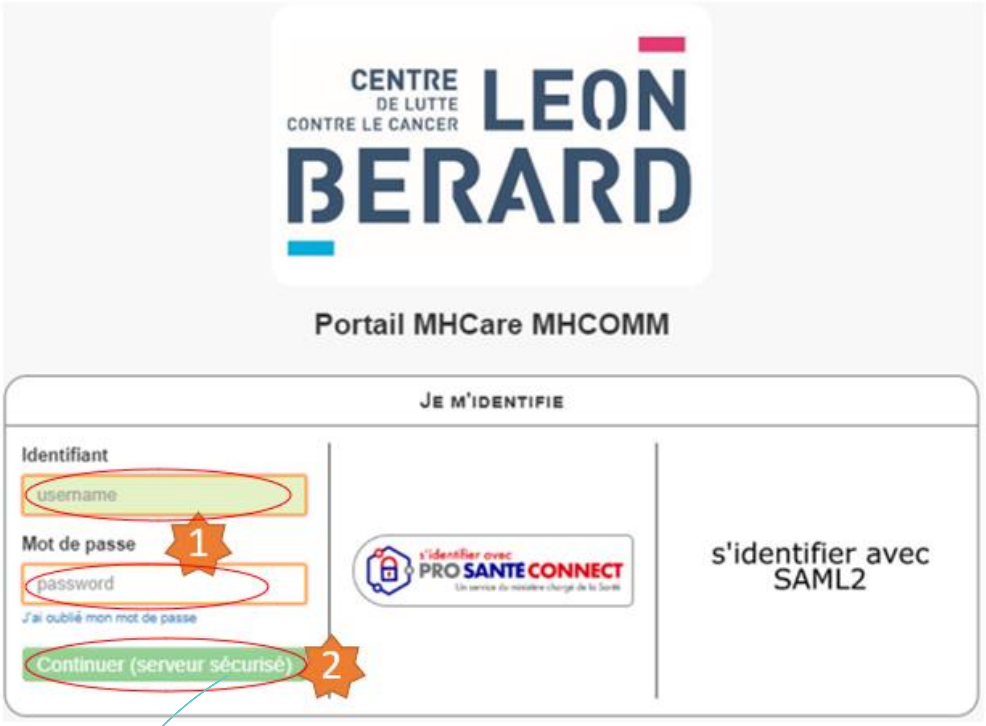


Première connexion de la journée sur « MhCare Web »

Lors de votre première connexion de la journée, que ce soit sur web ou sur mobile, vous aurez une double authentification à réaliser.

Sur l'**application web** https://domicile.centreleonberard.fr/, connectez-vous via ProSantéConnect ou entrez votre identifiant (mail personnel communiqué au service HAD) ainsi que votre mot de passe renseigné à l'étape 1, Puis cliquez sur « Continuer ».

Lors de votre première connexion de la journée, vous recevrez un SMS avec un code à saisir à l'écran 3



L'**Identifiant** MhCare est votre **adresse mail** communiqué au service HAD comme identifiant personnel (pas de mail de cabinet).

Le **SMS** est envoyé sur le numéro de mobile communiqué au service HAD comme numéro de téléphone personnel (pas de numéro de cabinet)

Ne pas faire « Entrer », mais bien cliquer sur le bouton « **Send Code** »

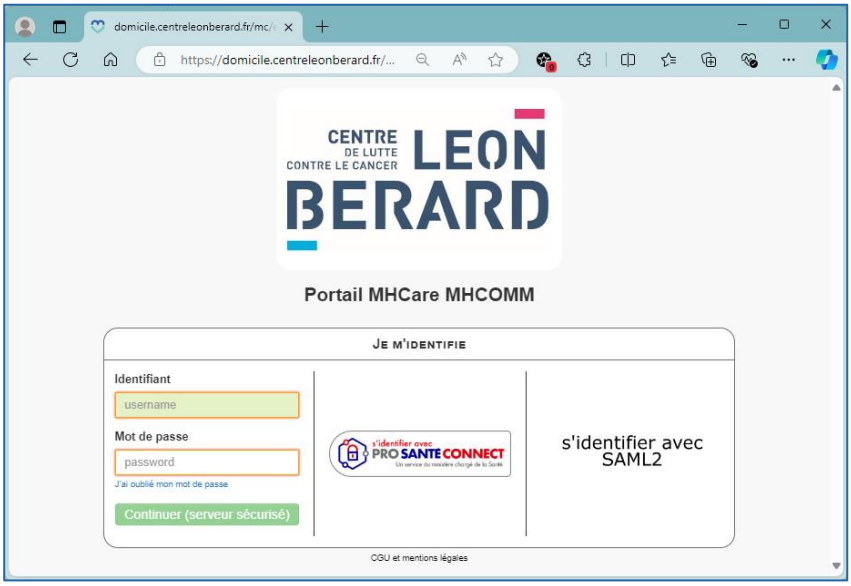
Étape 2 : Prérequis pour la facturation

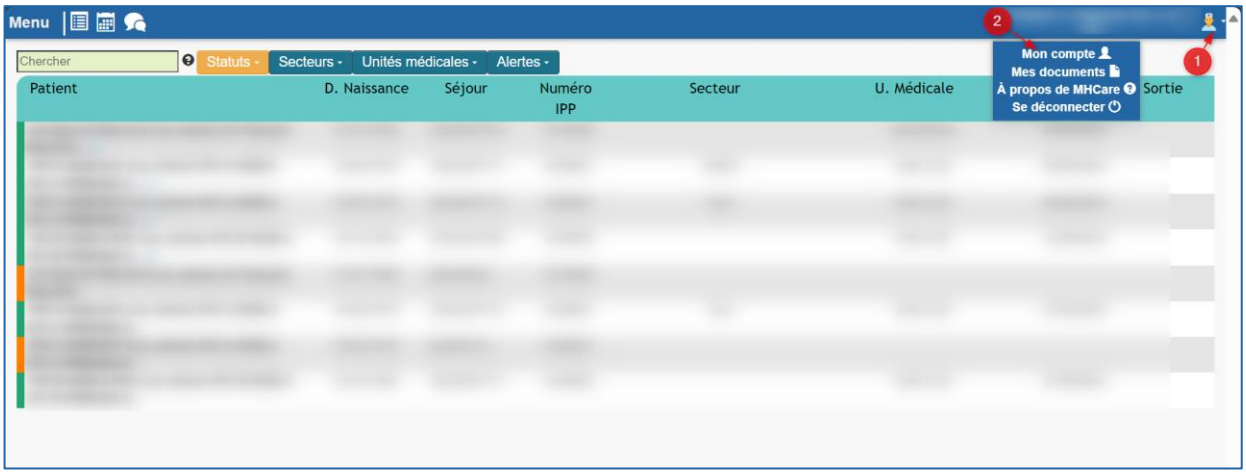
A la 1ere connexion sur l'application web https://domicile.centreleonberard.fr/ via Identifiant/mot de passe ou via ProSantéConnect

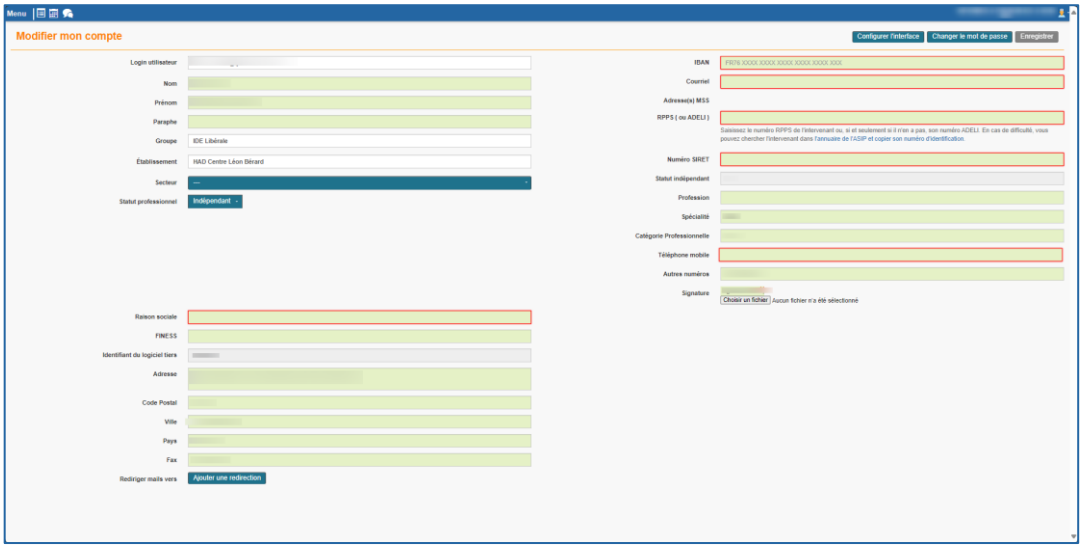
Mettre à jour à minima les éléments suivants de votre compte pour être réglé :

- **Raison sociale** (généralement votre **nom** suivi de votre **prénom** en **MAJUSCULE**)
- **IBAN**
- **N° RPPS** (pas ADELI)
- **SIRET** (14 chiffres)

Vous pourrez aussi modifier votre **mot de passe** via cet écran de modification des données de votre compte

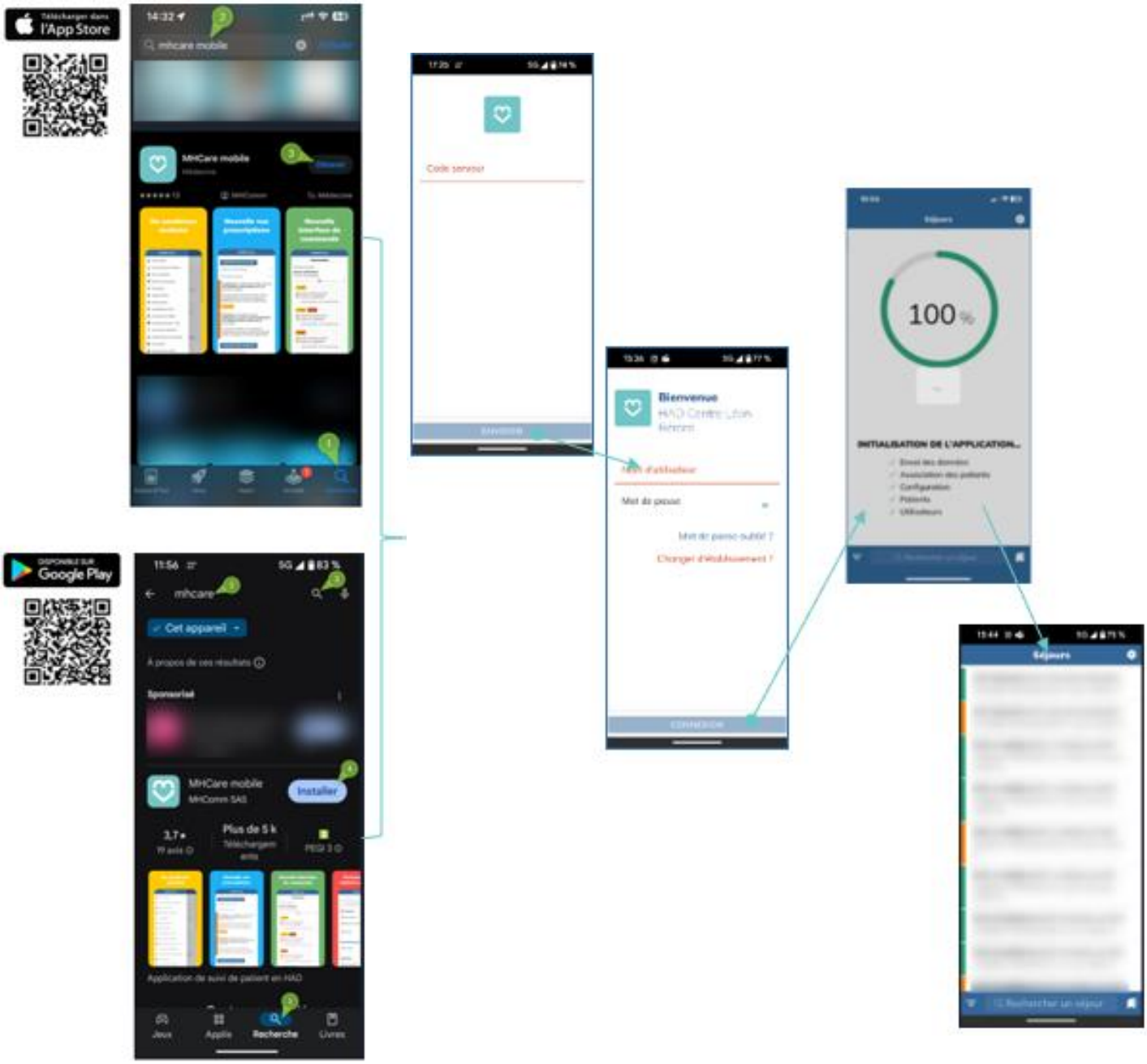






Étape 3 : Installer et ouvrir de l'application « MhCare mobile »

1- Recherchez et installez l'application mhcare de MHComm sur le Play Store ou l'Apple Store en fonction du type de mobile
   - Le code serveur à utiliser est **69000** et cliquer sur « Envoyer »
2- Renseignez ensuite le **Nom d'utilisateur** avec votre **adresse mail** que vous avez communiquez au service HAD comme identifiant personnel (pas de mail de cabinet)
3- Puis votre mot de passe personnel
4- Cliquez alors sur « Connexion »



Première connexion de la journée MhCare mobile

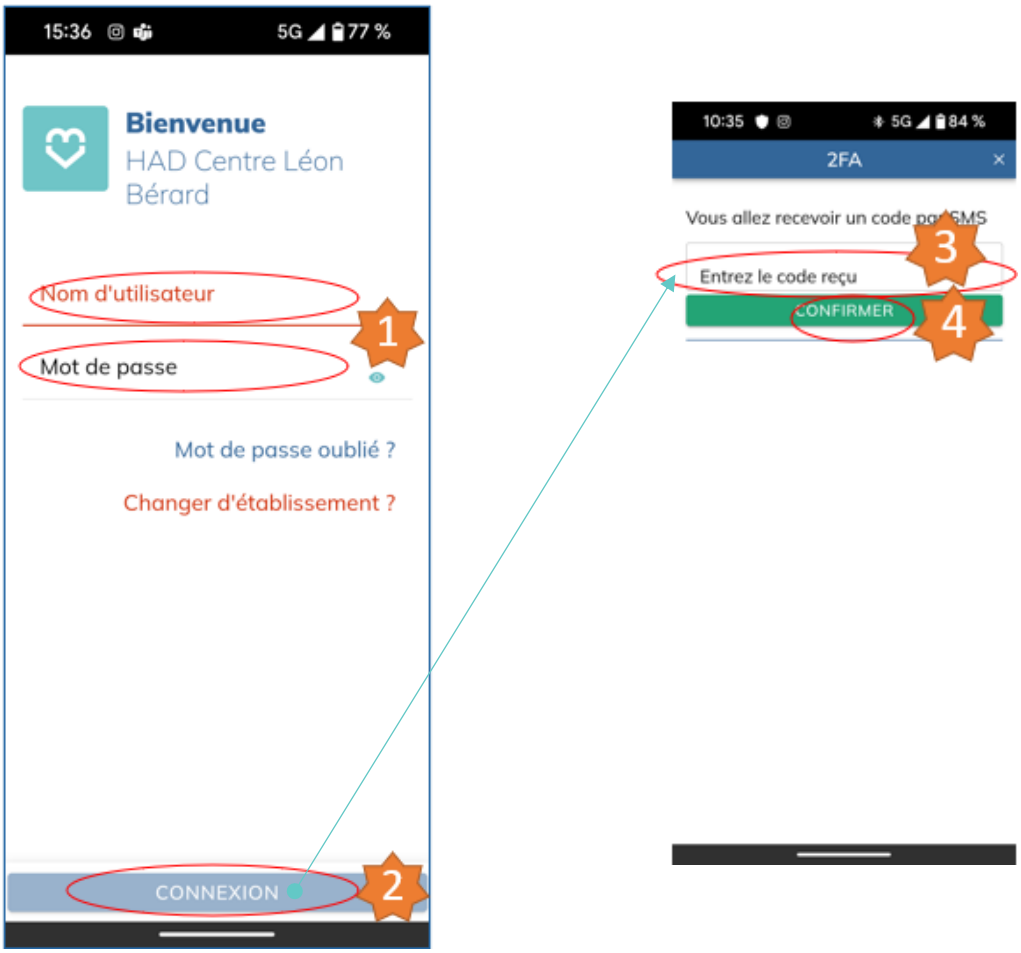
Lors de votre première connexion de la journée, que ce soit sur web ou sur mobile, vous aurez une double authentification à réaliser.

Sur l'**application Mhcare mobile**, entrez dans le « Nom d'utilisateur » le **mail personnel** communiqué au service HAD, **votre mot de passe** renseigné à l'étape 1, puis cliquez sur « CONNEXION »

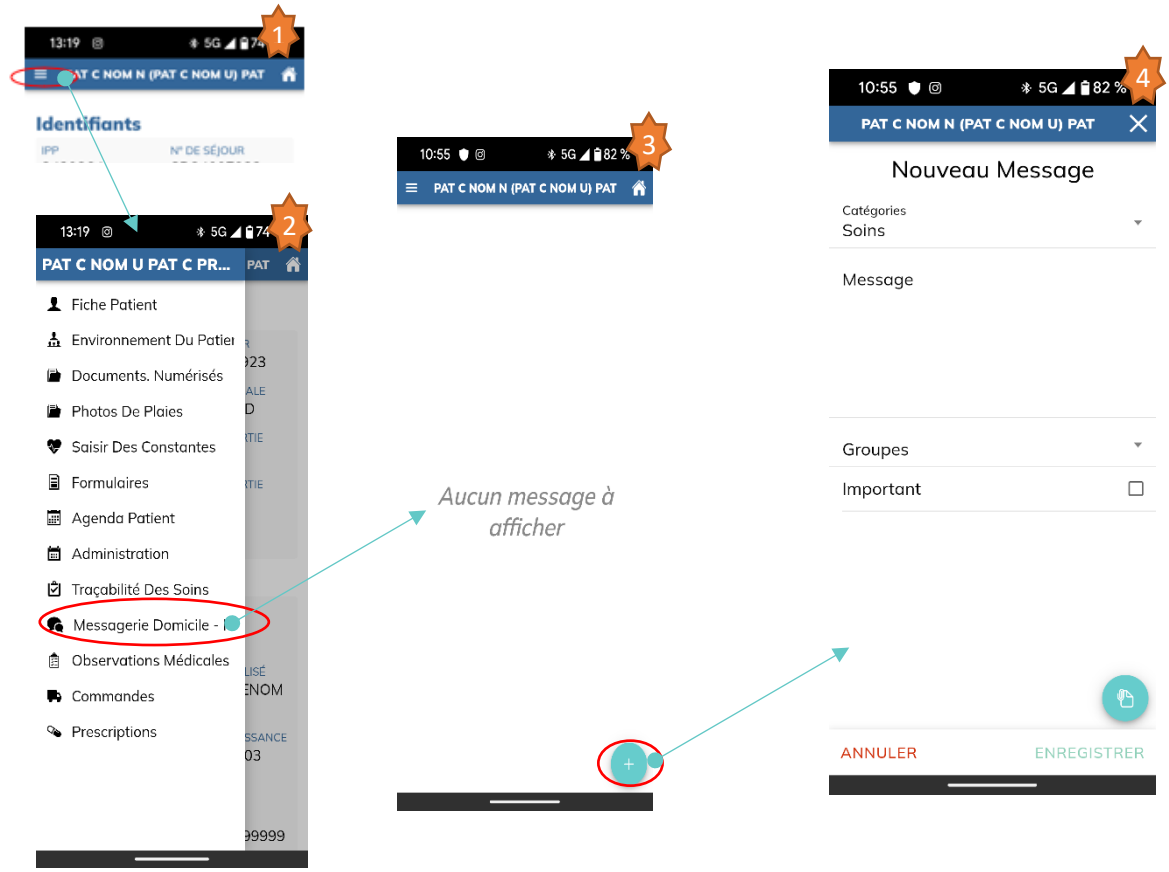
Lors de votre première connexion de la journée, vous recevrez un SMS avec un code à saisir à l'écran 3

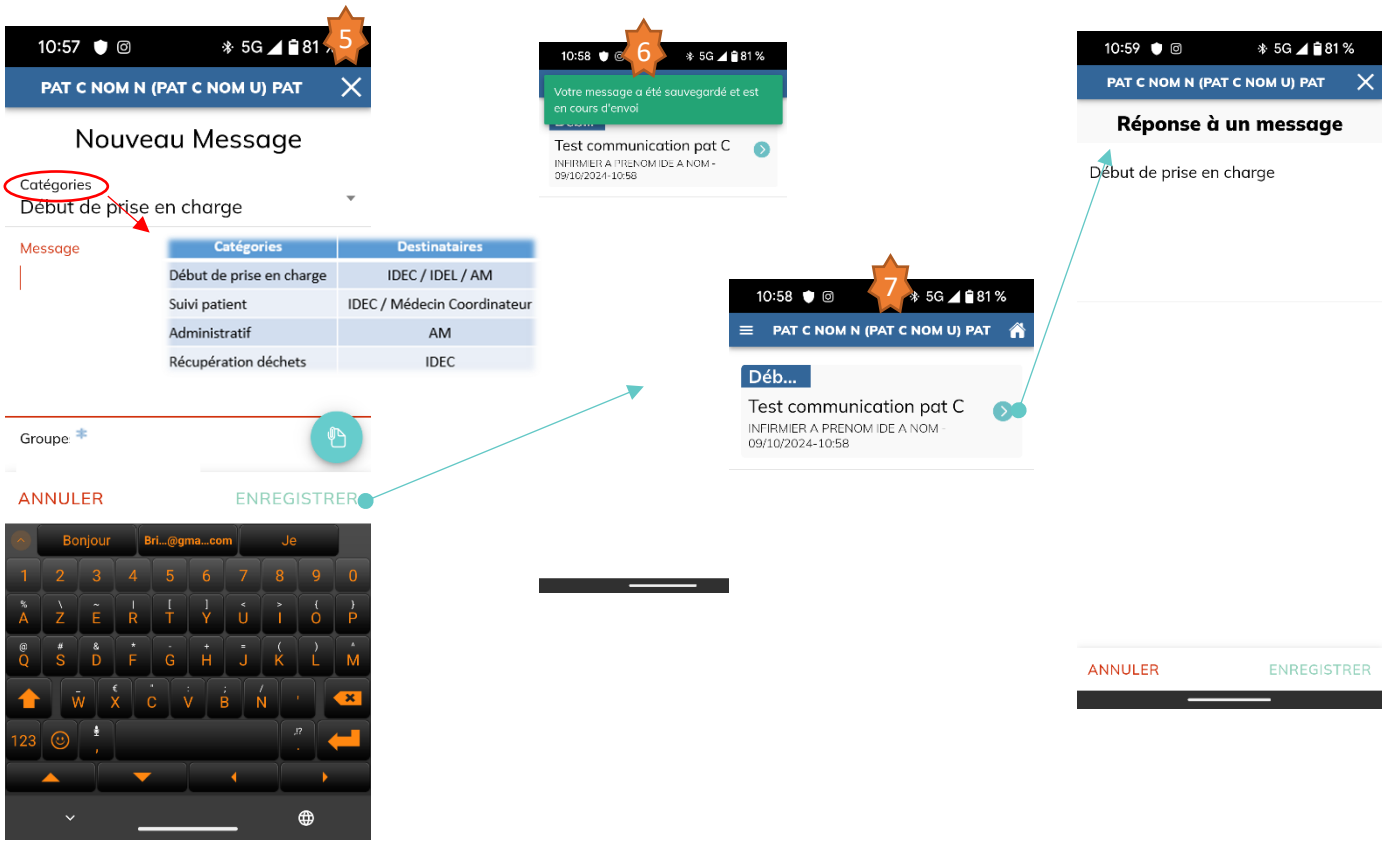
Le **Nom d'utilisateur** MhCare est votre **adresse mail** que vous avez communiquez au service HAD comme identifiant personnel (pas de mail de cabinet).

Le **SMS** est envoyé sur le numéro de mobile vous avez communiquez au service HAD comme numéro de téléphone personnel (pas de numéro de cabinet)



Élément complémentaire : Communiquer autour du patient

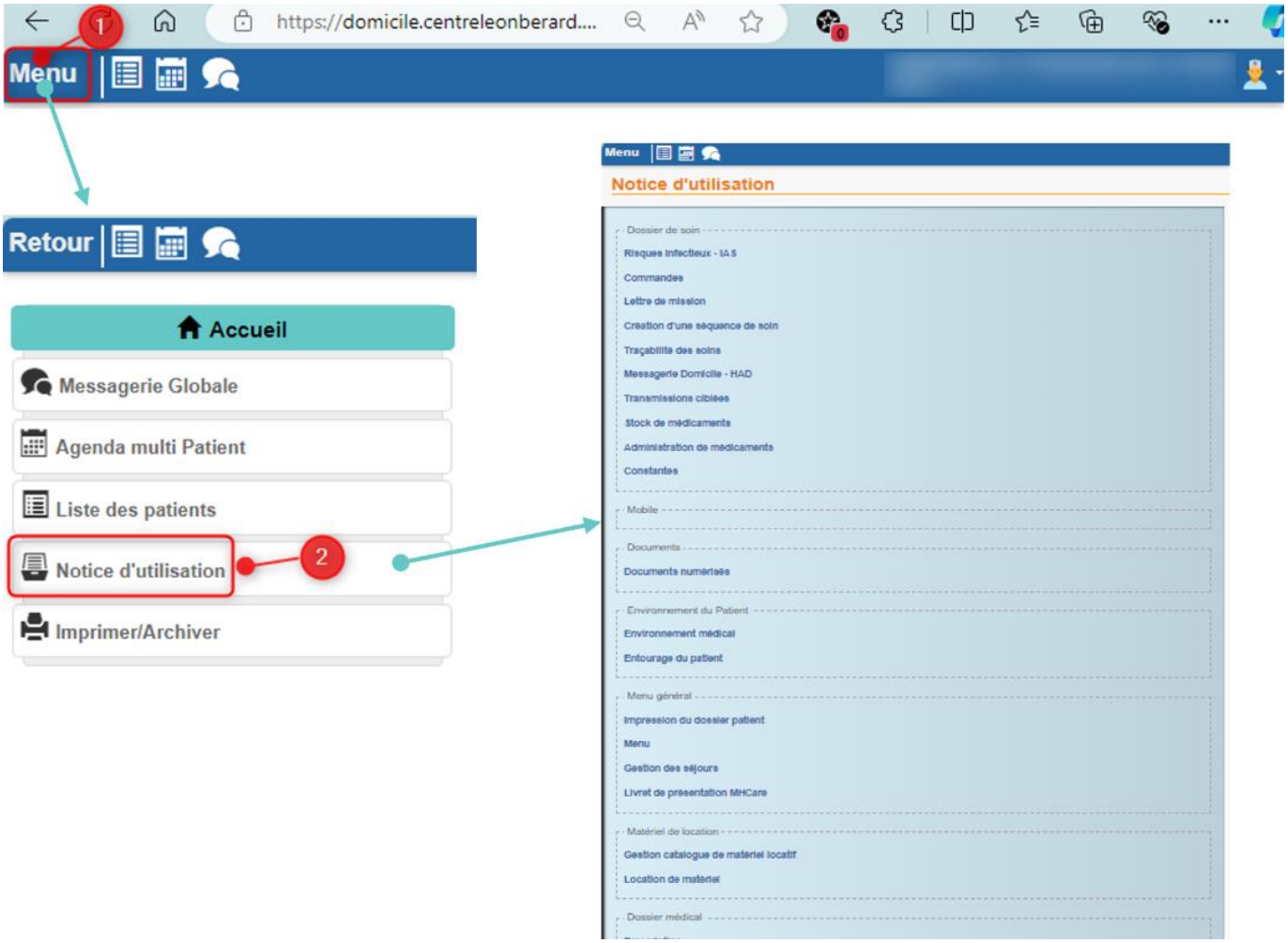




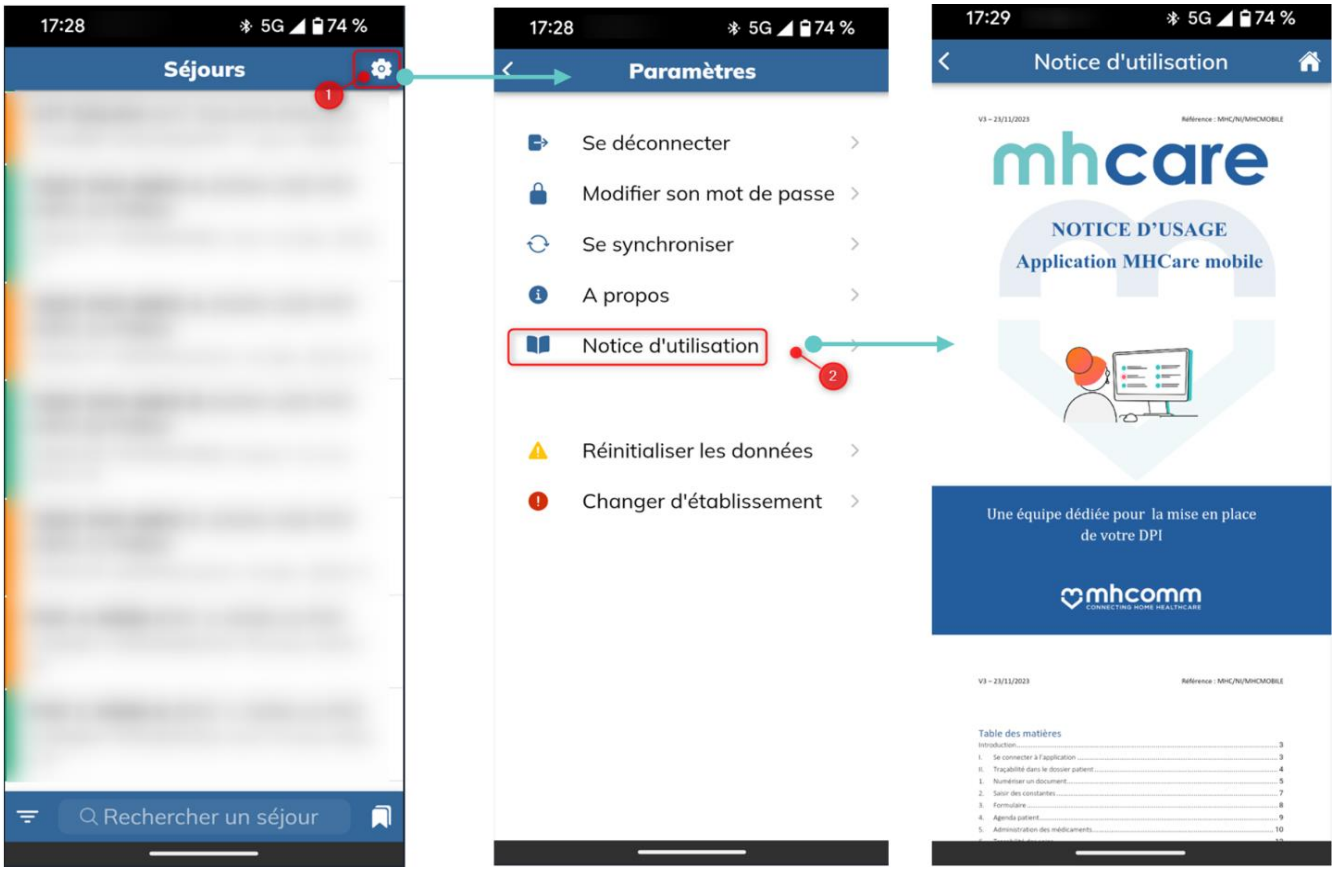
* **Ne pas utiliser les « Groupes »** (restriction sur les destinataires des catégories)

Élément complémentaire : Accéder à la documentation en ligne

MhCare Web



MhCare mobile



10 bonnes pratiques

POUR LA SÉCURITÉ INFORMATIQUE ET LA PROTECTION DES DONNÉES

à domicile

CENTRE LEON BERARD

Utilisez les bons outils 1

Utilisez des outils professionnels et sécurisés :

- MHCARE, pour la prise en charge HAD du Centre Léon Bérard,
- MonSisra, pour communiquer entre professionnels de santé,

Ces outils sont à même d'héberger de la donnée de santé car ils sont certifiés HDS (Hébergeur de Données de Santé).

A savoir

Je ferme la porte aux WhatsApp, boîtes mails, Wetransfer ou autres outils non sécurisés pour partager des données patients.

2 Protégez votre identité

Votre identité vous appartient, ne la partagez pas avec vos collègues, votre famille, ou vos amis. Votre identité numérique est généralement garantie par plusieurs facteurs permettant de confirmer votre identité (nom d'utilisateur, adresse mail mais aussi téléphone mobile personnel). Ces éléments sont associés à une clé secrète : votre mot de passe.

Un mot de passe, c'est comme une brosse à dents, cela ne se prête pas !

A noter

Dans MHCARE la double authentification journalière par SMS vous protège. C'est pour cette raison que nous vous demandons un numéro de téléphone mobile et une adresse mail dont vous êtes le seul propriétaire.

Gérez vos mots de passe 3

Nous vous conseillons de :

- Créer un mot de passe long et complexe pour le rendre robuste. Il doit être différent pour chaque site,
- Changer les mots de passe régulièrement,
- Utiliser un gestionnaire de mots de passe pour ne pas avoir à les retenir (Par exemple KeePass certifié par l'ANSSI)
- Activer la double authentification dès que possible.

Astuce

1. Écrivez une phase avec 12 mots dont 1 nombre, 1 majuscule, 1 signe de ponctuation ou 1 caractère spécial (dollar, dièse, ...). ex : « J'ai 1 plante verte et 3 arbres fruitier dans mon jardin. »
2. Pour retrouver votre mot de passe :
   - Mémoriser la phrase choisie avec les majuscules, les nombres et la ponctuation,
   - Prendre les premières lettres de chaque mot, garder les nombres et la ponctuation. Ex : « J'a1pve3afdmj. »

4 Vérifiez vos sources

Avant de cliquer, vérifiez :

- Les liens : Ne cliquez pas sur les liens contenus des e-mails non sollicités ou suspects, surtout s'ils ont un caractère urgent. Astuce pour voir le lien : survolez le lien avec votre souris ou appuyez longuement dessus avec votre doigt sur écran tactile.
- L'expéditeur : Si un message semble louche, contactez directement l'organisation concernée.
- Par téléphone aussi je confirme l'identité de la personne, en enregistrant les numéros fiables. Je ne communique jamais d'informations si j'ai un doute.

A retenir

80% des attaques informatiques passent par du "fishing", soyez particulièrement vigilant aux mails qui vous demandent de saisir vos identifiants !

Évitez les réseaux wifi publics et inconnus 5

- En mobilité préférez la 4G ou 5G,
- Si vous n'avez pas le choix, ne pas réalisez aucune opération sensible et essayez d'utiliser un VPN.

La raison

Les wifi publics sont souvent mal protégés et peuvent être piratés facilement.

6 Appliquez les mises à jour

L'explication

…Dès qu'elles sont proposées.

Les mises à jour permettent de corriger les failles de sécurité que pourraient exploiter des pirates pour détruire vos données, voler vos mots de passe ou vous espionner…

Installez un antivirus 7

Il permet de se protéger d'une grande majorité d'attaques et de virus connus.

A faire

- ☐ Vérifiez qu'il est bien actif,
- ☐ Le tenir à jour.

8 Utilisez les applications officielles

Je m'applique à :

- Installer les applications uniquement via les sites officiels,
- Vérifier qu'il s'agit bien d'un site officiel, comme https://domicile.centreleonberard.fr/,
- M'assurer qu'il ne s'agit pas d'une copie frauduleuse pour récupérer des informations bancaires,
- Vérifier que le site est sécurisé.

Le truc

Un site sécurisé est représenté dans le navigateur par un cadenas dans la barre d'adresse et l'adresse du site commence par https.

Je me méfie des clés USB 9

Utilisez des clés USB ou des périphériques USB uniquement si vous en êtes le propriétaire. Une clé USB malveillante peut griller un PC en 1 seconde ou récupérer toutes vos données.

Toujours

Se méfier des clés USB abandonnées…

10 Maîtrisez vos réseaux sociaux

Ils contiennent des données personnelles qui ne doivent pas tomber entre de mauvaises mains. Il est nécessaire de :

- Sécuriser l'accès par mot de passe robuste
- Définir les bons niveaux de sécurité sur vos profils pour qu'ils ne soient pas inconsidérément publics ou utilisés pour vous nuire

Vérifier la véracité des informations avant de les partager.

Ne pas oublier

Ne prenez pas de photo sur vos lieux de travail en dehors des usages à visée médicale (photos de plaies, pansements, …).

Les photos à visée médicale doivent être manipulées avec soins. Ne les stockez pas sur vos portables mais dans les applications dédiées. Ne les envoyez pas sur des canaux non professionnels ou non sécurisés.

Surtout ne postez jamais de photos de vos lieux de travail sur des réseaux sociaux, même si aucun patient n'est dessus.