

## UTILISATION DE MON COMPTE PROFESSIONNEL

L'utilisation d'un **compte professionnel** permet de vous identifier. **Vous seul devez l'utiliser!** Les accès aux données médicales sont **obligatoirement nominatifs**.

### ■ MOT DE PASSE

Le mot de passe est la **clé d'accès** aux systèmes et à votre identité numérique. Il doit être :

#### SECRET

Il ne faut **en aucun cas le dévoiler**.

#### RENOUVELÉ

Il doit être **changé régulièrement**.

#### ROBUSTE

**Conforme aux préconisations** de votre Direction Informatique (Ex: 10 caractères avec minuscules, majuscules, chiffres et caractères spéciaux).

#### UNIQUE

Utilisez **un mot de passe différent pour chaque site**.

### ■ DROITS D'ACCÈS

Dans le cadre du **respect de la confidentialité** et afin de limiter les accès illégitimes, **n'utilisez que votre compte personnel**.

**Pensez à vous déconnecter lorsque vous quittez votre poste.**

## COMMENT STOCKER ET ÉCHANGER DE L'INFORMATION SANS RISQUES



### MESSAGERIE ET EMAILS INCONNUS

Restez vigilants face aux **emails d'origine inconnue**. Une attaque courante consiste à **inciter à cliquer** sur un lien contenu dans un email.



### SMARTPHONES, CLÉ USB ET ÉQUIPEMENTS MOBILES

Tous les moyens techniques mobiles mis à votre disposition sont **pratiques mais pas sans risques**.

- **Ne modifiez pas leur paramétrage,**
- **À la maison, ne les laissez pas à la portée de tous,**
- **Ne les connectez pas à des équipements inconnus.**

Prenez connaissance des règles d'utilisation de la **Charte Informatique** de votre établissement.



### DOCUMENTS PAPIER

Dans notre quotidien, nous utilisons encore des documents papier **sensibles ou à caractère personnel**.

- **Ne les jetez pas à la poubelle,**
- **Ne les oubliez pas dans l'imprimante,**
- **Détruisez-les ou conservez-les sous clé.**



### HÉBERGEMENT EN LIGNE

**N'enregistrez pas** vos documents confidentiels ou les données de vos patients **en ligne** (Gmail, Hotmail, Google Docs, Dropbox, etc.).

L'hébergement de données de santé demande une **certification**.

Prenez connaissance des solutions existantes en contactant **la Direction Informatique**.

En cas de comportement suspect de votre poste de travail, **contactez votre Direction Informatique.**

## 10 BONNES PRATIQUES

- 1 Choisissez un mot de passe **complexe**, à garder **secret** et à changer régulièrement.
- 2 **N'ouvrez pas** un email dont vous ne connaissez pas l'origine.
- 3 **Soyez vigilants** lorsque vous connectez un support externe inconnu.
- 4 **Verrouillez votre session** lorsque vous quittez votre poste.
- 5 Sur les réseaux sociaux, **soyez discrets**.
- 6 **Protégez** les documents sensibles.
- 7 **Redémarrez votre poste** si une pop-up vous invite à le faire pour appliquer les mises à jour.
- 8 **Sauvegardez vos données conformément** aux préconisations de votre Direction Informatique.
- 9 **N'utilisez pas d'objets connectés** sur votre poste de travail sans validation de la Direction Informatique.
- 10 Vol ou perte de matériel : **contactez** au plus tôt la Direction Informatique.

## LES ENJEUX DE LA SÉCURITÉ MÉDICALE



Garantir l'**intégrité** des données de santé



Assurer la **disponibilité** des services et des informations médicales



Protéger la **confidentialité** des informations sensibles



Assurer la **traçabilité** des actions

CONTACT :



Ne pas jeter sur la voie publique

Plaquette réalisée par SESAN, maîtrise d'ouvrage opérationnelle des systèmes d'information en santé en Île-de-France - Avril 2019  
Service proposé par le GCS SESAN  
Script Laser - Paris 3

contact : ssi@sesan.fr



# SÉCURITÉ DES SYSTÈMES D'INFORMATION



## GUIDE DE BONNES PRATIQUES

Protégez les informations des patients et protégez-vous!