

LES SOINS AUX PATIENTS PASSENT AUSSI PAR LA CYBERSÉCURITÉ

Mot de passe

- Ayez un mot de passe robuste (long et complexe)
- Ne laissez pas sur votre bureau de post-it avec votre mot de passe

01

02

Ne laissez pas d'équipements sans surveillance

Lorsque vous n'utilisez pas votre poste de travail, pensez à le verrouiller

Protégez votre messagerie électronique

- Ne cliquez jamais sur une pièce jointe ou un lien douteux
- Ne répondez jamais à un e-mail suspect (contactez l'expéditeur par un autre canal)

03

04

Méfiez-vous des supports USB

- Ne branchez jamais sur votre équipement informatique une clé USB trouvée ou offerte
- Utilisez uniquement les clés USB fournies par le CHU

Maîtrisez ce que vous diffusez sur les réseaux sociaux

- Ne partagez pas d'informations qui pourraient porter préjudice à la patientèle ou à l'établissement
- Les données personnelles des patients sont confidentielles

05

06

Séparez les usages personnels et professionnels

- N'utilisez pas vos moyens personnels (téléphone, adresses e-mail, gadgets électroniques,...) à des fins professionnelles et inversement

En cas de risque / incident

- Informez immédiatement le pôle informatique, même en cas de léger doute
- Signaler, ce n'est pas déranger, c'est protéger

07

