

FICHE RÉFLEXE

SÉCURISATION DES VISIOCONFÉRENCES



Les réunions virtuelles sont devenues un outil de communication essentielle pour faciliter les échanges entre professionnels et la coordination des soins. Toutefois, elles présentent des risques de sécurité, notamment en ce qui concerne la confidentialité des échanges.

#1

CHOISIR UNE PLATEFORME APPROUVÉE

- Au sein de l'hôpital, la solution utilisée et approuvée par la DSI est Webex. Cette dernière est conforme aux normes de sécurité et de chiffrement, ainsi qu'aux exigences RGPD (Règlement Général sur la Protection des Données) et aux diverses réglementations sur la protection des données de santé.
- Éviter les outils non sécurisés (Skype non pro, WhatsApp...). Vous ne devez pas organiser une réunion sur une de ses plateformes. Par défaut, ils sont bloqués par le proxy de l'établissement.



Dans le cas où vous souhaitez rejoindre une réunion sur une solution autre que Webex, par exemple une réunion distanciel Microsoft Teams ou Zoom, vous pouvez nous adresser une demande afin de vous ouvrir les accès et pour effectuer une démonstration sur son lancement.

#2

CONFIGURER LA RÉUNION DE FAÇON SÉCURISÉE

- Ajouter un mot de passe à la réunion.
- Restreindre les accès aux seuls participants autorisés.
- Activer la « salle d'attente » virtuelle pour valider manuellement l'entrée des participants.
- Évitez de distribuer le lien de la visioconférence sur des réseaux sociaux.
- Désactiver la possibilité pour les participants d'enregistrer la réunion sans autorisation.

#3

VÉRIFIER DES PARTICIPANTS ET DES PARTAGES

- Vérifier l'identité des participants avant d'admettre quelqu'un dans la réunion.
- Expulsez immédiatement tout participant inconnu.
- Masquez ou fermez les documents sensibles avant de partager votre écran.
- Partager les documents via des espaces sécurisés plutôt que par le chat de la plateforme.

#4

CAMÉRAS ET MICROPHONES

- Désactiver la caméra et le micro lorsque leur utilisation n'est pas nécessaire.
- Utiliser un cache physique sur la caméra lorsqu'elle n'est pas en fonction (sur quelques ordinateurs, elle est intégrée au niveau de la caméra, sinon il est possible de la cacher avec un support qui ne fait pas passer la lumière)



EXEMPLE CONCRET

Cas pratique : Une équipe de psychiatres discute d'un cas patient en visioconférence. Ils activent la salle d'attente, vérifient l'identité de chaque participant, puis démarrent la réunion en mode confidentiel.

SIGNALEZ IMMÉDIATEMENT

- Une intrusion dans une visioconférence (quelqu'un que personne ne reconnaît, ou une personne connue n'ayant pas l'autorisation d'accéder à ces informations sensibles).
- Toute captation non autorisée (ex. enregistrement sans consentement).



Avertir le service informatique
1017 ou 05 55 43 10 17



Ou nous contacter sur
informatique@ch-esquirol-limoges.fr