

Comment mettre en place une organisation de télétravail dans une entreprise de santé ?

Mettre en place une organisation de télétravail dans une entreprise du secteur de la santé nécessite une approche structurée et sécurisée pour garantir la confidentialité des données, la productivité des employés, et le maintien de la qualité des soins. Voici une démarche détaillée avec les outils adaptés pour une mise en place efficace :

1. Analyse des besoins et du cadre réglementaire

- **Évaluation des postes éligibles** : Tous les employés du secteur de la santé ne peuvent pas télétravailler. Par exemple, les médecins, infirmiers ou techniciens de laboratoire ont besoin de présence physique pour soigner les patients. Par contre, les fonctions administratives, gestion des dossiers, support client, IT, etc., peuvent être effectuées à distance.
- **Cadre réglementaire** : Le télétravail dans la santé implique la gestion de données médicales sensibles (données de santé, dossiers patients). Il faut se conformer aux lois et réglementations telles que le **RGPD (Règlement Général sur la Protection des Données)** en Europe ou la **HIPAA (Health Insurance Portability and Accountability Act)** aux États-Unis. Un Délégué à la Protection des Données (DPO) peut être impliqué pour garantir la conformité.
- **Charte de télétravail** : Définir des règles claires sur les droits et obligations des employés en télétravail (horaires, objectifs, etc.).

2. Mise en place des outils de communication et de collaboration

Pour maintenir la coordination et la communication entre les équipes :

- **Outils de messagerie instantanée et visioconférence** :
 - **Microsoft Teams** : Très utilisé dans le secteur de la santé, permet la collaboration avec des fonctions de chat, visioconférence, partage d'écran, et intégration avec les applications Office 365.
 - **Zoom** ou **Google Meet** : Pour les réunions en visioconférence, avec une attention particulière à la sécurisation des échanges (Zoom propose des options avancées pour chiffrer les communications).
- **Outils de gestion de projets** :
 - **Trello** ou **Asana** : Pour organiser et suivre les tâches et projets en équipe. Cela permet de centraliser les informations et d'avoir une vue claire de l'avancement des projets.
 - **Monday.com** : Spécifiquement utile pour le suivi des projets complexes avec des intégrations avancées.
- **Outils de stockage et partage de documents** :
 - **SharePoint** (intégré à Microsoft 365) ou **Google Drive** : Permettent un stockage sécurisé des documents avec gestion des accès et versionnement des fichiers.
 - **Dropbox Business** : Une autre option de stockage sécurisé avec des fonctionnalités de synchronisation en temps réel.

3. Sécurisation des accès et protection des données sensibles

La protection des données des patients et la confidentialité sont cruciales dans le secteur de la santé.

- **VPN (Virtual Private Network)** : Chaque employé doit utiliser un VPN pour se connecter aux ressources internes de l'entreprise. Cela permet de sécuriser les échanges de données, surtout lors de l'utilisation de réseaux non sécurisés.
- **Systèmes de chiffrement des données** : Utiliser des solutions comme **VeraCrypt** pour chiffrer les disques durs, ou encore **BitLocker** (pour Windows) pour sécuriser les postes de travail.
- **Authentification multi-facteurs (MFA)** : Implémenter une double authentification (MFA) pour tous les accès aux systèmes sensibles, afin de limiter les risques de piratage.
- **Logiciels spécialisés dans le stockage sécurisé des dossiers patients** : Des solutions comme **Cerner** ou **Epic** sont largement utilisées dans la gestion des données médicales et des dossiers patients avec des fonctions de télétravail.

4. Assurer la continuité des soins et la gestion des dossiers médicaux

- **Téléconsultation** : Intégrer des outils comme **Doctolib** (en Europe) ou **Amwell** (aux États-Unis) pour permettre aux médecins de réaliser des consultations à distance, en respectant la confidentialité et la qualité des soins.
- **Dossiers patients électroniques (DPE)** : L'utilisation de systèmes de dossiers électroniques accessibles à distance, comme **Meditech** ou **Allscripts**, permet aux professionnels de santé de consulter et de mettre à jour les informations des patients, tout en garantissant la sécurité.

5. Formation et accompagnement des équipes

- **Formations sur les outils numériques** : Les employés doivent être formés à l'utilisation des nouveaux outils de communication, collaboration et gestion des données. Organiser des sessions de formation à distance pour assurer que chacun est à l'aise avec les outils technologiques.
- **Sensibilisation à la cybersécurité** : Former les employés à reconnaître les cyberattaques (phishing, ransomwares, etc.) et à adopter des bonnes pratiques (mots de passe forts, utilisation de VPN, etc.).

6. Suivi de la performance et bien-être des employés

- **Outils de suivi de la productivité** :
 - **Time Doctor** ou **Hubstaff** : Ces logiciels permettent de suivre les heures de travail et les activités des employés tout en respectant leur vie privée.
- **Enquêtes sur le bien-être** : Mettre en place des outils comme **Officevibe** pour surveiller le bien-être des employés en télétravail, identifier les problèmes potentiels et prendre des mesures pour améliorer leur expérience.

- **Politique de déconnexion** : Définir des limites claires sur les horaires de travail pour éviter le burnout des employés.

7. Évaluation continue et adaptation

- **Retour d'expérience des employés** : Organiser des réunions régulières pour recueillir les retours des employés sur l'organisation du télétravail et apporter les ajustements nécessaires.
- **Mise à jour des outils et technologies** : Il est essentiel d'être en veille sur les nouvelles technologies et les nouvelles réglementations afin d'adapter les outils en fonction des besoins de l'entreprise et des évolutions légales.

Conclusion

Cas d'usage

Le télétravail dans le secteur de la santé doit être structuré autour d'outils de collaboration sécurisés, d'une politique de protection des données strictes, et d'une gestion efficace des ressources humaines. La clé du succès réside dans l'équilibre entre la flexibilité offerte par le télétravail et la rigueur imposée par le cadre de sécurité et de confidentialité dans lequel opère le secteur de la santé.

Le CHU d'Amiens-Picardie a intégré le télétravail pour plusieurs catégories d'employés. Les services concernés incluent notamment les métiers administratifs, la gestion des ressources humaines, ainsi que des fonctions liées à l'informatique et à la documentation médicale. L'hôpital a mis en place des outils spécifiques comme des connexions sécurisées via VPN et des plateformes de gestion électronique de documents. Cette transition a permis de réduire certains coûts, notamment ceux liés à l'infrastructure physique et à la gestion des bureaux (Weka).

Les Hôpitaux Universitaires de Strasbourg (HUS) ont également développé une politique de télétravail pour certaines fonctions administratives ainsi que pour les professionnels de santé réalisant de la téléconsultation. Pendant la crise sanitaire, des investissements ont été réalisés pour permettre à des médecins de continuer à consulter à distance. Le coût principal a été lié à l'acquisition d'équipements informatiques et de logiciels de téléconsultation, ainsi qu'à la formation des personnels concernés (FHF).

From:

<https://wiki.ox2.fr/> - Ox2

Permanent link:

<https://wiki.ox2.fr/doku.php?id=cesi:grandoral:benchmark:mobilite>

Last update: **2024/09/16 10:33**

