#### Déclaration de confidentialité et de protection de la vie privée

**Informations fournies par l'employé(e)**

|  |  |  |  |
| --- | --- | --- | --- |
| Nom |  | Prénom |  |
| Date de naissance |  | Département |  |
| Employeur*(veuillez cocher)* | [ ]  ☐ [ ]  ☐ [ ]  ☐ [ ]  ☐  | [ ]  ☐ [ ]  ☐ [ ]  ☐ [ ]  ☐ (z.B extern) |

**Grâce à mon travail, j'acquière des connaissances**

1. dans les affaires de nature confidentielle, et
2. dans les données personnelles des clients, des patients et des employés

Je suis conscient que toutes les personnes concernées ont le droit de : l'*information*, *l'accès*,  *la rectification*, l'*effacement* et la *divulgation* de vos données personnelles .

**Enquêtes de tiers**

Les patients ont généralement le droit d'obtenir des informations sur leurs antécédents médicaux. Dans la plupart des cas, les employés sont confrontés à la question de la protection des données lorsque des tiers ont des demandes de données personnelles.

1. En principe,  **il faut faire preuve**  de prudence et ne pas donner d'informations directes !

Dans le cas **de** simples questions verbales ou téléphoniques de la part de tiers *(par exemple, « Mon père a-t-il bien supporté la thérapie ? », « Mme Smith est-elle toujours employée par vous ? »)* S' applique:

1. Je m'assure que la tierce personne est connue de moi et que cette information est autorisée.
2. Je demande à la personne qui fait la demande de me donner le nom complet et une autre caractéristique (par exemple, la date de naissance du patient) afin de l'identifier correctement.
3. Si l'identité du tiers ou sa relation avec la personne dont les données sont demandées n'est pas claire, je demande au tiers d'adresser sa demande par écrit au conseiller en protection des données (datenschutz@rehaklinik-zihlschlacht.ch ).

Dans le cas  **d'enquêtes complexes** de la part de nos patients eux-mêmes ou de tiers, ce qui suit s'applique :

1. Dans tous les cas, cela doit être soumis par écrit au conseiller en protection des données.
2. J'informe mon superviseur de la demande.
3. Ce n'est qu'en coordination avec le conseiller à la protection des données que des données précieuses ou très sensibles seront divulguées.

**Autres aspects de la protection des données**

Je suis conscient que

1. Non seulement moi-même, mais aussi les clients, les patients et les employés ont le droit de voir leurs données personnelles traitées de manière confidentielle
2. Vamed Schweiz AG attache une grande importance au respect de la protection des données et des secrets d'affaires.
3. le devoir de protection des données est stipulé par le secret professionnel conformément à l'article 35 de la loi Informatique et Libertés, ou le secret médical conformément à l'article 321 du Code pénal.

**Je m'engage à**

1. Lisez le [concept de protection des données](https://rzs.quam.vamedarea.com/Downloadcenter/Datenschutz%20Konzept.docx) et les informations sur la protection des données européennes ([fiche d'information EU-GDPR tous les employés](https://rzs.quam.vamedarea.com/Downloadcenter/Infoblatt%20EU-DSGVO%20alle%20Mitarbeiter.pdf)), qui sont stockées dans le « QUAM Document Management/ Topic : Security, » et respectez les règles
2. pour ne consulter que ces documents et obtenir les informations dont j'ai besoin pour mon travail.
3. Pour transmettre des connaissances / informations à d'autres employés de l'entreprise qui en ont besoin pour leur travail.
4. Garder le secret sur toutes les perceptions, quelle qu'en soit la nature, que j'ai en relation avec mon travail envers des tiers non autorisés pendant et après la fin de la relation de travail ou de l'activité de conseil.
5. Dans les salles publiques de la clinique (par exemple, café dans le parc, restaurant du personnel, réception, couloirs, salons) pour ne pas parler des patients, des incidents et/ou des expériences des patients, des antécédents médicaux, etc., où d'autres personnes peuvent écouter.

**Sécurité des données en informatique et en général**

Je m'engage à

1. Lorsque je quitte mon espace de travail, je prends les mesures nécessaires pour empêcher les personnes non autorisées de consulter et d'accéder à des données ou à d'autres appareils (par exemple, un ordinateur portable) (par exemple, verrouiller la porte / verrouiller le PC) Même lorsque je travaille à domicile
2. ne pas partager ou écrire mon mot de passe personnel à qui que ce soit
3. ne pas installer de logiciel à moins d'avoir les autorisations d'administrateur nécessaires et d'être autorisé à le faire.
4. Enregistrez les données uniquement sur les lecteurs réseau.
5. Aucune donnée à stocker sur le disque local
6. N'ouvrir les e-mails que si leur origine est connue.
7. Les supports de données externes (par ex. clé USB, disques durs, CD-DVD) ne doivent être utilisés qu'avec l'autorisation du service TIC
8. gérer le téléphone, le fax, l'e-mail et Internet uniquement conformément aux règles de conduite du concept de protection des données
9. Pour éliminer les fichiers et les données contenant des données personnelles uniquement dans les conteneurs/emplacements étiquetés désignés.

**Je déclare avoir lu, compris et respecté les dispositions susmentionnées.**

|  |  |
| --- | --- |
| Date |  |
| Signature Employé |  |