MESURES TECHNIQUES ET ORGANISATIONNELLES SELON LPD/OPD

Le présent document offre une vue d'ensemble des mesures techniques et organisationnelles de la protection des données (MTO) de Health Info Net AG. Les obligations légales découlent de la loi fédérale suisse sur la protection des données (LPD) et de l'ordonnance y afférente (OPD), en particulier des articles 7 et 8 LPD et de l'article 3 OPD.

Les mesures couvrent les besoins de protection normaux et élevés et concernent les données personnelles ainsi que les données personnelles sensibles. Si le traitement de données personnelles sensibles entraîne d'autres risques après la mise en œuvre des MTO, une évaluation des risques est effectuée afin de déterminer les mesures supplémentaires qui s'imposent.

Le tableau suivant présente les exigences découlant de l'ordonnance sur la protection des données, les mesures prises par HIN et les exigences correspondantes de la certification selon ISO/IEC 27001. Ce tableau sert aux clients de HIN – en complément de la déclaration de protection des données et des contrats-cadres – de preuve des mesures prises; il en va de même dans la relation entre HIN et ses fournisseurs, c'est pourquoi les accords de sous-traitance (AST) avec les fournisseurs y font référence.

Art. 3 OPD	**Brève description et mise en œuvre chez HIN**	**Exigences référencées ISO/IEC 27001:2017[1]**	**Exigences référencées ISO/IEC 27001:2022[2]**
1 Afin de garantir la **confidentialité** , le **responsable** et le **sous-traitant** doivent prendre des mesures appropriées pour que: a. les personnes autorisées aient accès uniquement aux données personnelles dont elles ont besoin pour accomplir leurs tâches **(contrôle d'accès**);	le contrôle d'accès comprend des mesures organisationnelles et techniques visant à garantir que seuls les utilisateurs authentifiés et autorisés peuvent accéder aux données et que les données à caractère personnel sont protégées contre tout accès non autorisé. Cela concerne aussi bien les serveurs, les bases de données, le stockage, les sauvegardes et les systèmes de réseau dans nos	A.6.1.2 Séparation des tâches A.6.2 Appareils mobiles et télétravail A.7.2.2 Sensibilisation, éducation et formation à	A.5.3 Séparation des tâches A.5.12 Classification des informations A.5.15 Gestion des accès A.5.16 Gestion des identités

	centres de données que les systèmes Client au bureau et en déplacement. Cela requiert notamment des directives appropriées, des responsabilités clairement définies, une identification univoque, une authentification forte, des processus pour l'obtention, la mutation et le retrait de droits d'accès, un accès à distance sécurisé, une journalisation, des formations initiales et récurrentes de sensibilisation à la sécurité et des contrôles/audits périodiques.	la sécurité de l'information A.8.2 Classification des informations A.9.1 Exigences commerciales liées à la gestion des accès A.9.2 Gestion des accès utilisateurs A.9.3 Responsabilités des utilisateurs A.9.4 Gestion des accès aux systèmes et applications A.12.4 Journalisation et surveillance	A.5.17 Données d'authentification A.5.18 Droits d'accès A.5.34 Protection des données et des données à caractère personnel (DCP) A.6.3 Sensibilisation, éducation et formation à la sécurité de l'information A.6.7 Travail à distance A.8.2 Droits d'accès privilégiés A.8.15 Journalisation
b. seules les personnes autorisées aient accès aux locaux et aux installations dans lesquels sont traitées des données personnelles **(contrôle d'accès**);	Le contrôle d'accès comprend des mesures organisationnelles et techniques visant à protéger les systèmes de traitement des données contre les utilisateurs non autorisés. Cela concerne aussi bien les serveurs, les bases de données, le stockage, les sauvegardes et les systèmes de réseau dans nos centres de données que les systèmes Client au bureau et en déplacement. Cela requiert notamment des directives appropriées, des responsabilités clairement définies, une identification univoque, des processus pour l'obtention, la mutation et le retrait de droits d'accès, des zones physiques, des systèmes de fermeture et d'accès sûrs, des armoires verrouillées pour les données personnelles physiques, l'accompagnement des visiteurs, une journalisation, des formations initiales et récurrentes de sensibilisation à la sécurité et des contrôles/audits périodiques.	A.6.1.2 Séparation des tâches A.7.2.2 Sensibilisation, éducation et formation à la sécurité de l'information A.8.2 Classification des informations A.9.1 Exigences commerciales liées à la gestion des accès A.11.1 Zones de sécurité A.12.4 Journalisation et surveillance	A.5.3 Séparation des tâches A.5.12 Classification des informations A.5.34 Protection des données et des données à caractère personnel (DCP) A.6.3 Sensibilisation, éducation et formation à la sécurité de l'information A.7.1 Périmètres de sécurité physique A.7.2 Accès physique A.7.3 Sécurisation des bureaux, locaux et installations

			A.7.4 Contrôle de sécurité physique A.8.15 Journalisation
c. que les personnes non autorisées ne puissent pas utiliser les systèmes de traitement automatisé de données à l'aide d'appareils de transmission de données **(contrôle des utilisateurs**).	Le contrôle des utilisateurs comprend des mesures organisationnelles et techniques qui garantissent que seules les personnes autorisées à le faire peuvent traiter des données. Cela requiert des mesures de contrôle d'accès.	Voir Contrôle d'accès.	Voir Contrôle d'accès.
2 Afin de garantir la **disponibilité** et **l'intégrité** , le **responsable** et le **sous-traitant** doivent prendre des mesures appropriées pour que: a. les personnes non autorisées ne puissent pas lire, copier, modifier, déplacer, supprimer ou détruire des supports de données **(contrôle des supports de données**);	Le contrôle des supports de données comprend des mesures organisationnelles et techniques visant à protéger les données enregistrées (Data at Rest). Cela concerne aussi bien les serveurs, les bases de données, le stockage, les sauvegardes et les systèmes de réseau dans nos centres de données que les systèmes Client au bureau et en déplacement. Cela requiert notamment des directives appropriées, des responsabilités clairement définies, une gestion d'actifs, le cryptage des supports de données, des processus de suppression ou de destruction lorsque la finalité n'est plus d'actualité, une journalisation, des formations initiales et récurrentes de sensibilisation à la sécurité et des contrôles/audits périodiques.	A.7.2.2 Sensibilisation, éducation et formation à la sécurité de l'information A.8.1 Responsabilité en ce qui concerne les valeurs A.8.2 Classification des informations A.8.3 Manipulation des supports de données A.11.2.6 Sécurité des appareils, équipements et valeurs à l'extérieur des locaux A.11.2.7 Élimination ou réutilisation sécurisée d'appareils et d'équipements A.12.4 Journalisation et surveillance	A.5.9 Inventaire des informations et des autres valeurs associées A.5.12 Classification des informations A.5.34 Protection des données et des données à caractère personnel (DCP) A.6.3 Sensibilisation, éducation et formation à la sécurité de l'information A.7.10 Supports de stockage A.7.14 Élimination ou réutilisation sécurisée d'appareils et d'équipements A.8.10 Suppression d'informations A.8.12 Prévention des fuites de données A.8.15 Journalisation
b. les personnes non autorisées ne puissent pas enregistrer, lire, modifier, supprimer ou détruire	Le contrôle des mémoires comprend des mesures organisationnelles et techniques visant à protéger les données dans des mémoires volatiles (Data in Use). Cela concerne	Voir Intégrité des données.	Voir Intégrité des données.

des données personnelles dans des mémoires **(contrôle des mémoires**);	aussi bien les serveurs, les bases de données, le stockage, les sauvegardes et les systèmes de réseau dans nos centres de données que les systèmes Client au bureau et en déplacement. Cela requiert des mesures de maintien de l'intégrité des données.		
c. les personnes non autorisées ne puissent pas enregistrer, lire, modifier, supprimer ou détruire des données personnelles lors de la communication de données personnelles ou du transport de supports de données **(contrôle du transport**);	Le contrôle de la transmission et du transport comprend des mesures organisationnelles et techniques visant à protéger les données lors du transport logique et physique (Data in Transit). Cela concerne aussi bien les serveurs, les bases de données, le stockage, les sauvegardes et les systèmes de réseau dans nos centres de données que les systèmes Client au bureau et en déplacement. Cela requiert notamment des directives appropriées, des responsabilités clairement définies, des émetteurs et destinataires authentifiés, un transport crypté, une journalisation, des formations initiales et récurrentes de sensibilisation à la sécurité et des contrôles/audits périodiques.	A.7.2.2 Sensibilisation, éducation et formation à la sécurité de l'information A.8.1 Responsabilité en ce qui concerne les valeurs A.8.2 Classification des informations A.8.3 Manipulation des supports de données A.10.1 Mesures cryptographiques A.11.2.6 Sécurité des appareils, équipements et valeurs à l'extérieur des locaux A.12.4 Journalisation et surveillance A.13.2 Transfert d'informations A.12.4 Journalisation et surveillance	A.5.9 Inventaire des informations et des autres valeurs associées A.5.12 Classification des informations A.5.14 Transmission d'informations A.5.34 Protection des données et des données à caractère personnel (DCP) A.6.3 Sensibilisation, éducation et formation à la sécurité de l'information A.7.14 Élimination ou réutilisation sécurisée d'appareils et d'équipements A.8.10 Suppression d'informations A.8.12 Prévention des fuites de données A.8.15 Journalisation A.8.24 Utilisation de la cryptographie
d. la disponibilité des données personnelles et l'accès à celles-ci puissent être rapidement	La disponibilité comprend des mesures organisationnelles et techniques visant à protéger les données contre toute	A.8.2 Classification des informations	A.5.12 Classification des informations

restaurés en cas d'incident physique ou technique **(restauration);**	perte. Cela concerne aussi bien les serveurs, les bases de données, le stockage, les sauvegardes et les systèmes de réseau dans nos centres de données que les systèmes Client au bureau et en déplacement. Cela requiert notamment des directives appropriées, des responsabilités clairement définies, une alimentation électrique sans interruption, des systèmes redondants, des sauvegardes régulières, des tests de restauration périodiques, des plans d'urgence et des audits.	A.12.3 Sauvegarde des données A.17.1 Préservation de la sécurité de l'information A.17.2 Redondances A.12.4 Journalisation et surveillance	A.5.30 Disponibilité des TIC pour la continuité des activités A.8.13 Sauvegarde des informations A.8.14 Redondance d'équipements de traitement des informations A.8.15 Journalisation
e. toutes les fonctions du système de traitement automatisé des données soient disponibles (disponibilité), les dysfonctionnements soient signalés (fiabilité) et les données personnelles enregistrées ne puissent pas être endommagées par des dysfonctionnements du système **(intégrité des données**);	L'intégrité comprend des mesures organisationnelles et techniques visant à garantir l'exactitude et l'exhaustivité des données. Cela concerne aussi bien les serveurs, les bases de données, le stockage, les sauvegardes et les systèmes de réseau dans nos centres de données que les systèmes Client au bureau et en déplacement. Cela requiert notamment des directives appropriées, des responsabilités clairement définies, la prise en compte d'exigences de sécurité dans le développement et l'exploitation, la segmentation de réseaux et de mémoires de données, un durcissement du système, une gestion des vulnérabilités, une protection contre les logiciels malveillants, une surveillance, une journalisation, des formations initiales et récurrentes de sensibilisation à la sécurité et des contrôles/audits périodiques.	A.7.2.2 Sensibilisation, éducation et formation à la sécurité de l'information A.8.2 Classification des informations A.12.1 Processus et responsabilités opérationnels A.12.2 Protection contre les logiciels malveillants A.12.4 Journalisation et surveillance A.14.1 Exigences de sécurité applicables aux systèmes d'information A.14.2 Sécurité des processus de développement et de soutien A.18.1.3 Protection des enregistrements	A.5.12 Classification des informations A.5.33 Protection des enregistrements A.5.34 Protection des données et des données à caractère personnel (DCP) A.5.37 Processus opérationnels documentés A.6.3 Sensibilisation, éducation et formation à la sécurité de l'information A.8.9 Gestion des configurations A.8.15 Journalisation A.8.32 Gestion des modifications
f. les systèmes d'exploitation et les logiciels d'application soient constamment maintenus à jour	La sécurité des systèmes comprend tous les aspects opérationnels de la sécurité. Cela concerne aussi bien les	Voir Contrôle d'accès et de l'utilisation, Contrôle	Voir Contrôle d'accès et de l'utilisation, Contrôle

en matière de sécurité et que les lacunes critiques connues soient comblées **(sécurité des systèmes**).	serveurs, les bases de données, le stockage, les sauvegardes et les systèmes de réseau dans nos centres de données que les systèmes Client au bureau et en déplacement. Cela requiert des mesures de contrôle d'accès et de l'utilisation, des mesures de contrôle des supports de données, des mémoires et du transport, ainsi que des mesures de maintien de la disponibilité et de l'intégrité.	des supports de données, Contrôle des mémoires et du transport, ainsi que Disponibilité et Intégrité.	des supports de données, Contrôle des mémoires et du transport, ainsi que Disponibilité et Intégrité.
3 Afin de garantir la **traçabilité** , le **responsable** et le **sous-traitant** doivent prendre des mesures appropriées pour pouvoir: a. vérifier quelles données personnelles sont saisies ou modifiées dans le système de traitement automatisé des données, à quel moment et par quelle personne **(contrôle des saisies**);	Le contrôle des saisies comprend des mesures organisationnelles et techniques visant à garantir la traçabilité des traitements de données, c-à-d. la saisie, le stockage, la modification, la transmission, la sauvegarde, l'archivage et la suppression. Cela requiert notamment des directives appropriées, des responsabilités clairement définies, un registre des traitements de données, une surveillance, une journalisation, des formations initiales et récurrentes de sensibilisation à la sécurité et des contrôles/audits périodiques.	A.7.2.2 Sensibilisation, éducation et formation à la sécurité de l'information A.8.1 Responsabilité en ce qui concerne les valeurs A.8.2 Classification des informations A.12.4 Journalisation et surveillance A.18.1.3 Protection des enregistrements	A.5.9 Inventaire des informations et des autres valeurs associées A.5.12 Classification des informations A.5.33 Protection des enregistrements A.5.34 Protection des données et des données à caractère personnel (DCP) A.6.3 Sensibilisation, éducation et formation à la sécurité de l'information A.8.15 Journalisation A.8.16 Surveillance des activités
b. vérifier à qui des données personnelles sont communiquées à l'aide d'appareils de transmission de données **(contrôle des communications**);	Le contrôle des communications comprend des mesures organisationnelles et techniques visant à garantir la traçabilité des traitements de données, c-à-d. la saisie, le stockage, la modification, la transmission, la sauvegarde, l'archivage et la suppression. Cela requiert des mesures de contrôle d'accès, de contrôle du transport et de contrôle des saisies.	Voir Contrôle d'accès, Contrôle du transport et Contrôle des saisies.	Voir Contrôle d'accès, Contrôle du transport et Contrôle des saisies.

c. détecter rapidement les violations de la sécurité des données **(détection**) et prendre des mesures afin d'en atténuer ou d'en éliminer les conséquences **(élimination**).	La détection et l'élimination comprennent des mesures organisationnelles et techniques visant à détecter, analyser, évaluer, traiter et communiquer les violations potentielles et réelles de la sécurité des données. Cela requiert notamment des directives appropriées, des responsabilités clairement définies, l'obligation de signaler les risques et incidents de sécurité, un contact avec les autorités, des formations initiales et récurrentes de sensibilisation à la sécurité et des contrôles/audits périodiques.	A.6.1.3 Contact avec les autorités A.7.2.2 Sensibilisation, éducation et formation à la sécurité de l'information A.7.2.3 Processus disciplinaire A.16.1 Gestion des incidents et améliorations de la sécurité des informations	A.5.24 Planification et préparation de la gestion des incidents de sécurité de l'information A.5.25 Évaluation et décision sur les événements liés à la sécurité de l'information A.5.26 Réponse aux incidents de sécurité de l'information A.5.27 Enseignements tirés des incidents de sécurité de l'information A.5.28 Collecte de preuves A.5.33 Protection des enregistrements A.5.34 Protection des données et des données à caractère personnel (DCP) A.6.3 Sensibilisation, éducation et formation à la sécurité de l'information A.6.4 Processus disciplinaire

[1] d'ici octobre 2025 au plus tard
[2] à partir d'octobre 2025 au plus tard