CURAVIVA.CH

VERBAND HEIME UND INSTITUTIONEN SCHWEIZ
ASSOCIATION DES HOMES ET INSTITUTIONS SOCIALES SUISSES
ASSOCIAZIONE DEGLI ISTITUTI SOCIALI E DI CURA SVIZZERI
ASSOCIAZIUN DALS INSTITUTS SOCIALS E DA TGIRA SVIZZERS

PROTECTION DES DONNÉES DANS LES EMS

DIRECTIVE CONCERNANT LE TRAITEMENT DES DONNÉES SUR LES RÉSIDENTS
RESPONSABLE: DS PERSONNES ÂGÉES
VERSION – MAI 2013

CURAVIVA Suisse
Zieglerstrasse 53
3000 Berne 14
Tél. +41 (0)31 385 33 33
www.curaviva.ch
info@curaviva.ch

But
Assurer la protection des données et la sécurité des données est important pour la protection des résidentes et des résidents au sujet desquels des données sont acquises, traitées, conservées et transmises. Le présent document contient des directives qui montrent au responsable d'un home et à leurs collaborateurs le comportement à adopter et les précautions à prendre pour assurer une utilisation des données sur les résidents conforme à la protection des données.

Les directives prennent en compte les principales exigences du droit sur la protection des données, importantes au quotidien dans un home. Elles se basent sur la loi fédérale sur la protection des données (19.6.1992) et sur l'ordonnance relative à la loi fédérale (14 juin 1993). Pour certains aspects, il est tenu compte de la loi sur la protection des données sur les résidents (6.6.1993, *Gesetz über den Schutz von Bewohnerdaten*) et de l'ordonnance sur la sécurité informatique (17.12.1997, *Informatiksicherheitsverordnung*) du canton de Zurich. S'y ajoutent les directives de l'arrêt du Tribunal fédéral LAMal du 21 mars 2007 (K12/06) «Edition de données sensibles».

Champ d'application
En règle générale, les directives s'appliquent à tous les homes de droit public ou privé dans le domaine des soins stationnaires. Pour les homes dont le statut juridique relève du droit public, il peut exister des dispositions supplémentaires au niveau cantonal et communal, qu'il s'agisse par ex. d'une ordonnance cantonale du droit des patients, ou d'instructions de la direction de la santé sur l'accès aux dossiers de résidents par leurs proches, etc. Ces dispositions **ne sont pas** prises en compte individuellement dans les explications qui suivent, mais les homes de droit public sont tenus de se conformer à ces dispositions supplémentaires.

Bases de la protection des données
La loi fédérale sur la protection des données vise à protéger la personnalité et les droits fondamentaux des personnes qui font l'objet d'un traitement des données. Dans ce cadre, les principes suivants doivent être respectés :

- *Les données sur les résidents doivent être obtenues légalement.*
- *Leur traitement doit respecter le principe de la bonne foi et le principe de la proportionnalité.*
- *Les données sur les résidents doivent être traitées uniquement dans le but qui a été indiqué lors de leur obtention, qui apparaît comme évident dans de telles circonstances ou qui est prévu par la loi.*

Les principes juridiques s'appliquent indépendamment des procédures et des moyens mis en œuvre, donc indépendamment du fait que les données sur les résidents soient traitées manuellement ou par un logiciel du home.

La notion de **traitement** des données sur les résidents recouvre les activités d'obtention, d'utilisation, de remaniement, de modification, de conservation, de transmission et de destruction de données personnelles sur des résidentes et résidents.

Responsabilité
La garantie de la protection des données relève de la responsabilité de l'institution qui traite ou fait traiter les données sur les résidents dans le cadre de ses prestations de service.
Par conséquent, la direction du home est responsable de l'application des dispositions fédérales et cantonales sur la protection des données et de leur utilisation au sein du home.

Principe de proportionnalité

Le principe de proportionnalité implique que seules les données sur les résidents du home qui sont nécessaires à la prise en charge des résidents et aux tâches administratives afférentes, peuvent être collectées et traitées.

Ce principe signifie qu'une collaboratrice (ou un collaborateur) du home n'est en droit de traiter que les données qui lui sont objectivement nécessaire dans un but déterminé et que l'atteinte à la personnalité soit raisonnable par rapport au but de ce traitement des données. Par conséquent, les droits d'accès aux données sur les résidents enregistrées sous forme électroniques doivent être attribués de telle manière que chacun ne puisse accéder qu'aux données nécessaires pour exécuter son travail effectif. Cela s'applique aussi à la transmission des données sur les résidents.

Le principe de proportionnalité implique aussi que les données sur les résidents ne peuvent pas être conservées sans limite de temps, mais au plus aussi longtemps que c'est nécessaire à la prise en charge des résidents et aux tâches administratives afférentes.

Principe de finalité

Les données sur les résidents doivent être traitées uniquement dans le but qui a été indiqué lors de leur obtention, ou qui apparaît comme évident dans de telles circonstances ou encore, qui est prévu par la loi. Les données sur les résidents ne doivent pas être traitées d'une manière contraire au principe de la bonne foi, soit d'une manière à laquelle la résidente ou le résident ne pouvait pas s'attendre et à laquelle il/elle se serait opposé(e). Il est interdit d'obtenir des données secrètement. De ce fait, le principe de la bonne foi implique aussi que le traitement des données sur les résidents doit avoir lieu de manière transparente pour les résidents concernés. Il doit être reconnaissable pour la personne concernée.
Les systèmes informatiques modernes permettent des utilisations multifonctionnelles. Les résidents concernés par le traitement informatique de leurs données sont en droit de savoir dans quel but elles sont utilisées. Pour pouvoir utiliser les données à d'autres fins que celles communiquées, le consentement de la personne concernée doit être obtenu.

Droits des résidentes et des résidents (résidents)

Les résidents, le cas échéant leur représentant légal, sont en droit d'obtenir des informations complètes sur leurs droits en relation avec leurs données personnelles au sein du home.

- **Droit à l'information.**
  Les résidentes et résidents doivent obtenir des informations concrètes sur les données la concernant et le but dans lequel elles sont récoltées, traitées, conservées et transmises à des tiers et que cela se fait sur papier et principalement par voie électronique.

- **Droit de consulter.**
  Les résidentes et résidents sont en droit de consulter ses données/dossier de résident en tout temps, pour en vérifier l'exactitude et elle est en droit d'en exiger la rectification. (Principe de l'intégrité des données)

- **Procurations**
  Les résidentes et résidents sont en droit de donner une procuration à un tiers (par ex. un proche) afin qu'il puisse consulter les données de la résidente. Elle est en droit de révoquer en tout temps une telle procuration.

Obligations des responsables d'un home

- Les responsables d'un home sont tenus d'informer les résidentes et résidents sur ses droits au moment de son entrée ou lors de l'introduction d'applications informatiques.

- Une procuration de résident (octroi de procurations) doit être réglée avec la résidentes ou le résident

- Le complément au contrat de pensionnaire doit être intégré au contrat de pensionnaire ordinaire ou il doit être signé par la résidente ou le résident s'il prend la forme d'une annexe à ce contrat. Le consentement éclairé de la résidente ou du résident est nécessaire à la conclusion du complément au contrat de pensionnaire. Un refus de le signer doit, le cas échéant, être consigné par écrit.

Utilisation des données sur les résidentes et résidents

Dans les homes, ce sont principalement des données personnelles qui sont traitées. Les données sur les résidentes et résidents sont éminemment dignes de protection, à traiter de manière **confidentielle**, à conserver **soigneusement** et à **protéger** des tiers.

- **Protection contre des accès non autorisés**
  - Les données sur les résidentes et résidents consignées sur papier (documents de soin, dossier) doivent être protégées contre tout accès non autorisé par des tiers au moyen de mesures matérielles appropriées (par ex. serrure).
  - L'accès aux données électroniques sur les résidents doit être restreint aux seules personnes autorisées du home par une réglementation stricte des mots de passe. Le cercle des personnes autorisées doit être aussi restreint que possible, en se basant sur l'organisation interne du travail dans le home.

- **Conservation et archivage des données sur les résidents**
  Les données sur les résidentes et résidents sont conservées dans les archives, sous forme papier ou électronique, pendant 10 ans à partir du moment de la sortie de la résidente ou du résident, puis elles sont détruites. Les mêmes directives s'appliquent aux archives.

- **Consultation de ses propres données par la résidente ou le résident**
  Les responsables d'un home doivent garantir à la résidente ou au résident le droit de consulter ses données conservées. Pour divulguer et s'entretenir au sujet de données médicales sensibles, il faut faire, au vu de la situation, appel à un médecin.

- **Consultation de données médicales sur les résidentes et résidents par l'équipe soignante**
  La direction d'un home est en droit de transmettre les données médicales pertinentes à l'équipe soignante. Le médecin traitant se conforme aux instructions données par la résidente ou le résident (contrat de soin-pensionnaire).

- **Consultation de données sur les résidentes et résidents par des tiers**
  Les tiers ne peuvent être autorisés à consulter les données sur les résidentes et résidents que s'ils disposent d'une procuration donnée par la résidente ou le résident.

- **Consultation de données sur les résidentes et résidents par des proches**
  Le droit ne définit pas la notion de «proche». De ce fait, les proches sont assimilés à des «tiers». Une procuration écrite n'est pas nécessaire si les proches consultent les données sur la résidente ou le résident en sa présence.

- **Transmission à l'assureur des documents sur les besoins en soins et sur le décompte de prestations**
  L'assureur n'a le droit d'obtenir que le formulaire de saisie et les documents qui ont fait l'objet d'un accord avec la section CURAVIVA concernée dans le cadre des contrats tarifaires cantonaux. La divulgation de ces informations est obligatoire pour le remboursement par les assureurs des prestations de soin relevant de la LAMal.

- **Vérification de l'obligation de prise en charge par les assureurs**
  Afin de vérifier leur obligation de prise en charge, les assureurs sont en droit de consulter les résultats de l'instrument de clarification des besoins et le diagnostic médical pour autant que ce diagnostic médical fasse partie des données traitées au sujet de la résidente ou du résident.

  Les responsables d'un home sont tenus d'autoriser l'assureur à consulter, en cas de vérification de la facturation adressée à l'assureur ainsi que lors du contrôle ou de désaccord au sujet du classement sur l'échelle de soin, toutes les données personnelles de la résidente ou du résident, même celles considérées comme sensibles, notamment le rapport de soins, la planification standardisées des soins, la surveillance des signes vitaux et les plans thérapeutiques individuels.

  Afin de procéder à la consultation, l'assureur doit s'engager, après en avoir été informé, à traiter les données de manière confidentielle et à s'assurer de la sécurité des données conservées en interne chez l'assureur et à ne les rendre accessibles qu'aux personnes en charge du traitement du cas. De plus, l'assureur doit s'engager à ne pas utiliser les dossiers confidentiels qu'il a consultés dans le cadre de l'assurance de base, dans celui des assurances complémentaires.

  La direction d'un home est autorisée à procéder à la remise des dossiers au médecin conseil de l'assureur seulement et exclusivement sur la base d'instructions écrites en ce sens de la part de la résidente ou du résident.

- **Surveillance du canton**
  Dans le cadre de sa surveillance des soins et de l'assistance, le canton peut consulter tous les documents des résidentes et résidents. Ce droit ne peut être exercé que par les personnes titulaires d'une autorisation émanant de l'office compétent dans le domaine des soins et de l'assistance aux personnes âgées, soit du médecin cantonal.

- **Transmission de données sur les résidentes et résidents pour les demandes de prestations complémentaires**
  Le certificat des besoins en soins (=documents pour les assureurs) peut être transmis en cas de demande de prestations complémentaires et d'assistant(e)s en soin à l'office compétent, à savoir au service communal compétent.

- **Changement de home**
  En cas de départ dans un autre home, les données ne sont transmises qu'avec le consentement de la résidente ou du résident. Pour le home, le mieux est de remettre à la résidente ou au résident les documents avec le rapport de soins et de la ou le laisser libre de remettre ces documents ou non. Le consentement de la résidente ou du résident est aussi nécessaire pour la transmission de données électroniques. L'échange des données personnelles entre homes au sein d'une association des homes doit se faire, et être réglé, de manière transparente pour la résidente ou le résident.

- **Transmission de données électroniques sur les résidentes et résidents**
  Les données électroniques ne peuvent quitter le home que si elles ont été rendues complètement anonymes et que le but est clairement annoncé. Cela s'applique par exemple dans le cadre d'évaluations statistiques portant sur le calcul des indices de qualité auprès des homes.

Mesures techniques et organisationnelles

Les responsables d'un home doivent s'assurer qu'au cours du traitement de données sur les résidentes et résidents, la confidentialité, la disponibilité et l'exactitude des données sur les résidentes et résidents soient garanties par des mesures organisationnelles et techniques. Cette règle s'applique aussi bien si le traitement des données sur les résidentes et résidents est effectué sur papier que par informatique.

Les données sur les résidentes et résidents traitées au sein du home sont éminemment dignes de protection et, de ce fait, le risque pour les résidentes et résidents concernés est élevé. Les mesures techniques et organisationnelles doivent être appropriées et proportionnelles à l'importance des risques auxquels la résidente ou le résident et le home seraient exposés en cas d'utilisation abusive des informations.

- **Instructions au personnel**
  Le personnel doit être informé et instruit au sujet de la signification de la protection des données, des directives sur la protection des données et des dispositions spécifiques et des mesures de protection prises au sein du home.
- **Confidentialité**
  Le respect des dispositions légales et contractuelles sur la confidentialité et la protection des données doit être confirmé par écrit par le personnel.
- **Confidentialité imposée aux tiers**
  Les administrateurs système externes ainsi que les personnes et organisations externes qui traitent des données sur les résidentes et résidents sur mandat du home, sont tenues de conclure une convention de confidentialité qui doit prévoir une peine conventionnelle sanctionnant les violations.
- **Protection contre des accès physiques non autorisés**
  Les données sur les résidentes et résidents consignées sur papier (documents de soin, dossier) doivent être protégées contre tout accès non autorisé par des tiers au moyen de mesures matérielles (appropriées ; par ex. serrure).
- **Mesures de sécurité informatique**
  voir la notice annexée

Notice

Mesures de sécurité informatique

Les mesures de sécurité des systèmes informatiques et des logiciels d'application doivent garantir la confidentialité, la disponibilité et l'exactitude des données sur les résidentes et résidents.

Avant l'utilisation et au cours de l'exploitation d'un système informatique et d'un logiciel d'application, les responsables d'un home sont tenus de vérifier les mesures de sécurité. Ce faisant, il s'agit de répondre, ou d'obtenir des réponses de la part du fournisseur, aux questions suivantes, telle une checklist : l'exhaustivité des questions n'est pas garantie.

- L'accès aux systèmes informatiques (locaux) qui traitent des données sur les résidents par des personnes non autorisées est-il interdit ?
- L'utilisation d'installations qui traitent des données sur les résidentes et résidents par des personnes non autorisées est-elle interdite ?
- La lecture, copie, modification ou suppression de supports de données est-elle rendue impossible, pour les personnes non autorisées, au moyen d'un cryptage des données ?
- Des mesures de sécurité appropriées (par ex. cryptage des données, identification du destinataire, etc.) empêchent-elles qu'au cours d'un transport de données sur les résidents celles-ci puissent être lues, copiées, modifiées ou supprimées sans autorisation ? Cela s'applique notamment dans le cadre des systèmes en réseau et de transfert de données par Internet.
- Des droits d'accès appropriés empêchent-ils la saisie de données sans autorisation, ainsi que la consultation, la modification ou la suppression des données enregistrées sur les résidentes et résidents?
- Les droits d'accès sont-ils différenciés ? Les droits d'accès sont-ils calqués sur la fonction de l'utilisateur et limités aux données sur les résidentes et résidents nécessaires à l'utilisateur pour exécuter son travail ?
- Les droits d'accès sont-ils mis à jour en permanence selon l'organisation du travail (fonction) actuelle et l'utilisation correcte des mots de passe fait-elle l'objet d'une instruction, d'une mise en application et d'un contrôle régulier ?
- Un contrôle de saisie adapté est-il disponible pour permettre de contrôler quelles données sur les résidentes et résidents ont été saisies, à quel moment et par quelle personne ?
- Les résidentes et résidents peuvent-ils consulter leurs données personnelles et exercer ainsi leur droit d'être renseigné et leur droit à faire rectifier leurs données ?
- La sauvegarde des données quotidienne/périodique est-elle réglée ? Les supports de données sont-ils conservés sous clé, séparément et en un autre lieu que le système informatique, pour des raisons de sécurité ?
- Une procédure de sauvegarde et de rétablissement des données est-il disponible en cas d'urgence ?
- En cas d'exportation des données (par ex. à des fins statistiques), les données sur les résidentes et résidents sont-elles rendues anonymes et le but de l'exportation des données est-il annoncé clairement ?