

Traitement des documents confidentiels

Objet

Cette directive définit les règles applicables au traitement des documents considérés comme confidentiels, qu'ils concernent les patients, les collaborateurs ou des tiers et quel qu'en soit le support. Toute personne qui manipule ce type de documents doit particulièrement respecter un devoir de prudence et de discrétion. Il convient de protéger la sphère privée de chacun, que ce soit dans la collecte des données, l'élaboration des documents, leur manipulation et utilisation, leur transmission, leur conservation et archivage et enfin leur destruction.

Table des matières

1. Principes et règles
2. Définition des documents confidentiels
3. Collecte
4. Elaboration
5. Manipulation
6. Transmission
7. Conservation et archivage
8. Destruction

Domaine d'application

Cette directive s'adresse à tous les collaborateurs du CHUV.

1. Principes et règles

Le CHUV est habilité à récolter des données se rapportant à une personne identifiée ou identifiable (des données personnelles) et à les traiter pour l'accomplissement de sa tâche publique. La législation sur la protection des données oblige à protéger contre tout emploi abusif ces données qui concernent les patients, mais aussi les collaborateurs de l'institution.

On entend par traitement de données personnelles, toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données personnelles. Ces transactions consistent notamment en la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction.

L'utilisation des données personnelles en dehors du but d'accomplissement de la tâche publique dédiée au CHUV est illicite et abusive. Le traitement des données personnelles doit ainsi être conforme au principe de la proportionnalité et se faire dans un cadre qui garantit leur sécurité, soit notamment contre leur perte, leur destruction, ainsi que tout traitement illicite. Leur divulgation est interdite, sauf obligations légales.

Du fait des activités de soins et de recherche médicale du CHUV, tous ses collaborateurs sont soumis au respect du secret professionnel. Comme tels, ils font en sorte d'exercer leur tâche dans le souci de protection de la sphère privée des patients et des collaborateurs. Pour plus de détails : cf. directives institutionnelles « Secret médical, secret de fonction et protection des données informatisées », « Confidentialité des données des patients lors de l'utilisation d'applications informatiques du CHUV ».

2. Définition des documents confidentiels

Est considéré comme confidentiel au sens de la présente directive :

- A. Un document qui contient des indications sur la vie privée des individus identifiables (patients ou collaborateurs) comme la santé, les données salariales, la situation financière, la religion, etc.;
- B. Tout document – quel qu'en soit le support (papier, CD, DVD, carte mémoire etc.) - qui contient des informations se rapportant à un patient identifié ou identifiable;
- C. Un document qui porte la mention de « confidentiel »;

Du fait de leur contenu sensible, les documents confidentiels doivent faire l'objet d'un traitement particulier permettant dans la mesure du possible d'en maintenir le secret. Un document confidentiel ne doit être accessible qu'à ses destinataires et la collecte des informations confidentielles ne se justifie que pour l'accomplissement des tâches professionnelles. L'obligation de confidentialité signifie qu'une information sur un patient ne doit pas être diffusée au-delà des personnes en charge de ce patient (sauf exceptions prévues par la loi).

Les chefs de service sont responsables du traitement des documents confidentiels dans leur service. Pour ce faire, ils identifient quels sont les documents confidentiels et veillent au respect des règles suivantes :

3. **Collecte:** Est seule admise la collecte des informations confidentielles à des fins d'accomplissement des tâches professionnelles. Toute autre fin est interdite (cf. Directive institutionnelle « Confidentialité des données des patients lors de l'utilisation d'applications informatiques du CHUV »).
4. **Elaboration:** Les documents correspondant aux lettres A et B ci-dessus sont considérés d'office comme confidentiels. Tout autre document dont on veut une protection accrue doit porter la mention de « confidentiel » (cf. lettre C).
5. **Manipulation:** Ces documents doivent être manipulés dans le respect de la sphère privée des personnes concernées et répondre à un souci particulier de discrétion et de précaution. Ils ne doivent pas être laissés à la vue de personnes non concernées et/ou non destinataires. Il convient d'éditer les documents comportant des informations confidentielles sous un **mode d'impression suspendue ou sécurisée** (cf. annexe 1) lors d'utilisation d'imprimantes partagées. Dans tous les cas, les impressions sont récupérées au plus vite.

Il faut éviter de multiplier et disperser les documents contenant des données sensibles sur plusieurs supports externes : clé USB, CD-Rom, photocopies.

6. **Transmission:** L'expéditeur s'assure de l'exactitude de l'adresse du destinataire, mentionne le caractère confidentiel du contenu du message, et précise ses coordonnées professionnelles. Pour éviter la divulgation de son contenu à des personnes non autorisées, l'expéditeur est responsable de s'assurer que la transmission est **sécurisée** de manière adéquate, en fonction du type de transmission :

Transmission physique (courrier) : Les documents confidentiels sont transmis impérativement sous pli fermé avec mention de l'expéditeur et du destinataire concerné, y compris pour les envois internes à l'institution. Ces derniers peuvent toutefois être groupés.

Télécopie (fax) : La sécurité des « fax » repose essentiellement sur un choix judicieux de localisation des télécopieurs et l'existence de procédures adéquates chez l'expéditeur et le destinataire. (Par exemple, l'expéditeur avertit systématiquement le destinataire par téléphone de l'arrivée imminente de la télécopie.) En l'absence de telles garanties de sécurité, il faudrait privilégier un moyen de transmission mieux protégé.

Messagerie électronique (courriel ou « e-mail ») : La messagerie institutionnelle fournit un bon niveau de protection des messages internes. Cependant, elle **ne garantit pas** la protection du contenu d'un message **en dehors** du réseau informatique de l'institution. La page intranet de la Sécurité informatique sur le Courrier électronique décrit les précautions que l'expéditeur doit prendre pour assurer la sécurité de tout message confidentiel.

Réception de documents / messages : Un document reçu par erreur - destiné manifestement à une autre personne - ne doit pas être lu, mais renvoyé à l'expéditeur (dans le cas d'un courrier) ou détruit (dans le cas d'un message électronique ou d'un fax).

7. **Conservation et archivage:** Les documents sensibles enregistrés sur des supports externes ou imprimés sont mis dans un endroit sûr. Les données confidentielles sur supports informatiques amovibles (CD-Rom, clé USB, ordinateur portable etc) doivent être protégées par un mot de passe (cf. page intranet sur les Règles relatives au stockage des données confidentielles sur support informatique).

Destruction : Selon degré de confidentialité de la zone concernée: ramassage par Service de maison et broyage à la déchèterie ou déchiquetage sur site.

Les documents confidentiels sont détruits exclusivement selon les procédures ci-jointes (cf. annexe 1). Les chefs de service sont responsables de leur respect au sein de leur service.

Responsabilités

Cette directive est placée sous la responsabilité du:

- Comité de direction du CHUV

Sont associés à la responsabilité pour son élaboration, son application et sa mise à jour :

- l'Unité des affaires juridiques
- la Direction médicale
- le Service de transports, communications et approvisionnements
- le Service de la sécurité

Sont associés à la responsabilité pour son application :

- les Chefs de service

Abbreviations

AFJ :	Unité des affaires juridiques	DI :	Directive institutionnelle
DG :	Direction générale CHUV	TCA :	Service de transports, communications et approvisionnements

Documents et textes de référence

Code pénal suisse du 21 décembre 1937 (CP, RS 311.0)
Loi vaudoise sur la santé publique du 29 mai 1985 (LSP, RSV 800.0.1)
Loi vaudoise sur la protection des données personnelles du 11 septembre 2007 (LPrD, RSV 172.65)

Documents associés

- DI sur le Secret médical, secret de fonction et protection des données informatisées
- DI sur la Confidentialité des données des patients lors de l'utilisation d'applications informatiques du CHUV
- DI sur la Transmission et accès aux informations du dossier patient
- DI sur l'Utilisation des équipements informatiques
- Aide-mémoire relatif à la sécurité informatique (http://intranet/insec/insec_home/insec-infos-pratiques/insec-aide-memoire.htm), notamment sur le courrier électronique et les mots de passe.
- Annexe 1 : Procédures de destruction des documents confidentiels (Fiches du TCA pour la destruction des documents confidentiels (nos 04, 17, 41, 42))
- Annexe 2 : Mode d'emploi pour l'impression suspendue ou sécurisée

Distribution

Département, service, unité	Fonction
Directions des départements CHUV	Charge aux directeurs administratifs des départements de faire suivre aux personnes concernées.
Comité de direction élargi CHUV	
Chefs de service	
Infirmiers-ères chefs de service	
Secrétariats	

Validation, classement, archivage

N° de version	Elaboration/Modification	Validation Date	Distribution Date	Classement archivage
V1.0	DGH/AFJ/jps...	CD/19.01.2010	AFJ...date...	AFJ

Annexe 1 : Procédures de destruction des documents confidentiels

Les données confidentielles sont principalement stockées sur les types de supports suivants :

- Le papier, via une imprimante, un fax, un photocopieur, une mention manuscrite ; le document peut être en vrac, en classeurs, en boîtes à archives, en rapports etc.
- Les supports magnétiques avec des composants électroniques : disque dur interne (dans PC), disque dur externe, clé USB etc.
- Les supports magnétiques mobiles ou consommables : cassettes vidéo, CDS, disquettes, cartouches, DVDS, bandes magnétiques.

La production peut être régulière, découlant de l'activité routinière, ou exceptionnelle, lors de déménagement par exemple, ou d' « à-fonds »

Divers moyens existent actuellement pour gérer les déchets confidentiels.

Le premier est d'EVITER d'en produire ; en se posant la question « dois-je imprimer/copier/sauvegarder ceci ? » et le cas échéant, s'abstenir.

Lorsque le déchet confidentiel est produit, plusieurs moyens sont à disposition pour l'éliminer correctement. Au vu des coûts, logistiques et financiers en jeu, il est important de n'utiliser ces moyens que pour les déchets confidentiels et les filières banales pour les déchets non confidentiels.

Vous trouverez les modalités d'élimination dans le Vademecum du TCA :

http://livelink/intranet/loh_home/loh_organisation/loh_organisation_tca/loh_tca_prestations/loh_tca_gp_dec_hets/loh_tca_fp_vademecum_dechets/loh_tca_fp_vademecum_supports_confidentiels-2.htm

Annexe 2 : Mode d'emploi pour l'impression suspendue ou sécurisée

Pour l'impression suspendue ou sécurisée, un mode d'emploi existe sur l'intranet à l'adresse suivante :

http://intranet/dsi/dsi_home/dsi_documentation/dsi_bureautique.htm