

Fiche d'information

Dossier électronique du patient et compétence en matière de protection des données

La protection des données personnelles fait l'objet d'une surveillance étatique, dont les modalités varient selon le domaine. Cette tâche est soumise à la législation en vigueur en la matière : sa répartition entre les autorités et son organisation ne sont pas libres. Le texte applicable dépend toujours de l'institution qui traite les données personnelles. S'il s'agit d'un organe fédéral ou d'une personne privée, la loi fédérale sur la protection des données (ci-après « LPD fédérale ») s'applique. Si le traitement incombe à une institution publique cantonale, la loi sur la protection des données édictée par le canton fait foi.

L'identification de la loi applicable permet aussi de déterminer l'autorité compétente pour la surveillance. Lorsque la LPD fédérale s'applique, le Préposé fédéral à la protection des données et à la transparence (PFPDT) est compétent. Quand le traitement de données est soumis à une loi cantonale, la surveillance relève du préposé cantonal à la protection des données. À ces textes généraux viennent s'ajouter des lois spéciales contenant des dispositions spécifiques à certains domaines, que l'institution effectuant le traitement doit également respecter.

La législation relative au dossier électronique du patient (DEP) comporte des prescriptions spécifiques en matière de protection des données. L'autorité de surveillance doit les prendre en compte au même titre que la loi sur la protection des données applicable. En outre, la législation sur le DEP prévoyant une obligation de certification pour les communautés et les communautés de référence, les organismes de certification exercent aussi une certaine surveillance dans les domaines soumis à leur examen.

Le tableau ci-après offre un aperçu des autorités de surveillance et de la législation applicable dans le cadre de la mise en œuvre du DEP. Il distingue les fournisseurs de prestations en fonction de leur forme juridique et selon qu'ils agissent ou non dans le cadre d'un mandat de prestations.

Dans le cas des prestataires (p. ex., les exploitants de l'infrastructure informatique) qui traitent des données sur mandat d'une autre institution, l'autorité de surveillance et la législation applicable dépendent du mandant.

Le tableau permet, de façon générale, de déterminer l'autorité responsable et les règles juridiques applicables. Des divergences peuvent toutefois survenir en fonction de la situation concrète. En cas d'incertitude, il convient d'effectuer des recherches supplémentaires.

N°	Entité traitant les données	Forme juridique	Autorités de surveillance et droit applicable
1.	Communautés de référence/ communautés	Organisation de droit privé (association, SA) → en l'état actuel	- Organismes de certification : pour tout ce qui relève du domaine soumis à certification. Application de la législation sur le DEP, collaboration avec l'OFSP. - PFPDT : pour tout ce qui ne relève PAS du domaine soumis à certification. Application de la LPD fédérale, de la législation sur le DEP et, le cas échéant, d'autres prescriptions spécifiques.
2.	Hôpitaux, cliniques, établissements médico-sociaux SANS mandat de prestations cantonal ou communal	Organisation de droit privé (SA, fondation)	- PFPDT : pour tous les domaines. Application de la LPD fédérale, de la législation sur le DEP et, le cas échéant, d'autres prescriptions spécifiques. - Organismes de certification (éventuellement)* : uniquement pour ce qui concerne les domaines couverts par la certification. Application de la législation sur le DEP.

N°	Entité traitant les données	Forme juridique	Autorités de surveillance et droit applicable
3.	Hôpitaux, cliniques, établissements médico-sociaux AVEC mandat de prestations cantonal ou communal	Deux possibilités : A) établissement de droit public ou B) organisation de droit privé (SA)	A) Établissement de droit public : Préposé cantonal à la protection des données : pour tous les domaines. Application des lois cantonales pertinentes sur la protection des données, de la législation sur le DEP et, le cas échéant, d'autres prescriptions spécifiques. B) Organisation de droit privé avec mandat de prestations cantonal ou communal : - Préposé cantonal à la protection des données : pour tout ce qui a trait directement au mandat de prestations. Application des lois cantonales pertinentes sur la protection des données, de la législation sur le DEP et, le cas échéant, d'autres prescriptions spécifiques. - PFPDT : pour tout ce qui n'a PAS trait directement au mandat de prestations. Application de la LPD fédérale et des éventuelles prescriptions spécifiques.
4.	Services de soins ambulatoires SANS mandat de prestations cantonal ou communal	Organisation de droit privé (association, fondation)	- PFPDT : pour tous les domaines. Application de la LPD fédérale, de la législation sur le DEP et, le cas échéant, d'autres prescriptions spécifiques. - Organismes de certification (éventuellement)* : uniquement pour ce qui concerne les domaines couverts par la certification. Application de la législation sur le DEP.

N°	Entité traitant les données	Forme juridique	Autorités de surveillance et droit applicable
5.	Service de soins ambulatoires AVEC mandat de prestations cantonal ou communal (p. ex., services d'aide et de soins à domicile)	Organisation de droit privé (association, fondation)	- Préposé cantonal à la protection des données : pour tout ce qui a trait directement au mandat de prestations. Application des lois cantonales pertinentes sur la protection des données, de la législation sur le DEP et, le cas échéant, d'autres prescriptions spécifiques. - PFPDT : pour tout ce qui n'a PAS trait directement au mandat de prestations. Application de la LPD fédérale et des éventuelles prescriptions spécifiques.
6.	Autres fournisseurs de prestations, comme les cabinets médicaux, les pharmacies et les prestataires paramédicaux (physiothérapeutes, diététiciens, ergothérapeutes, etc.)	Organisation de droit privé (entreprise individuelle, SA, Sàrl, association)	- PFPDT : pour tous les domaines. Application de la LPD fédérale, de la législation sur le DEP et, le cas échéant, d'autres prescriptions spécifiques. - Organismes de certification (éventuellement)* : uniquement pour ce qui concerne les domaines couverts par la certification. Application de la législation sur le DEP.
7.	Exploitants de systèmes décentralisés pour le DEP (p. ex., Swisscom, La Poste)	Organisation de droit privé (SA) ...mais traitement de données sur mandat des communautés et des communautés de référence → mêmes responsables et même législation applicable que pour les communautés et les communautés de référence	- Organismes de certification : pour tout ce qui relève du domaine soumis à certification. Application de la législation sur le DEP, collaboration avec l'OFSP. - PFPDT : pour tout ce qui ne relève PAS du domaine soumis à certification. Application de la LPD fédérale, de la législation sur le DEP et, le cas échéant, d'autres prescriptions spécifiques.

* Il existe des incertitudes quant à l'étendue effective de l'obligation ou du droit de surveillance des organismes de certification à l'égard des entités concernées.