LAUX LAWYERS AG
ZURICH | BASEL

Le cloud pour le secteur de la santé

Solutions pour les réserves fréquemment exprimées – non réservé aux organisations de santé

Traduction pratique de l'original Allemand; traduit avec DeepL Pro

Laux Lawyers AG
Octobre 2023

À l'initiative et avec l'aimable soutien de AWS

LAUX LAWYERS AG
ZURICH | BASEL

CONTENU

I RÉSUMÉ EXÉCUTIF

Les hôpitaux, les cabinets médicaux et d'autres acteurs du secteur de la santé traitent et enregistrent 24 heures sur 24 de grandes quantités de données. Ces vastes ensembles **de données contiennent** en grande partie des données relatives à la santé. Le besoin de contrôle et de protection des personnes concernées quant à les données relatives à la santé est reconnu et incontesté.

Le système de santé et ses fournisseurs de prestations sont réglementés. Les données relatives à la santé sont considérées comme sensibles. Elles doivent être traitées de manière confidentielle. Le droit de la protection des données exige en outre que ces données ne soient pas falsifiées („intégrité") et qu'elles soient disponibles. La protection réglementaire est d'intérêt public.

La digitalisation promet de grands avantages au secteur de la santé. Mais la digitalisation est freinée par des réserves. Qu'est-ce qui est autorisé ? Qu'est-ce qui ne l'est pas ? De nombreuses questions se posent. Et il n'y a pas assez de réponses claires. Une chose est sûre : La digitalisation est impensable sans la **confiance** des patients, des médecins, des hôpitaux, des autorités, des législateurs et des autres parties prenantes.

C'est au milieu de cette tension que se trouvent les **services cloud**[1]. Leur potentiel est grand : les services cloud facilitent considérablement de nombreuses initiatives de digitalisation. Les coûts peuvent être réduits, ce qui est particulièrement important dans le secteur de la santé. En utilisant des services cloud, les acteurs du secteur de la santé peuvent également accroître leur efficacité, augmenter la sécurité et la flexibilité de leurs systèmes informatiques et libérer des ressources pour leur activité principale. En outre, les acteurs peuvent mettre en place des solutions modernes et hautement évolutives, avec des normes de sécurité et une sécurité contre les pannes maximales, pour la fourniture de soins de santé, le développement de nouvelles méthodes de traitement et, non des moindres, pour des soins personnalisés aux patients. Les infrastructures informatiques utilisées sont à la pointe de la technologie en termes de fonctionnalité et de cybersécurité, même si l'institution de santé ne doit pas mettre en place et exploiter elle-même une infrastructure informatique et de sécurité importante. Avec la diffusion croissante des services cloud des grands fournisseurs internationaux de cloud (appelés „hyperscaler"), la conscience générale et la compréhension de la manière dont ils traitent les données qui leur sont confiées augmentent.

Les avantages peuvent être contrebalancés par des **défis** d'un autre ordre. Les données sont détenues par le fournisseur cloud. Les réserves à ce sujet font l'objet d'intenses discussions dans le débat public : le cloud (c'est-à-dire les services cloud) serait problématique du point de vue de **la protection des données** et **du secret médical** ; en outre, les références à l'étranger s'opposeraient à son utilisation.

[1] Dans ce livre blanc, nous entendons par **services cloud** l'ensemble des prestations par lesquelles un fournisseur accorde à une institution de santé l'utilisation de certaines infrastructures informatiques. Cette offre s'effectue de manière standardisée, automatisée, évolutive et sous une forme non dédiée via des réseaux de données. **Le terme „service cloud"** est également utilisé pour désigner le terme **„cloud public"**, ce qui signifie que les composants de base du fournisseur ne peuvent être utilisés par aucun client de manière individuelle et exclusive („dédiée") ; en revanche, la possibilité d'utilisation mise à disposition au sein d'un tenant est individuelle et délimitée par rapport aux autres clients („isolation"), ce qui est possible par exemple grâce à la technologie de réseau.

Une chose est sûre : la Suisse a une culture qui accorde une grande valeur aux données de santé. Et c'est bien ainsi. L'expression de cette culture est que l'on veut protéger les données relatives à la santé - précisément parce qu'elles sont importantes. Cela conduit aux conclusions fondamentales et aux exigences importantes suivantes :

- **premièrement,** il y a un grand potentiel de risque lié aux données de santé
- **deuxièmement,** les patients doivent être protégés contre l'utilisation abusive de leurs données
- **troisièmement,** les patients doivent avoir le droit de décider si d'autres personnes peuvent consulter leurs données
- **quatrièmement,** les données confiées par les patientes doivent rester dans la sphère d'influence du médecin
- **cinquièmement,** des mesures de sécurité élevées sont nécessaires pour protéger les données des patients.

Ces exigences et les valeurs qui les sous-tendent constituent le fondement sur lequel repose ce livre blanc. Les auteurs les tiennent en haute estime et réaffirment leur importance.

Cela ne signifie pas pour autant que les auteurs déconseillent le cloud ou qu'ils partagent les prises de position problématisant qui sont parfois présentées. Bien au contraire. Bien que l'on s'accorde sur les exigences et les valeurs fondamentales, le débat public sur le cloud dans le secteur de la santé souffre de malentendus.

Le droit de la santé se déroule en grande partie dans les hôpitaux publics. Dans la mesure où il est organisé au niveau cantonal, le secteur de la santé est à cet égard placé sous la **surveillance des autorités cantonales.** Les autorités cantonales de protection des données participent activement à la discussion et édictent des guides, des listes de contrôle et des notices. **Il s'agit d'avis qui, en tant que tels, n'engagent pas les institutions du secteur de la santé.**[2] Il en va de même pour les recommandations des associations professionnelles concernées. L'insécurité augmente néanmoins.

Les explications qui suivent montrent que certaines réserves discutées dans le débat public ne résistent pas à un examen juridique.

Le cloud pour le secteur de la santé est possible et offre de nombreux avantages

Il faut prendre soin du système de santé. Il convient d'appliquer un niveau de diligence raisonnable. **Les institutions de santé peuvent relever ces défis juridiques grâce aux services cloud disponibles aujourd'hui, qui sont d'un haut niveau de qualité et de sécurité.**

[2] Dans le domaine de la santé, le droit cantonal de la protection des données joue un rôle important. Les avis exprimés par les autorités cantonales de surveillance de la protection des données sont un instrument de communication proactive du droit d'être entendu - l'instance explique au préalable comment elle juge un cas particulier sur le plan juridique. Cela permet d'assurer la clarté juridique et la sécurité de la planification, et donc l'utilisation efficace des ressources de ceux qui pourraient être affectés ou freinés par une décision d'un tel service - dans la mesure où il a une compétence décisionnelle. Les déclarations publiques n'engagent donc en premier lieu que l'autorité cantonale de protection des données elle-même. En ce qui concerne le traitement des données lors de la fourniture de prestations de santé dans le cadre du mandat de prestations cantonal, l'hôpital peut compter sur le fait que l'autorité de surveillance appliquera la loi telle qu'elle est décrite dans le communiqué. Il *ne* s'agit toutefois *pas* d'instructions juridiquement contraignantes *pour l'hôpital*.

II CLOUD POUR LE SECTEUR DE LA SANTÉ

Les données de santé dans le cloud

Ce livre blanc examine sous différents angles juridiques la question de savoir si les hôpitaux, les cabinets médicaux et autres institutions de santé peuvent stocker et traiter des données de santé „dans le cloud". Qu'englobe la notion de „données de santé" du point de vue juridique? Différentes lois utilisent ce terme ou une variation de celui-ci. Il n'existe pas de définition juridique universelle.

La loi fédérale sur la protection des données **(LPD)** ainsi que les lois cantonales sur la protection des données règlent les exigences relatives au traitement des **données personnelles.** Dans le contexte de l'hôpital ou du médecin, cela concerne d'une part les données de base (données personnelles générales telles que le nom, l'adresse et le numéro d'assuré) et d'autre part les données de santé qui se rapportent au patient concerné. Les données de santé comprennent des informations sur l'état de santé passé ou actuel, sur le déroulement du traitement ainsi que sur le recours aux prestations de santé et leur facturation. La notion de données relatives à la santé au sens de la protection des données ne comprend cependant pas seulement des indications sur des maladies ou des accidents actuels ou passés, mais aussi des résultats d'examens (par exemple l'analyse d'échantillons de sang ou de données génétiques) qui permettent de déduire des risques de maladie ou d'autres indications sur l'état de santé futur.

Des lois spéciales du droit de la santé précisent cette conception large. Il convient également de noter que dans le contexte d'un diagnostic, d'un examen ou d'un traitement dans un hôpital ou un cabinet médical, ou encore dans le cadre de la recherche sur l'être humain, même les informations relatives au mode de vie (p. ex. alimentation, tabagisme, activité physique), les données relatives à l'environnement de vie (p. ex. qualité de l'air et de l'eau), à l'environnement social (p. ex. famille ou profession) ainsi que les données de mesure de la condition physique ont un rapport avec la santé et sont donc qualifiées et catégorisées comme données relatives à la santé dans un tel contexte.

Données relatives à le santé (terme)

Les données relatives à la santé sont des données sur l'état de santé passé, actuel ou futur d'une personne. Dans le contexte de l'hôpital ou du cabinet médical, elles comprennent elles-mêmes des informations sur le mode de vie et l'environnement social du patient ainsi que les résultats d'examens qui permettent de déduire des indications sur l'état de santé.

1. Les données relatives à la santé en tant que données personnelles sensibles
La LPD et les lois cantonales sur la protection des données classent les données relatives à la santé dans la catégorie des données personnelles sensibles (ou similaires : données personnelles particulières). Le législateur considère que le besoin de protection spéciale réside en premier lieu dans le fait que le risque de mise en danger est particulièrement élevé en cas de communication ou de divulgation incontrôlée. C'est essentiellement la protection contre la discrimination qui est ici visée. Le patient doit être protégé contre la stigmatisation ou la discrimination par l'État, les assurances, l'environnement social ou professionnel en raison d'un état de santé.

En d'autres termes, il s'agit d'éviter d'élargir de manière incontrôlée le cercle de ceux qui ont accès en clair à des données personnelles sensibles (ce qu'on appelle l'élargissement incontrôlé du cercle). Un patient doit pouvoir compter sur le professionnalisme du médecin dans le traitement de ses données. Cela doit fonctionner de manière aussi fiable que le secret médical. Lorsque le patient se confie à un médecin, les informations ne doivent pas quitter sa sphère d'influence. Dans ce contexte, la médecine doit contrôler son cercle (concrètement : son cabinet médical avec tout ce qui en fait partie, y compris les moyens informatiques tels que les services cloud qu'elle utilise).

Besoin particulier de protection

Dans le cas des données relatives à la santé, la nécessité d'une protection particulière découle du fait que la personne concernée pourrait subir des préjudices, par exemple en raison d'une maladie révélée de manière incontrôlée.

Exemples d'inconvénients :
- Stigmatisation dans l'environnement social
- Discrimination au travail (conséquences économiques ou psychologiques)
- Discrimination par l'assurance (risque de coûts, limitation du choix des partenaires contractuels ou des prestations disponibles)

2. Sur le risque associé aux données relatives à la santé
L'utilisation abusive de données relatives à la santé peut, dans des cas extrêmes, entraîner des conséquences très graves. Le potentiel de danger peut être illustré à l'aide d'exemples concrets (voir annexe „éléments de l'analyse des risques"). Dans la pratique, des conclusions erronées sont toutefois tirées sur cette base. Parfois, les perspectives sont perdues.

Quel est le problème d'un élargissement incontrôlé du cercle?

L'élargissement incontrôlé du cercle désigne le processus par lequel un nombre ouvert de personnes reçoit des données relatives à la santé et peut en faire ce qu'il veut. Des abus sont alors possibles. Il est donc important de protéger les données relatives à la santé contre un élargissement incontrôlée du cercle.

Concernant le contexte :

- Si des données sont transmises à un **cercle ouver**t de destinataires qui ne sont soumis à **aucun contrôle** sur les données personnelles ainsi obtenues, il en résulte une situation incontrôlable. L'exemple typique est la violation de données. Un grand nombre d'auteurs potentiels de préjudices peuvent effectuer un grand nombre d'actes potentiellement préjudiciables, sans que ce risque puisse être réduit. Cette situation de risque ne peut pas être maîtrisée.
- En revanche, si elles sont destinées à un **destinataire déterminé**, soumis à un **contrôle** sur les données personnelles transmises, il est possible d'évaluer concrètement le risque concret que représente le destinataire en question. Cette situation de risque peut être maîtrisée.

Au vu de ce qui précède, il est clair qu'il serait faux de dire que le danger découle de l'information elle-même. Une seule et même information sur la santé peut entraîner des risques de danger différents pour la personnalité et les droits fondamentaux de la personne concernée, selon la personne qui consulte ou traite les données et dans quel contexte. Le danger ne peut pas être évalué de manière abstraite, mais doit être considéré dans un cas concret.

En d'autres termes, c'est le contexte d'utilisation **(contexte)** qui rend le traitement des données risqué. Une déclaration sur l'état de santé d'une personne peut avoir une signification différente selon le contexte d'utilisation. Par exemple, les mesures de la condition physique dans le contexte des loisirs ont une autre signification que si elles sont intégrées dans un diagnostic médical ou constituent une base pour des décisions thérapeutiques. L'annexe montre plus en détail dans quelle mesure les déclarations de risque découlent du contexte.

Si l'on reprend ce constat pour le présent livre blanc, il est clair que le contexte d'utilisation ou la finalité d'un traitement ne change pas du fait que l'on utilise des services cloud. En cas d'utilisation des services cloud matures[3], les données relatives à la santé ne sont justement pas rendues accessibles à un nombre indéterminé de personnes. Les données sont stockées chez un destinataire déterminé, et ce de manière contrôlée (c'est l'obligation de l'institution de santé de s'en assurer).

Il n'y a pas non plus d' élargissement incontrôlé du cercle si, par exemple, une autorité de poursuite pénale étrangère exige, dans le cadre d'une procédure judiciaire, la remise de certaines données auprès du fournisseur cloud. A cet égard, les risques (théoriques) doivent être évalués concrètement. Mais il n'y a pas d'élargissement incontrôlé du cercle tant que le processus est suffisamment surveillé par le tribunal dans le respect de l'État de droit et que l'autorité ne divulgue pas à son tour les données à un nombre indéterminé d'autres destinataires (p. ex. par publication ou autre) ou ne les utilise pas de manière contraire au but (en dehors de la poursuite pénale). Il convient toutefois de déterminer quels sont les actes d'utilisation qu'elle effectue. Et c'est à cela que doit se rattacher l'évaluation des risques (de manière concrète).

L'utilisation des services cloud n'est donc pas en soi un facteur déclenchant pour parler d'un élargissement incontrôlé du cercle. Le passage au cloud est plutôt un processus comme un autre, même s'il s'agit de données de santé : il fautidentifier les dangers possibles et décrire leur probabilité d'occurrence (probability) ainsi que leur potentiel de dommage (impact). A partir de là, il est possible d'établir une déclaration de risque dans le sens d'une synthèse. C'est tout ce qu'on demande.

[3] La notion de **„service cloud mature"** est un terme générique. Un fournisseur cloud mature doit établir un état contrôlé en ce qui concerne la fourniture de prestations, la sécurité de l'information et la gouvernance. S'il le fait, ses services cloud peuvent être qualifiés de „matures". Le fournisseur cloud mature doit contrôler ses propres infrastructures informatiques, les personnes engagées pour fournir la prestation et les processus définis à cet effet. En outre, il doit être prêt à indiquer à son client lesquelles de ces mesures il prend, de sorte que l'institution de santé soit en mesure, en tant que client, d'intégrer le fournisseur cloud et ses prestations dans son contrôle.

Cas concrets d'utilisation du cloud dans le secteur de la santé

1. Introduction

Le secteur de la santé est hautement réglementé. Une multitude de lois spéciales définissent des conditions-cadres pour les activités des hôpitaux, des autres fournisseurs de prestations de santé, des chercheurs, des fabricants de produits médicaux ou de médicaments et d'autres acteurs du secteur de la santé. Les lois spéciales en matière de droit de la santé et les ordonnances d'exécution[4] contiennent également des règles qui complètent les règles générales du droit de la protection des données et du secret ou qui les concrétisent pour un cas d'application particulier (p. ex. recherche sur l'être humain ou analyses génétiques sur l'être humain). Les règles correspondantes s'appliquent indépendamment de l'infrastructure ou de la technologie utilisée. Par exemple, c'est l'utilisation prévue qui détermine si un logiciel est un produit médical.

La décision d'utiliser un service cloud a donc un effet „neutre" dans la mesure où les règles s'appliquent de toute façon aussi en cas d'utilisation d'une „solution sur site". L'analyse ci-dessous de quelques cas d'application typiques le montre à titre d'exemple. Ce qui change, ce sont les moyens utilisés, par exemple pour exercer un contrôle – les services cloud augmentant les possibilités de contrôle, en particulier dans le domaine de la sécurité de l'information, mais les institutions de santé doivent aussi s'assurer, sur le plan organisationnel, qu'elles utilisent les possibilités de contrôle de manière conséquente.

2. Système d'information clinique dans le cloud

Les Systèmes d'Information Hospitalier (SIH) doivent représenter de manière complète le quotidien d'un hôpital. En ce qui concerne les aspects de la protection des données, les dispositions relatives à l'obligation de documentation et de conservation sont particulièrement pertinentes. Dans la mesure où le traitement dans le SIH entraîne des objectifs d'utilisation considérablement étendus, il faudrait également en discuter du point de vue de la protection des données.

Les exigences juridiques qui en découlent (en particulier celles découlant du droit du secret et du droit cantonal de la protection des données) pour le SIH d'un hôpital sont examinées ci-après. Aucun de ces aspects n'est toutefois spécifiquement hostile au cloud. En d'autres termes, le cloud ne rend pas ces thèmes plus problématiques, mais les aborde souvent mieux :

Dans quelle mesure le cloud change-t-il quelque chose pour l'utilisation d'un SIH à l'hôpital?

Sujet	Exigence[5]	Influence du cloud
Dossier du patient	Droits d'information, de consultation et de publication découlant des lois cantonales sur la santé et les patients[6]	neutre (exigence fonctionnelle[7])
	Droits d'accès, de communication, de rectification ou d'effacement fondés sur la législation relative à la protection des données	neutre (exigence fonctionnelle)
Système global (SIH)	Toutes les personnes tenues au secret doivent pouvoir garder leur secret professionnel ; et ce, bien qu'une organisation globale soit rattachée au SIH (obligations de secret).	neutre (concept d'autorisation nécessaire) (exigence fonctionnelle)
	Protection contre les accès non autorisés (sécurité de l'information, en raison des obligations de protection des données et de confidentialité ; également sur la base du mandat de prestations[8])	neutre (cloud généralement meilleur) (exigence fonctionnelle)
	Protection contre les modifications non autorisées (sécurité de l'information, en raison des obligations de protection des données et de confidentialité ; également sur la base du mandat de prestations)	neutre (cloud généralement meilleur) (exigence fonctionnelle)
	Garantie de la disponibilité (sécurité de l'information, protection des données ; également sur la base du mandat de prestations)	neutre (cloud généralement meilleur) (exigence non fonctionnelle)
	Processus d'exportation des informations sur les patients, concept d'effacement et journalisation des accès et des traitements de données (bonne gouvernance).	neutre (exigence fonctionnelle)

La représentation montre que les exigences légales et contractuelles en matière de documentation, de conservation, de sécurité de l'information et de préservation des droits des patients ne changent pas lorsqu'un hôpital met à disposition et exploite son SIH sur une infrastructure cloud. Ce sont généralement les caractéristiques fonctionnelles qui sont pertinentes. L'exigence relative au secret médical ne change pas non plus (voir par exemple la réserve 1 ci-dessous).

Ce qui va changer : Il y a externalisation du traitement des données. L'hôpital doit garantir par contrat l'obligation de suivre des instructions et des mesures de protection techniques et organisationnelles appropriées. C'est faisable, comme le montre l'expérience.

Il convient de noter ce qui suit : Souvent, le passage à un SIH en tant que service cloud n'est pas le premier pas d'un hôpital vers le „cloud". L'expérience montre que ce sont plutôt des applications telles qu'un portail pour les patients (p. ex. pour la prise de rendez-vous), des solutions de sécurité de l'information ou des solutions de formation qui marquent le début de la transformation d'un hôpital vers le cloud. Il vaut la peine qu'un hôpital élabore et teste, dans le cadre de petits projets de mise en œuvre, la méthodologie qui est également déterminante pour les analyses de risques et les mesures de mise en œuvre dans le cadre de la mise en œuvre d'une stratégie de cloud computing pour le SIH.

3. „Omics" dans le cloud

Les caractéristiques biologiques et génétiques des personnes influencent l'efficacité d'un médicament ou d'une thérapie dans leur cas. Les scientifiques, les entreprises pharmaceutiques et les médecins obtiennent les données nécessaires à l'individualisation du traitement et des soins notamment grâce à des examens dits **omiques.** Celles-ci comprennent l'étude des prédispositions génétiques d'un individu **(génomique)**, l'analyse de la composition des protéines dans les tissus humains **(protéomique)** et l'analyse des produits du métabolisme **(métabolomique)**. Les résultats de ces mesures et analyses **omiques** permettent de déduire des indications sur les maladies existantes ou les risques de maladie, ainsi que des indications sur la manière dont les patients vont probablement réagir à une médication ou à un traitement.

4 L'annexe contient une liste de lois et d'ordonnances qui, avec les dispositions légales générales (par ex. la LPD ou les lois cantonales sur la protection des données), constituent le cadre légal pour l'utilisation du cloud dans le secteur de la santé.

5 Les exigences discutées ici découlent d'une part de lois (p. ex. lois sur les patients ou la santé, loi sur la protection des données, loi pénale), d'autre part d'obligations contractuelles (connexion au dossier électronique du patient) ou de réflexions sur les meilleures pratiques ou la bonne gouvernance, qui découlent en partie aussi de devoirs de diligence professionnelle.

6 Par exemple, L`art. 55 de la loi sur la santé du canton de Genève ; l`art. 33 de la loi sur la santé du canton de Valais.

7 Par exemple, les fonctions d'exportation et la prise en charge de la suppression automatique et du réglage des délais de conservation.

8 Dans le cadre des mandats de prestations cantonaux, les hôpitaux sont tenus de garantir à la population des soins hospitaliers de qualité et de sécurité suffisantes.

Exigences légales spéciales[9] aux mesures omics : Pertinence du cloud?		
Sujet	**Exigence**	**Influence du cloud**
Données : données de santé (traitement)	Respect du droit de la protection des données (fédéral et cantonal) et des droits de la personnalité	neutre
	Exigences en matière d'information, d'éducation et de consentement	neutre
	Protection de la confidentialité	neutre
	Protection de l'intégrité	neutre
	Évaluation uniquement avec consentement	neutre
	Principe du besoin de savoir	neutre
	Des protocoles pour garantir la traçabilité des opérations de traitement	neutre
	Transmission sécurisée des données	neutre
	Économie des données	neutre
Actions : transfert de données génétiques à l'étranger	Si le transfert à l'étranger est envisagé sans protection adéquate des données, une obligation de pseudonymisation s'applique[10] : la conservation des données dans un tel pays est interdite sans le consentement de la personne concernée pour les données génétiques qui n'ont pas été pseudonymisées.	neutre
Les actions : essais cliniques	Procédure d'autorisation et de déclaration	neutre
	Exigences en matière de conservation des données	neutre
Les actions : analyse génétique humaine	Interdiction de la discrimination	neutre

4. Intelligence artificielle/apprentissage automatique dans le cloud

L'intelligence artificielle (IA) et le Machine Learning (ML) gagnent en importance dans le domaine médical. Les domaines d'application possibles sont le diagnostic du cancer du sein ou du cancer du poumon ou la détection d'hémorragies cérébrales en tomographie assistée par ordinateur. L'accent est mis, par exemple dans le domaine de la radiologie, sur le développement de logiciels médicaux intelligents qui „apprennent" à chaque diagnostic.

Les logiciels intelligents sont aujourd'hui utilisés comme outils d'aide au diagnostic, où ce sont les médecins et non les machines qui établissent le diagnostic. Mais des recherches sont également menées sur des formes d'utilisation de l'IA et de la ML dans lesquelles le logiciel prend en charge au moins une partie du diagnostic, par exemple en réduisant la quantité de données à analyser lors de l'analyse de grandes quantités de données en éliminant les résultats d'un screening qui ne poseront probablement pas de problèmes. La médecine attend de l'IA et de la ML des avantages tels que la réduction de la charge de travail des médecins et l'augmentation de l'efficacité et de la précision.

D'un point de vue juridique, des questions se posent surtout concernant la qualification des logiciels intelligents en tant que dispositifs médicaux. Swissmedic et la Commission Européenne définissent des critères dont le respect permet de qualifier un logiciel de dispositif médical. Ces critères se réfèrent en premier lieu aux fins médicales poursuivies par le logiciel ou aux fins d'examen. Le mode de stockage et de traitement - „on-premises ou cloud" - n'a aucune influence sur ces critères. De même, la décision „on-premises ou cloud" ne change rien au fait que le logiciel soit un dispositif médical ou non.

9 La loi relative à la recherche sur l'être humain (LRH), Ordonnance relative à la recherche sur l'être humain à l'exception des essais cliniques (ORH), la loi fédérale sur l'analyse génétique humaine (LAGH), l'ordonnance relative à la LAGH (OAGH), la loi fédérale sur les produits thérapeutiques (LPTh) et l'ordonnance sur les essais cliniques hors essais cliniques de dispositifs médicaux (OClin) sont centrales.

10 La pseudonymisation des données génétiques est nécessaire pour le transfert de données vers des pays dont la législation, selon l'évaluation du Conseil fédéral (https://www.fedlex.admin.ch/eli/oc/2022/568/fr#annex_1), ne garantit pas une protection adéquate des données.

En outre, des questions de diligence médicale se posent lors de l'utilisation de logiciels basés sur l'IA/ML, ainsi que des questions de responsabilité. Là encore, il n'existe pas de directives spécifiques au cloud. Cloud ou non : les règles générales de diligence et de responsabilité s'appliquent.

Du point de vue de la protection des données, les dispositions relatives aux décisions individuelles automatisées peuvent être pertinentes dans le domaine de l'IA/ML. Toutefois, il n'y a décision individuelle automatisée que lorsqu'une décision entraînant une conséquence juridique ou un préjudice important est prise exclusivement de manière automatisée (c'est-à-dire par un logiciel ou une machine). Ainsi, tant que les logiciels médicaux intelligents ne sont utilisés qu'à titre subsidiaire, mais que les médecins établissent le diagnostic, les obligations d'information et les droits de consultation correspondants de la personne concernée en matière de protection des données ne sont pas pertinents. Même s'ils étaient pertinents, il ne s'agit pas non plus de dispositions dont l'application dépend du fait que le traitement automatisé a lieu „dans le cloud" ou „on premises".

5. Dispositifs médicaux dans le cloud

Les fabricants et les utilisateurs de dispositifs médicaux utilisent des services cloud sous différentes formes. Par exemple, les plateformes d'échange de données d'analyse issues de l'utilisation de stylos à insuline peuvent être stockées sur une infrastructure basée sur IaaS[11]. La plateforme elle-même peut être mise à disposition selon le modèle SaaS[12], ou bien le logiciel utilisé dans le dispositif médical contient des composants SaaS. En outre, SaaS est utilisé pour combiner des données provenant de différents dispositifs médicaux avec d'autres données - par exemple en les reliant à un SIH ou à un système d'information de laboratoire.

L'utilisation de composants cloud n'exerce aucune influence sur la qualification de dispositif médical. Selon Swissmedic, seul le but d'utilisation (finalité)[13] du logiciel détermine si le logiciel est un dispositif médical.[14] Le „cloud" n'est pas une finalité, mais un thème de mise en œuvre technique („chemin vers le but"). Par conséquent, l'utilisation des services cloud ne détermine pas si la réglementation sur les dispositifs médicaux est applicable.

Lorsqu'un logiciel est qualifié de dispositif médical, les exigences en matière de sécurité du produit et de gestion de la qualité des acteurs impliqués doivent être respectées. Ces exigences découlent de lois, d'ordonnances et de normes industrielles.[15] Une analyse des exigences légales montre qu'aucune exigence ne s'applique dans le contexte du „cloud" qui ne s'appliquerait pas en dehors de ce contexte. Toutefois, les aspects de la sécurité de l'information et d'autres aspects de la sécurité des produits spécifiques au „cloud" doivent être pris en compte lors du respect des exigences.

Sécurité de l'information

Les lois et autres directives exigent à juste titre une sécurité de l'information élevée dans le secteur de la santé. Cela vaut notamment aussi pour les exigences relatives aux logiciels lorsqu'ils sont considérés comme des produits médicaux. On ne peut pas répondre de manière abstraite à la question de savoir si la sécurité de l'information est suffisante. Il faut regarder la solution concrète. Les éventuels défis techniques de la réglementation sur les dispositifs médicaux ne peuvent pas être abordés ici. Ces derniers doivent être examinés au cas par cas, notamment en ce qui concerne les normes techniques industrielles, qui peuvent donner lieu à d'autres exigences.

11 **Infrastructure-as-a-Service** ; ces types des services cloud peut dispenser l'établissement de santé d'exploiter ses propres centres de données, son propre matériel et ses propres logiciels de serveur.

12 **Software-as-a-Service** ; ces types des services cloud sert à ce que l'institution de santé n'ait pas à exploiter et à entretenir elle-même certains logiciels (logiciels d'exploitation ou applications utilisateur).

13 Les définitions des dispositifs médicaux figurant à l'art. 3 ODim et à l'art. 3 OIPD énumèrent les objectifs qui permettent de qualifier le matériel ou le logiciel de dispositif médical.

14 Swissmedic, Fiche d'information sur les logiciels de dispositifs médicaux, 26 mai 2021.

15 La LPTh, la LRH, l'ODim, l'OICM et l'OClin-Mep sont pertinentes. En outre, il convient de respecter une série de normes industrielles, notamment en ce qui concerne la sécurité de l'information, la gestion des risques, la gestion de la qualité et l'assurance qualité des logiciels pour dispositifs médicaux et des logiciels pour appareils médicaux.

III RÉSERVES FRÉQUENTES ET SOLUTIONS POSSIBLES D'UN POINT DE VUE JURIDIQUE

Introduction

Malgré le fait que l'on s'accorde sur les valeurs fondamentales à protéger, il existe des malentendus dans le débat public sur le cloud. Parce que le besoin de protection est grand, il est fréquent de penser que le recours à des infrastructures informatiques tierces est un défi. Pour l'institution de santé, un service cloud peut souvent paraître plus complexe que sa propre infrastructure informatique familière. Les institutions de santé en déduisent alors qu'elles ne peuvent pas maîtriser le cloud. C'est sans doute pour cette raison qu'il existe des réserves à l'égard du cloud. Mais une fois que l'institution de santé s'est familiarisée avec le fonctionnement du service cloud et, dans de nombreux cas, avec le gain de sécurité de l'information qui en découle, la nouvelle infrastructure cloud est plus facile à gérer, permet de réaliser des économies et améliore la sécurité de l'information. De même, les réserves juridiques ne résistent souvent pas à un examen objectif. Certaines réserves exprimées dans le débat public sont abordées ci-après.

Réserves rencontrées en détail

Réserve 1 : „Le secret médical s'oppose à l'utilisation du cloud".

„Nous sommes tenus au secret médical. Nous ne pouvons pas le respecter en utilisant des services cloud. En outre, le traitement des commandes n'est pas autorisé par la législation suisse sur la protection des données si les obligations en matière de respect du secret professionnel ne peuvent pas être respectées. C'est pourquoi le secret médical s'oppose à l'utilisation du cloud".

Réponse : La réserve est infondée. Le secret médical peut être protégé et respecté même en cas d'utilisation du cloud.

L'utilisation des services cloud entraîne une externalisation du traitement des données. Dans le discours public, on suppose souvent un peu vite qu'une externalisation dans le cloud n'est pas possible sans que le fournisseur cloud ait accès aux données. De plus, il est avancé que seul un stockage crypté permet d'éviter que des personnes extérieures aient connaissance de données protégées par le secret.

Le secret médical (également appelé „secret des patients") doit être respecté par les détenteurs du secret - et pas seulement en raison de la menace d'une sanction pénale. La protection du secret permet aux patientes de confier à leur médecin des plaintes désagréables ou honteuses. C'est la seule façon de permettre un examen et un diagnostic minutieux avec la participation de la patiente. Il est donc compréhensible et important que les médecins évaluent soigneusement les services cloud - aussi et surtout en ce qui concerne les éventuelles violations du secret médical.

Le fait que le fournisseur cloud contrôle l'ensemble du système et puisse théoriquement avoir le pouvoir technique d'accéder aux données peut amener le médecin à penser qu'il donne inévitablement au fournisseur cloud la possibilité de prendre effectivement connaissance des données stockées sur l'infrastructure cloud. Cependant, cette supposition est incorrecte. Dans le cas des services cloud matures, il n'est ni nécessaire ni raisonnable de s'attendre à ce que des personnes extérieures - par exemple des collaborateurs du service de support du fournisseur cloud - „regardent" les informations et les perçoivent effectivement dans le cadre d'une utilisation normale et quotidienne de la solution (fonctionnement normal). Seules les machines - et non les personnes - accèdent aux données en fonctionnement normal. Le fournisseur cloud doit mettre en place des mesures techniques et organisationnelles afin de sécuriser cela. Les techniques de cryptage jouent déjà un rôle important selon le fournisseur. L'importance des mesures de cryptage, de l'encapsulation des informations et du routage contrôlé va encore augmenter à l'avenir.

Le secret médical (selon l'article 321 du Code pénal) n'est toutefois violé que si des personnes extérieures (humaines) perçoivent effectivement les informations enregistrées dans les données. Dans ce cas, on parle d'"accès en clair". Pour qu'il y ait punissabilité, il faut en outre que le médecin ou son auxiliaire (p. ex. assistante médicale) ait activement divulgué les informations ou qu'il ait omis, de manière fautive et contraire à ses obligations, de protéger les données de manière adéquate contre les accès en texte clair. Comme plusieurs avis juridiques l'ont déjà expliqué, ce n'est pas le cas lorsqu'on utilise des services cloud matures.

Il est essentiel que le client du cloud comprenne l'infrastructure de cloud utilisée par le fournisseur cloud et les processus garantis par ce dernier. En effet, seul celui qui comprend comment le traitement des données doit se dérouler chez le fournisseur cloud peut exercer un contrôle efficace. Cela implique que le fournisseur cloud soit disposé à se pencher sur les besoins de ses clients et à fournir des réponses solides.

Certains fournisseurs cloud peuvent avoir besoin d'accéder à l'environnement du client dans des situations très spécifiques souhaitées par ce dernier. Si le traitement de la demande de support n'est pas possible avec des exemples des données, il peut éventuellement y avoir un accès en texte clair aux données des patients. Si le médecin souhaite agir sans consulter ses patients, il doit inclure de tels fournisseurs cloud dans le cercle de ceux qui font partie du cabinet médical au sens large et donc de la sphère de responsabilité du médecin, en prenant des mesures contractuelles et organisationnelles. De nombreux fournisseurs cloud sont aujourd'hui prêts à donner des garanties contractuelles en ce sens.

Réserve 2 : „Le cloud augmente le risque de discrimination".

„Les données relatives à la santé sont des données particulièrement sensibles et dignes de protection. L'accès non autorisé à de telles données ou leur divulgation présente un risque élevé pour la personnalité et les droits fondamentaux des patients, notamment le risque d'être victime de discrimination. **L'utilisation des services cloud augmente l'impact et/ou la probabilité de discrimination.** Cela est inacceptable compte tenu du devoir de diligence des professionnels de la santé".

Réponse : La réserve est infondée. Le fait que l'utilisation des services cloud matures augmente le risque de discrimination ne peut être justifié objectivement.

Il est vrai que les données relatives à la santé constituent des données personnelles sensibles. Le risque de discrimination latent dans les données de santé doit être abordé et atténué - également, mais pas seulement, dans les projets de mise en œuvre du cloud.

Il n'est pas exact de dire que le recours à un fournisseur cloud entraîne en soi un accès par des tiers non autorisés. En tout cas, il ne faut pas l'affirmer de manière aussi générale. Tout dépend de la qualité du fournisseur cloud. Un fournisseur avec de mauvaises mesures de protection peut justifier un risque d'élargissement du cercle involontaire. Il peut alors y avoir des risques accrus.

Dans le cas inverse - utilisation d'un service cloud mature - la probabilité d'un accès non autorisé est réduite. Par conséquent, le risque de discrimination est également réduit.

Le fait que le risque de discrimination soit accru dans un scénario d'utilisation quotidienne et normale de la solution (fonctionnement normal) sans fuite de données chez le fournisseur cloud ne peut toutefois pas être justifié objectivement. Il convient de mentionner dans ce contexte que le risque d'une fuite de données chez le fournisseur cloud peut être réduit par des mesures techniques (et ne peut pas non plus être exclu dans le cadre d'autres infrastructures informatiques).

Réserve 3 : „Le cloud ne peut pas être contrôlé".

„Le déplacement de données vers l'infrastructure d'un fournisseur cloud entraîne la perte du contrôle direct de l'infrastructure et des données. La loi exige un tel contrôle direct, car les patients ne doivent pas être moins bien traités que si l'hôpital utilisait sa propre infrastructure".

Réponse : La réserve est infondée. Le cloud computing représente certes un changement de paradigme, mais il n'entraîne pas de perte de contrôle s'il est mis en œuvre de manière technique et permet même, le cas échéant, d'accroître le contrôle et la sécurité des informations.

Les institutions de santé évoluent dans un environnement très complexe. Elles doivent saisir les opportunités offertes par la digitalisation, sans pour autant perdre de vue des objectifs importants.

C'est une situation très exigeante dans laquelle se trouvent les institutions de santé aujourd'hui. Comment le cloud s'inscrit-il dans ce contexte ?

La réponse se lit d'abord comme un fardeau : les institutions de santé doivent maîtriser leur organisation. Cela vaut bien entendu aussi pour l'utilisation des services cloud par les institutions de santé. Les organes de direction doivent contrôler la situation dans son ensemble. Ils ne peuvent pas non plus simplement ignorer les prestataires tiers auxquels ils ont recours, comme justement les fournisseurs cloud.

Pour les institutions de santé qui ont jusqu'à présent évité les services cloud, l'intégration d'un service cloud dans leur propre organisation peut sembler à première vue un défi. L'analyse à cet égard est complexe et repose sur l'examen d'un grand nombre de facteurs. La règle reste la même : pour contrôler, il faut comprendre.

Exemple „Lieu de stockage"

Crainte : On ne peut pas savoir où les données sont stockées dans le cloud.

Classement : Aujourd'hui, la plupart des services cloud permettent aux clients de choisir eux-mêmes le lieu de stockage parmi les options existantes. Il est conseillé de choisir des fournis-seurs cloud qui garantissent par contrat qu'ils ne changeront pas de lieu de stockage, sauf si la cliente en fait la demande.

Exemple „Traitements à l'étrange"

Crainte : On ne peut plus savoir où les données sont traitées dans le cloud.

Classement : De nombreux fournisseurs cloud peuvent, au moyen de descriptions de processus, donner des indications claires sur les services qui entraînent un lien avec l'étranger et de quelle manière.

Exemple „Sous-traitant"

Crainte : On ne peut plus savoir qui accède aux données.

Classement : L'institution de santé n'a pas besoin d'acquérir une connaissance détaillée jusqu'aux différents individus impliqués chez le fournisseur cloud et/ou le sous-traitant. Elle peut se baser sur des réponses conceptuelles. Cela comprend l'identité des sous-traitants engagés et des informations sur les services auxiliaires qu'ils fournissent ou sur la manière dont ils traitent les données dans le cloud.

Pour que l'objectif de contrôle soit atteint, il faut embarquer les bonnes connaissances. Il faut avoir une vision transversale de la situation. Pour y parvenir, la direction peut se faire aider. Mais s'appuyer entièrement sur des ressources externes, c'est se rendre dépendant de l'approche de conseil. L'objectif de l'organisation de santé ne devrait pas être de servir uniquement la conformité à court terme, mais plutôt de s'adapter à la situation du cloud de manière complète et donc transformatrice. Celui qui reconnaît une transformation du cloud comme une chance pour le développement de sa propre organisation et l'extension de la sécurité de l'information, acquiert un véritable contrôle (au lieu d'une documentation de conformité) et fait un grand pas de fitness vers l'avenir. Une telle approche est de toute façon une bonne idée. Il est avantageux de s'y engager correctement dès le départ (on rate toutefois cette occasion avec une approche purement axée sur la compliance).

On ne peut contrôler que ce que l'on comprend. L'inverse est également vrai. Une compréhension suffisante des processus qui répondent aux objectifs de contrôle conduit au contrôle.

La compréhension doit porter sur les aspects essentiels des infrastructures cloud, des sites, de l'architecture et des contrôles de sécurité, des garanties contractuelles et des exigences légales et réglementaires applicables.

Les institutions de santé peuvent élaborer ces réponses. Elles peuvent donc également exercer un contrôle global dans le nouveau monde du cloud computing. Les moyens d'exercice du contrôle sont adaptés aux nouvelles conditions et souvent différents de ceux de l'époque où le personnel propre utilisait encore des appareils physiques.

Le fait que quelque chose soit différent ne permet pas de conclure à une perte de contrôle. Entre-temps, des instruments modernes comme les services cloud permettent d'obtenir un meilleur contrôle qu'auparavant. Mais en même temps, il est vrai qu'il n'est pas possible de faire des déclarations générales. L'infrastructure informatique utilisée concrètement doit être soumise à un contrôle dans le cadre de la méthodologie de contrôle et réussir les tests correspondants.

Perte de contrôle : point de cristallisation, échelle et point de départ de la méthodologie de contrôle

Les **exigences** suivantes doivent être vérifiées à l'aide de **questions de test :**

- Confidentialité : La confidentialité des informations à protéger est-elle assurée ?
- Disponibilité : La disponibilité est-elle assurée ?
- Intégrité : L'institution de santé peut-elle protéger l'information contre toute modification non souhaitée ?
- Intégrité : L'institution de santé peut-elle exiger de tiers la suppression de certaines informations qui sortent de l'infrastructure informatique ?
- Responsabilité : Les modifications apportées aux données ou l'accès à celles-ci doivent pouvoir être retracés sans ambiguïté à tout moment („audit trail").
- Continuité de l'activité : L'institution de santé peut-elle maintenir son activité à long terme même après avoir fait appel à un fournisseur cloud ?
- Traçabilité : L'institution de santé peut-elle garantir qu'elle peut décider à tout moment avec quel fournisseur informatique elle souhaite travailler ?

Les **points de contrôle** suivants sont importants pour pouvoir décider si l'institution de santé garde le contrôle sur les infrastructures informatiques auxquelles elle souhaite faire appel :

- Accès : Seules les personnes autorisées peuvent-elles obtenir et avoir un accès contrôlé aux infrastructures informatiques ?
- Accès en texte clair : Dans le cadre de la fourniture générale des services cloud, le fournisseur cloud a-t-il accès au contenu des données du client ?
- Support : Existe-t-il des processus clairs et garantis d'accès aux données en cas de support (lorsque le support est nécessaire) ?

Pour tous les points concrétisés ci-dessus, il convient de déterminer l'importance d'éventuels événements du type décrit (p. ex. une personne peut obtenir l'accès au centre de calcul) et l'impact de tels événements par rapport aux questions de test pertinentes sur le plan juridique (voir ci-dessus).
Les points de contrôle sont abordés à l'aide de mesures et il est ensuite vérifié si ces mesures sont appropriées pour partir du principe que le risque est raisonnable en ce qui concerne le point de contrôle à vérifier. Les mesures peuvent être de nature technique, organisationnelle ou contractuelle.

Réserve 4 : „Le cloud augmente les risques ; car il y a d'innombrables sous-traitants".

„Pour nous, en tant qu'hôpital, il est important de garder également le contrôle sur les fournisseurs de solutions IaaS, qui sont utilisés comme sous-traitants par les fournisseurs de logiciels de cybersanté. La sous-traitance est toutefois problématique, car nous ne contrôlerons pas directement les fournisseurs IaaS".

Réponse : La réserve est infondée. Le contrôle peut également être respecté en cas de recours à d'autres sous-traitants. Des mesures de protection contractuelles et organisationnelles sont notamment nécessaires à cet effet.

Le droit de la protection des données autorise le recours à des sous-traitants par les fournisseurs cloud. Des conditions préalables doivent être respectées, ce qui est toutefois régulièrement le cas dans la pratique.

Le fournisseur cloud auquel il est fait appel peut faire appel à d'autres prestataires (sous-traitants) pour exécuter ses prestations. Dans la mesure où ces derniers ont accès à des données personnelles (il suffit d'avoir accès à des données cryptées, c'est-à-dire sans accès en clair), les conditions suivantes doivent être mises en œuvre : l'autorisation de l'institution de santé est nécessaire, mais elle peut être donnée de manière générale et à l'avance. Le recours à d'autres prestataires par le fournisseur cloud ne constitue donc pas un élargissement du cercle , tant que l'institution de santé contrôle et maîtrise les risques.

Autorisation générale avec réserve de révocation

En ce qui concerne les services cloud, la variante de l'autorisation générale avec droit d'opposition est usuelle dans la branche et appropriée. Dans cette variante, le fournisseur cloud est tenu d'informer les clients de l'appel à de nouveaux sous-traitants ou du remplacement de sous-traitants existants et de leur permettre de s'opposer à l'appel, ce qui peut également être réalisé en leur accordant un droit de résiliation.

L'institution de santé devrait s'assurer que les exigences spécifiques découlant des prescriptions légales (p. ex. garanties concernant l'intégration de personnes auxiliaires sous le sceau du secret, etc.) sont prises en compte par le fournisseur primaire du système (fournisseur SaaS) et que les sous-traitants concernés ont également pris des dispositions correspondantes dans leurs contrats standard. Il devrait au moins y avoir une explication des principales relations, étayée par une documentation.

Réserve 5 : „Il faut une base légale explicite".

„Les hôpitaux ayant un mandat de prestations d'un canton doivent respecter **les lois cantonales sur la protection des données** lorsqu'ils traitent des données relatives à la santé. Les lois cantonales exigent que tous les traitements de données **reposent sur une base légale.** Cette base légale doit également couvrir l'utilisation du cloud".

Réponse : La réserve est infondée. Même les hôpitaux avec un mandat de prestations cantonal peuvent utiliser des services cloud sans base explicite dans la loi. Il faut une base légale dans une loi pour le traitement des données et pour certaines utilisations - mais pas pour la technologie utilisée (p. ex. cloud computing).

Selon la Constitution fédérale et les constitutions cantonales, les actions de l`État doivent avoir une base légale. Lorsque les autorités traitent (ou doivent traiter) des données personnelles dans leur domaine d'activité, elles doivent en principe disposer d'une autorisation spéciale explicite. Il ne doit pas y avoir de traitement de données par les autorités sans base légale. L'exigence d'une règle de droit est d'une grande importance dans un État de droit. En tant que règle de contrôle, la disposition poursuit les objectifs cardinaux suivants (dans le sens d'une soi-disant interdiction d'extension) : (a) contrôle sur des sujets importants (comprend la protection des données), (b) protection contre les débordements de l'État sans légitimation dans la règle de droit. Le seul fait qu'une autorité soit chargée d'une tâche ne doit pas être utilisé abusivement pour des traitements de données sans limites.

Si la loi garantit que (a) la portée de l'utilisation des données est pour l'essentiel connue ou peut être déduite du contexte (principe de transparence) et (b) que les finalités de l'utilisation des données ne sont pas excessives (principe de précision), l'exigence est satisfaite. Pour que les finalités ne soient pas excessives, elles doivent être décrites dans la disposition juridique pertinente. La technologie utilisée pour mettre en œuvre les étapes du cycle de vie des données n'est pas une finalité en soi. Le fait que des technologies telles que le cloud computing („chemin vers l'objectif") soient utilisées à des fins d'analyse des données ne modifie pas la finalité de l'utilisation.

Il ne fait pas partie des exigences de la règle de droit que les moyens d'exécution des tâches soient également limités en détail. C'est la raison pour laquelle aucune base légale autonome n'est requise pour les „activités administratives auxiliaires". Par activité administrative auxiliaire, on entend l'acquisition des biens matériels ou des prestations nécessaires à l'administration pour accomplir sa mission publique. L'achat de matériel de bureau, la conclusion de contrats d'entreprise pour la construction d'un bâtiment public ou le recours à un fournisseur de prestations TIC en sont des exemples. Dans la mesure où l'exigence d'une base légale est respectée pour l'activité de l'État proprement dite, qui nécessite une légitimation, l'activité administrative auxiliaire qui en fait partie est également couverte par la base légale et ne doit pas être mentionnée explicitement. Pour celles-ci, la base légale découle directement de la base juridique de la tâche publique concernée. Une base légale spécifique n'est pas nécessaire pour les activités de gestion de la demande.

Dans le cadre d'un projet de mise en œuvre, le respect du droit de la protection des données doit être assuré, notamment toutes les exigences relatives à la sécurité des données, donc à la technique, et le respect des principes de traitement des données. Les autorités cantonales de surveillance de la protection des données surveillent le projet de mise en œuvre de l'hôpital ayant un mandat de prestations cantonal.

Il existe donc déjà une protection suffisante par le droit de la protection des données. **En revanche, l'opinion selon laquelle les nouvelles technologies doivent toujours être régies par une loi au sens formel ne peut pas être maintenue.**

Dans le débat public, il est avancé que les citoyens ne devraient pas être moins bien lotis en cas d'utilisation des services cloud que si l'institution publique accomplissait la même tâche sans recourir à des services cloud. Ce point de vue implique l'idée que l'utilisation des services cloud n'est pas proportionnelle.

Sous cette forme globale, cela ne résiste pas à un examen juridique. En optant pour l'un des nombreux moyens appropriés, l'autorité dispose d'une grande marge d'appréciation dans le cadre de la gestion des besoins. Lors du choix du moyen, l'autorité doit tenir compte de l'intérêt public à une exécution efficace, économique et sûre des tâches publiques, tout comme des intérêts légitimes de protection des données des personnes concernées.

Il est donc nécessaire d'examiner au cas par cas les services cloud concrets, les types de traitement et le contexte ainsi que les types de données traitées. Il est tout à fait possible d'utiliser des services cloud de manière qu'il n'y ait pas d'atteintes pertinentes aux droits fondamentaux lors de l'exécution de la même tâche administrative.

Réserve 6 : „Un cloud présentant des risques d'accès aux autorités depuis l'étranger est inadmissible".

„Le risque d'accès par les forces de l'ordre ou les services de renseignement étrangers interdit l'utilisation des services cloud".

Réponse : La réserve est infondée. La discussion sur ce sujet prend aujourd'hui trop de place ; le sujet peut être résolu par des mesures techniques, organisationnelles et contractuelles.

Les pratiques des autorités dans tous les pays du monde devraient être classées et distinguées en deux catégories. Cette distinction est importante, car des considérations fondamentalement différentes doivent être prises en compte :

1. Surveillance : L'État a l'intention de procéder à des analyses de données sur un grand nombre de personnes. Un nombre indéterminé de personnes est concerné. Il s'agit de surveiller la société et éventuellement d'atteindre des objectifs de protection multiples ou indéterminés. Nous ne souhaitons toutefois pas vivre dans un État de surveillance.

2. Poursuite pénale : L'État a l'intention de mener une procédure pénale contre une personne accusée. Il s'agit d'un individu et non d'un nombre indéterminé de personnes. Il ne s'agit pas non plus d'objectifs de protection indéfinis, mais de permettre l'obtention de preuves contre un individu impliqué ou devant être impliqué dans la procédure.

IDans le premier cas **(surveillance)**, il s'agit de savoir si et dans quel but les actes de surveillance sont acceptables du point de vue de l'État de droit et de la société. On peut faire une distinction entre la surveillance de masse (p. ex. caméras vidéo enregistrant en permanence, toutes les prises de vue étant enregistrées dans un nouveau fichier et éventuellement examinées plus avant) et la collecte systématique de données (également appelée „Bulk Data Collection", p. ex. l'exploration d'un fichier concernant un grand nombre de personnes sur la base de critères de recherche „numéro de téléphone" ou „identifiant e-mail", seuls les résultats positifs étant enregistrés dans un nouveau fichier et éventuellement examinés plus avant). Du point de vue de la protection des données, ces questions sont abordées et résolues dans un contexte transfrontalier par les règles relatives à la communication à l'étranger.[16] Dans la pratique, le risque lié à ce type d'ingérence étrangère peut être réduit, voire totalement exclu sur de longues distances, par le choix du lieu de stockage (p. ex. en Suisse) ou par des mesures techniques (p. ex. cryptage).

Dans le second cas **(poursuites pénales)**, il faut évaluer dans quelle mesure les droits procéduraux de la personne concernée sont respectés dans la procédure pénale qui la touche. Il faut en outre décider qui doit veiller à ce qu'il en soit ainsi (le propre État, un État étranger ou, le cas échéant, un fournisseur cloud). Le motif de cette réflexion est par exemple le US CLOUD Act, qui permet aux autorités de poursuite pénale américaines d'exiger du fournisseur cloud actif dans leur propre pays qu'il mette en sécurité les données du client du cloud (legal hold), afin qu'elles puissent ensuite être utilisées dans une procédure pénale.[17] Cela doit être possible même si les données sont stockées à l'étranger[18] (tant que le fournisseur cloud a la possibilité de restituer effectivement les données[19]).

16 Tant les décisions d'adéquation selon l'art. 16 al. 1 LPD (y compris à l'avenir les règles relatives au Swiss-US Data Privacy Framework) que les mécanismes relatifs aux transferts dans le cadre des clauses contractuelles standard de l'UE (art. 16 al. 2 let. d LPD) abordent et résolvent cette question pour l'institutions de santé.

17 Voir déjà en détail sur le US CLOUD Act nos explications dans le livre blanc „Nuage public pour les services publics - Solutions pour les réserves fréquemment exprimées - non réservé aux autorités" (https://www.lauxlawyers.ch/wp-content/uploads/2023/02/Nuage-public-pour-les-services-publics.pdf)

18 Il devrait donc être possible de faire ce qui est prévu (pour certaines données : subscriber Information, mais pas les données de contenu) à l'article 18 de la Convention sur la cybercriminalité (CCC). Cette remarque est intéressante car la Suisse a adhéré à cet accord international.

19 En droit américain, on parle ici de „Possession", de „Custody" et de „Control". La résistance juridique part du principe, contrairement aux procédures, d'un accès immédiat au texte clair dès qu'un procureur américain demande un „legal hold" au fournisseur cloud. Or, ce n'est pas le cas. L'analyse des notions purement juridiques, comme la Possession, Custody et Control, ne va pas assez loin.

Le US CLOUD Act en bref : Qu'est-ce qui va changer?

En conclusion, qu'est-ce qui change exactement avec le US CLOUD Act? Dans le cadre du concept actuel d'entraide judiciaire internationale, les États-Unis reçoivent par exemple de la Suisse des données relatives au contenu (également appelées „content" ou, selon la terminologie de la Convention sur la cybercriminalité, „computer data"), le cas échéant sous certaines conditions. Si l'on parle de réflexions sur les risques, le statu quo devrait également être pris en compte. Aujourd'hui déjà, la Suisse fournit des données de contenu (computer data) aux Etats-Unis.

La discussion sur le US CLOUD Act concerne l'aspect **des poursuites judiciaires.** Mais elle est généralement menée de manière trop abstraite. Les juristes discutent des possibilités d'accès avec des approches de pensée purement juridiques. Mais cet examen ne répond pas à la question qui nous intéresse vraiment, à savoir : (1) s'il y a de facto des accès en clair par des autorités étrangères et (2) si les valeurs fondamentales de notre ordre juridique sont alors encore respectées. Ce que nous voulons en fait en tant que société et ce que veut la patiente : la patiente doit être protégée contre une utilisation abusive des données („élargissement incontrôlé du cercle"). Dans le contexte du US CLOUD Act, on ne peut toutefois pas parler sérieusement d'un „élargissement incontrôlé du cercle" ou d'une perte de contrôle juridiquement pertinente. Dans la discussion, on perd la focalisation sur l'essentiel.

US CLOUD Act : ne pas perdre de vue l'essentiel

L'hôpital doit protéger les données des patients contre les abus. Mais on ne peut en aucun cas considérer le US CLOUD Act comme un risque d'abus. Le US CLOUD Act ne s'oppose pas aux valeurs fondamentales mentionnées au début. Il est important de noter que les questions relatives à la protection du secret ne se posent que lorsqu'il est déjà possible de donner à la personne concernée le droit d'être entendue ou au moins à l'institution de santé des droits de participation. Ce point est abordé en détail dans l'avis de droit accessible au public pour la ville de Zurich.[20]

Cela étant dit, il ne s'agit plus que (mais tout de même) de savoir s'il est possible de gérer de manière appropriée le risque d'accès étranger qui subsiste dans le contexte du cloud. Dans le cadre des projets de mise en œuvre, il convient d'examiner et d'inventorier toutes les mesures de nature technique, organisationnelle et contractuelle, dans la mesure où elles servent à protéger les données du client contre la divulgation aux autorités étrangères. Tant le fournisseur cloud que le client (dans le cadre du projet de mise en œuvre) peuvent être tenus de mettre en œuvre de telles mesures.

20 www.lauxlawyers.ch/oiz-cloud-gutachten

Mesures contre l'accès des autorités		
Mesure	**Utilité contre surveillance**	**Utilité contre poursuite judiciaire**
Clauses „Defend Your Data" (Défendez vos données)	Oui	Oui
Pas d'accès au contenu des données des clients par le fournisseur[21]	Non	Oui
Reconnaissance du secret de fonction et du secret professionnel[22]	rarement[23]	Oui
Engagements de confidentialité	Non	Oui
Localisation du centre de données : Suisse	Oui	Oui
Organisationnelles (par ex. restrictions d'accès par des processus d'autorisation impliquant la cliente)	rarement[24]	Oui[25]
Cryptage	Oui	Oui
Autres mesures techniques	Oui	Oui

«Defend Your Data» désigne les clauses visant à protéger contre la divulgation de données aux autorités chargées de l'application de la loi, le fournisseur cloud devant mettre en œuvre une **cascade de défense** complète :

Cascade de défense	
Renvoi direct des autorités étrangères demandeuses vers la cliente	
en cas d'échec :	**Notification** immédiate de la cliente (et efforts pour remédier à une éventuelle interdiction d'informer)
en cas d'échec	**Contestation** judiciaire de : (a) les vices juridiques selon le droit américain[26] (b) les conflits avec le droit suisse[27]

21 Pas d'accès en texte clair du fournisseur cloud dans le cadre de la mise à disposition générale des services cloud ; processus d'accès aux données clairs et garantis en cas de support (si nécessaire).

22 Par example, Art. 320 CP, Art. 321 CP ; Art. 62 LPD).

23 Les bénéfices ne sont pas prévisibles et ne peuvent pas être présentés comme une mesure robuste dans le domaine de la surveillance de masse.

24 Les bénéfices ne sont pas prévisibles et ne peuvent pas être présentés comme une mesure robuste dans le domaine de la surveillance de masse.

25 Peut être traité comme une mesure dans le domaine de la protection de l'accès contre les mesures de la poursuite pénale étrangère aux Etats-Unis, „Control" à nier chez le fournisseur américain.

26 Si on le décrit de manière abstraite : „selon le droit de l'autorité qui le demande".

27 Les „blocking statutes" sont également à mentionner dans ce contexte. Sont en tout cas considérés comme tels les interdictions faites à une entreprise suisse d'aider une autorité étrangère sur le territoire suisse sans impliquer sa propre autorité compétente et sans coordonner la procédure avec elle (art. 271 CP, similaire: art. 273 CP). Les obligations de garder le secret selon l'art. 320 CP et l'art. 321 CP peuvent également en faire partie.

Selon la situation et le besoin de protection, il convient également d'examiner si l'on souhaite mettre en place une sécurité accrue, voire quasi absolue (p. ex. technologies de cryptage), pour le cas où la cascade de défense, plutôt marquée par le droit, ne serait pas efficace. Cela ne sera toutefois indiqué ou utile que dans de rares cas. L'hôpital ne doit pas une protection absolue contre les accès dans le cadre d'une procédure pénale (p. ex. selon le US CLOUD Act). Souvent, l'approche „Bring Your Own Key" (BYOK) est justement surestimée. „Hold Your Own Key" (HYOK) apporte certes plus de sécurité pour la discussion sur l'accès des autorités, mais cela se fait souvent au prix de risques supplémentaires injustifiables. Dans de nombreux cas, même avec HYOK, un (autre) fournisseur est impliqué, ce qui relativise aussitôt l'effet de protection obtenu.

Le cryptage : une bonne mesure entourée de mythes

Un cryptage complet de toutes les données clients dormants n'est pratiquement jamais obligatoire. Lorsqu'un tel cryptage est possible sans nuire considérablement à la conception du service ou aux possibilités d'utilisation des services cloud, il peut être tout à fait intéressant d'envisager, par exemple, la gestion des clés par l'hôpital lui-même.

L'expérience montre que les mesures esquissées ci-dessus (cascade de défense et autres mesures) conduisent dans leur ensemble à une protection de fait très étendue contre les accès des autorités étrangères.

US CLOUD Act : l'hôpital ne doit pas résoudre la tâche de la Confédération

Le monde numérique nous place devant de nouveaux défis. Si la Suisse veut faire valoir ses droits en matière de poursuite pénale, cela peut entrer en conflit avec les droits d'organisation d'autres États (l'inverse est également vrai). Les intérêts nationaux d'un État peuvent nécessiter l'accès à des données qui relèvent de la souveraineté territoriale d'un autre État. La Confédération devrait se pencher sur la question ; un hôpital ne doit toutefois pas résoudre ce conflit international. En revanche, l'hôpital doit seulement (mais tout de même) organiser son propre fonctionnement en accord avec le droit en vigueur. Cela implique qu'il doit protéger le secret médical. Le US CLOUD Act ne constitue toutefois pas un obstacle à cet égard.

Réserve 7 : „Le cloud est en contradiction avec la souveraineté des données".

„Les données relatives à la santé doivent être stockées en Suisse et ne peuvent pas être transmises au niveau international".

Réponse : La réserve est infondée. La souveraineté des données est une exigence d'action pour la Confédération, mais pas une limite pour l'institution de santé. Celle-ci doit nécessairement, mais aussi suffisamment, se conformer au droit suisse en vigueur.

Dans le cadre de la digitalisation, les efforts pour la souveraineté - la reconquête du contrôle que plusieurs États-nations ont progressivement perdu récemment - se concentrent de plus en plus sur l'économie en réseau. La souveraineté des données, en tant qu'aspect partiel important de la souveraineté numérique, formule ce qu'il convient de faire en matière de données pour que l'État devienne souverain. Dans le cadre de la discussion sur la souveraineté, la souveraineté des données signifie un rétrécissement du regard sur toutes les questions relatives aux données.

La souveraineté des données est une tâche que la Confédération doit assumer. Elle doit pour cela prendre des mesures dans le domaine interétatique. Cela peut conduire à des formes particulières de traités internationaux, dans lesquels les exigences centrales du point de vue Suisse - responsabilité en matière de garantie et points de départ sur la manière d'améliorer le commerce interétatique dans le trafic numérique transfrontalier - devraient être placées au premier plan. Un aspect central de la responsabilité en matière de garantie consiste à assurer l'accès à la justice.

Les entreprises comme les institutions de santé doivent se conformer au droit en vigueur. Dans la mesure où celui-ci reproduit les éléments clés de la responsabilité de garantie, l'institution de santé intégrera donc également les aspects de la souveraineté des données dans les objectifs de son projet. Un hôpital n'est toutefois pas tenu de respecter davantage que le droit en vigueur. La souveraineté des données ou la souveraineté numérique n'entraîne pas pour les institutions de santé d'obligations d'agir ou de s'abstenir allant au-delà du droit en vigueur.

Cette délimitation des compétences s'applique dans la même mesure que pour les institutions de santé privées aux hôpitaux de droit public ou aux autres institutions de santé des pouvoirs publics, comme l'a montré un récent avis de droit établi pour la ville de Zurich.[28]

L'expérience pratique montre que les institutions du secteur de la santé (tout comme celles du secteur financier et du secteur public) veulent très souvent, pour de bonnes raisons, aller plus loin que ce que la loi exige. Elles souhaitent assurer leur fonctionnement à long terme. Les départements informatiques de ces institutions accordent à juste titre une grande attention à la planification de la continuité. La motivation n'est toutefois pas le droit ni le débat sur la souveraineté, mais tout simplement ce qu'impose une gestion d'entreprise saine et prudente.

Conclusion : Que reste-t-il des réserves? Après avoir examiné les principales réserves à l'égard du cloud en tant que tel dans le domaine de la santé, il est clair que le scepticisme à l'égard du cloud ne peut pas être justifié objectivement. Il faudrait déplacer le centre d'intérêt et consacrer les énergies internes à la manière de se protéger et surtout de protéger les patients de manière optimale *avec* le cloud.

28 www.lauxlawyers.ch/oiz-cloud-gutachten

IV ANNEXES

Sur les éléments de l'analyse des risques

1. Un danger futur ne peut être décrit que par des déclarations de risque
Si nous savions ce que l'avenir nous réserve, les données de santé seraient également plus faciles à gérer sur des systèmes électroniques. Mais ce n'est pas le cas. L'institution de santé doit donc faire des prévisions sur l'avenir et examiner le niveau de risque que représente la gestion d'un système donné dans un contexte concret. Il est évident que la décision „cloud" ou „non-cloud" n'entraîne pas en soi plus ou moins de risques. Chaque choix de système nécessite une analyse de risque particulière. Ne pas entreprendre un changement vers un système plus sécurisé comporte autant de risques que de décider de changer et de rencontrer (également) des risques dans le nouveau système.

Les déclarations de risque devraient être faites comme suit :
- la situation souhaitée doit être décrite
- pour la situation souhaitée, il convient d'identifier les dangers potentiels.
- chacun des dangers identifiés devrait être évalué en fonction de sa probabilité d'occurrence (localisation en fonction de la probabilité d'occurrence, souvent appelée probability)
- chacun des dangers identifiés devrait faire l'objet d'une évaluation supplémentaire de son potentiel de dommage (localisation en fonction du potentiel de dommage, souvent appelé impact).

2. Les déclarations de risque comme synthèse de probability et d'impact
La combinaison de la probability et d`impact permet alors de faire une déclaration de risque.

Une crainte qui n'a pas beaucoup de chances de se réaliser et qui, si elle se réalise, fait peu de dégâts, est un **petit risque**.

Inversement, un danger qui se produit avec une grande certitude et qui, s'il se produit, cause à chaque fois de gros dégâts, est un **grand risque** (traverser une pente avalancheuse d'une inclinaison supérieure à 30° après des précipitations comporte un grand danger pour la vie et l'intégrité corporelle, et il est très possible qu'une avalanche se déclenche lorsqu'on traverse la pente).
Un événement potentiellement très dommageable, mais qui ne se produit pratiquement jamais (chute de météorites), est évalué différemment **(risque faible**) d'un événement au potentiel dommageable moyen, mais dont la survenue est très probable **(risque moyen)**.

3. Illustration par un exemple (information sur le groupe sanguin)
L'existence d'un potentiel de dommage et la manière dont il se réalise dépendent du **contexte.** Ce qui est important ici : le type d'information n'est pas nécessairement déterminant. Il n'y a pas d'automatisme en ce qui concerne les déclarations de risque. Cela vaut indépendamment du fait que dans le domaine de la santé, il s'agit de données personnelles sensibles. En d'autres termes, il n'existe pas de raccourci pour parvenir à une évaluation des risques adéquate. Il faut se mettre au travail et évaluer concrètement un risque. Les explications fournies dans la présente annexe visent à illustrer ce point.

L'information abstraite selon laquelle un nombre indéterminé de personnes ont le „groupe sanguin 0" est une information anonyme (la législation sur la protection des données ne s'applique pas ; **scénario 01**). Si un médecin indique qu'au cours de sa carrière de 35 ans, il a traité 8000 patientes de groupe sanguin 0 **(scénario 02)**, il exprime une information agrégée - l'affirmation est de nature statistique et repose sur des données personnelles réelles, mais les références à des personnes réelles ne sont plus reconnaissables. Dans le premier cas (information anonyme qui pourrait figurer dans un manuel), tout risque est objectivement exclu. Dans le deuxième cas, une certaine mise en danger (minimale) surviendrait éventuellement si une enquête était menée contre le médecin sur la base de l'information, dans le cadre de laquelle serait examinée la preuve qu'il s'est occupé d'un nombre aussi élevé de telles patientes. Indépendamment de cela : le risque est très faible dans les deux cas.

Cependant, si l'information „groupe sanguin O" est associée à une personne et donc individualisée, il faut distinguer d'autres scénarios pour décrire le risque, comme le montre ce qui suit :

• **Scénario 03 :** Lors d'une fête, quelqu'un raconte en passant, au cours d'une conversation, qu'il est également du groupe sanguin O. L'information est individualisée. Il n'y a pas de mesures particulières pour protéger l'information. Mais l'information est vite oubliée par l'interlocuteur ; elle ne l'intéresse pas. Il est difficile d'identifier un risque. Même si, au lieu du groupe sanguin, une information sur une maladie incurable existante avait été échangée : on pourrait partir du principe que le risque est faible.

• **Scénario 04 :** Quelqu'un enregistre les informations relatives à son groupe sanguin dans le dossier électronique du patient. Il s'agit donc de la déclaration „J'ai le groupe sanguin O". Il existe des mesures de protection prescrites dans des ordonnances. La personne concernée peut avoir des attentes très élevées en matière de sécurité technique et de protection de ses données.

• **Scénario 05 :** L'employeuse se trouvait par hasard à la table voisine lors de la fête (scénario 03) et a entendu l'information. Peut-être en déduira-t-elle quelque chose. Si les valeurs des groupes sanguins ont un potentiel de dommage dans le contexte concret ? Tout au plus, non. S'il s'agissait plutôt d'une information sur une maladie incurable qui entraîne normalement à court terme une incapacité de travail de plusieurs mois à plusieurs années, on voit que : contrairement au scénario 03, l'évaluation du risque pour le scénario 05 change si la nature de l'information change. Dans le scénario 03, il n'y avait pas d'évaluation du risque significativement différente malgré la modification de la situation, maintenant si ; car l'employeur pourrait avoir un intérêt à mettre fin à la relation de travail. On le voit bien : Le contexte particulier modifie l'évaluation des risques. En revanche, l'information en soi n'a pas modifié la situation de risque.

Conclusion : Ce n'est pas parce que des données personnelles sensibles sont traitées qu'il en résulte une „excursion" maximale sur l'échelle de contrôle (impact ou probabilité). Il ne serait pas défendable d'affirmer que les données relatives à la santé présentent toujours un risque maximal. Ce n'est pas le jeu de données (l'information) qui conduit à l'évaluation du risque, mais le **contexte**.

Après avoir mis en évidence la signification du contexte, il convient de passer en revue une autre „forme d'augmentation". Dans les exemples suivants, le „vrai sang" fait partie du processus, et pas „seulement" de l'information à son sujet :

• **Scénario 06 :** Un enfant joue au football. Pendant le jeu, un ballon touche l'enfant à la tête. Un saignement de nez se produit. L'enfant jette le mouchoir ensanglanté dans la poubelle. Le jour suivant, les éboueurs vident la poubelle. Il est évident qu'il s'agit d'une situation quotidienne. Bien qu'un échantillon de sang se trouvait dans la poubelle et que l'on aurait pu en déduire des informations sur le groupe sanguin, le risque est très faible que l'information sur le groupe sanguin soit effectivement recueillie de cette manière (ou même utilisée abusivement par la suite). Et si c'était le cas, le danger qui en découlerait est très diffus. Les liens avec l'enfant sont à peine visibles. Il faudrait que quelqu'un avec une très grande énergie criminelle s'en prenne déjà à l'enfant. En tout cas, dans la perspective actuelle de la Suisse, on peut dire que ce n'est pas notre expérience qui nous permet d'avoir autant d'énergie criminelle à chaque coin de rue. Il existe un faible potentiel de dommage avec une faible probabilité d'occurrence.

• **Scénario 07 :** Un coupable potentiel est accusé d'un délit grave (par ex. délit violent). Les autorités chargées de l'enquête manquent de preuves pour confondre le coupable. L'information sur le groupe sanguin pourrait permettre de confondre le coupable. Un enfant du prévenu a déposé un échantillon d'ADN auprès du service en ligne 23&me. Les autorités d'enquête tombent sur cette information et peuvent déduire le groupe sanguin de l'accusé à partir des données concernant l'enfant.[29] Cela permet ensuite de confondre l'auteur de l'infraction. Du point de vue de la personne concernée (l'auteur), il existe un potentiel de dommage considérable. Dans un premier temps (comme son enfant s'était enregistré auprès de 23&me), il fallait parler d'une faible probabilité d'occurrence. Au vu de l'énergie déployée par les autorités de poursuite pénale dans le cas actuel, le risque de probabilité d'occurrence a changé. Les autorités de poursuite pénale avaient profité de la gravité de l'affaire pour procéder à des investigations considérables (ce qu'elles ne font pas habituellement). La volonté de consacrer autant d'énergie à l'affaire a considérablement modifié l'analyse des risques. Cet exemple montre que c'est une fois de plus le contexte, et non l'information en soi, qui influence concrètement l'analyse des risques.

4. Ce qui reste

Qu'est-ce que cela signifie concrètement pour une institution de santé? Une chose est claire en tout cas : le fait que le désavantage maximal soit potentiellement possible ne doit pas conduire à la conclusion qu'il existe obligatoirement un risque incontrôlable ou élevé. Cela vaut également lorsqu'il s'agit de la gestion des données de santé. Si l'on partait d'un risque incontrôlable et que l'on considérait ainsi la voie du cloud comme inadmissible, on **occulterait** le **contexte.** Or, celui-ci est déterminant pour évaluer le risque. La position d'interdiction est inadmissible. L'approche basée sur les risques s'applique, pour laquelle toutes les circonstances (y compris celles qui plaident en faveur d'une utilisation du cloud ; comme des capacités de traitement massivement plus élevées, une plus grande sécurité en cas de panne ou une cybersécurité plus complète et toujours à jour, etc.) doivent être appréciées dans un contexte donné.

29 www.nytimes.com/2021/12/27/magazine/dna-test-crime-identification-genome.html

Liste des bases légales

1. Protection des données
- Droit fédéral de la protection des données : LPD, OPDo (RS 235.1; RS 235.11)
- Droit de la protection des données des cantons : p. ex. LPrD-VD, LIPAD-GE et ordonnances correspondantes
- Droit européen et international de la protection des données, selon le contexte : p. ex. RGPD de l'UE

2. Droit pénal
- Secret de fonction : art. 320 CP (RS 311.0)
- Secret médical : art. 321 CP (RS 311.0)
- Art. 62 LPD (RS 235.1)

3. Actes législatifs spéciaux de la Confédération en matière de droit de la santé
- Loi relative à la recherche sur l'être humain (LRH), Ordonnance relative à la recherche sur l'être humain (ORH), (RS 801.30; RS 810.301)
- Loi fédérale sur l'analyse génétique humaine (LAGH), Ordonnance sur l'analyse génétique humaine (OAGH) (RS 810.12 ; RS 810.122.1)
- Loi sur les produits thérapeutiques (LPTh) (RS 812.21)
- Ordonnance sur les essais cliniques (OClin) (RS 810.305)
- Ordonnance sur les dispositifs médicaux (ODim) (RS 812.213)
- Ordonnance sur les dispositifs médicaux de diagnostic in vitro (ODiv) (RS 812.219)
- Ordonnance sur les essais cliniques de dispositifs médicaux (OClin-Dim) (RS 810.306)
- Loi fédérale sur le dossier électronique du patient (LDEP) (RS 816.1)
- Ordonnances d'exécution de la LDEP (RS 816.11 ; RS 816.111)

4. Actes législatifs spéciaux des cantons en matière de droit de la santé
- Lois cantonales sur les hôpitaux ; par ex. Loi sur les établissements publics médicaux (LEPM) de GE, Loi sur les établissement et institutions sanitaires (LEIS) de VS
- Lois cantonales sur la santé ; p. ex. Loi sur la santé (LS) ct. VS, Loi sur la santé (LS) ct.de GE
- Mandats de prestations cantonaux des hôpitaux

5. Lois fédérales sur la sécurité sociale
- Loi fédérale sur la partie générale du droit des assurances sociales (LPGA) (RS 830.1)
- Loi fédérale sur l'assurance-maladie (LAMal) (RS 832.10)
- Loi fédérale sur l'assurance-accidents (LAA) (RS 832.20)

LAUX
LAWYERS AG
ZURICH | BASEL

BÜRO ZÜRICH
A Schiffbaustrasse 10
Postfach · CH 8031 Zürich
T +41 44 880 2424
W www.lauxlawyers.ch

BÜRO BASEL
A Steinenring 40 · CH 4051 Basel
T +41 61 283 0606
W www.lauxlawyers.ch