Avis de droit

À l'attn de	eHealth Suisse, organe de coordination Confédération-cantons
Établi par	Michael Isler, docteur en droit, En collaboration avec David Vasella, docteur en droit, et Dr Kerstin Noëlle Vokinger
Sujet	**Protection des données et sécurité de l'information dans le domaine de la santé mobile (mHealth)**
Date	19 janvier 2018 MIS / bme / 7480783v3

Table des matières

1. Synthèse

1.1. Contexte et problématique

1 Selon l'art. 8 de la loi sur le dossier électronique du patient (LDEP), le patient peut non seulement accéder à ses données (al. 1), mais également **saisir ses propres données** (al. 2) dans le dossier en question (**DEP**). Il est prévu que le patient bénéficie aussi de ces possibilités d'accès et de saisie via des applications mobiles spécifiquement développées dans le domaine de la santé (**applications mHealth**). Le présent avis de droit porte en premier lieu sur les données que le patient enregistre lui-même. Différentes questions en matière de protection et de sécurité des données se posent à cet égard.

2 Étant donné que le marché de la santé mobile a une dimension internationale et qu'il est plus développé dans l'Union européenne (**UE**) et aux États-Unis qu'en Suisse, l'avis de droit étudie le cadre juridique qui y est appliqué. En fonction des résultats obtenus, il sera possible d'identifier les points à adapter dans le droit suisse et de définir les mesures à prendre pour combler les lacunes.

1.2. Santé mobile : cadre juridique dans l'UE et aux États-Unis

1.2.1. Cadre juridique appliqué dans l'UE

3 Il n'existe pas de réglementation spécifique de la santé mobile au niveau européen. En 2014, la Commission européenne a toutefois résumé le cadre réglementaire dans son Livre vert sur la santé mobile (**livre vert**).

4 Plusieurs projets ont vu le jour suite à la publication du livre vert ; la Commission européenne a notamment lancé l'élaboration d'un code de protection des données collectées par des applications mHealth (**code de conduite UE**). La commission entend ainsi mettre à la disposition des développeurs d'applications mHealth un guide leur permettant de se conformer au droit européen en matière de protection des données et accroître ainsi la confiance des consommateurs dans cette technologie. Le code de conduite UE doit encore être adopté. Le cas échéant, il sera appliqué sur une base volontaire. Les développeurs qui ont obtenu la certification pourront figurer dans un registre public. La gestion du code est confiée à un organe de surveillance.

5 Le code de conduite UE s'inscrit dans le droit fil du Règlement général de l'UE sur la protection des données (**RGPD**), qui entrera en vigueur le 25 mai 2018 et abrogera la directive européenne sur la protection des données ainsi que les lois nationales en découlant. Les grands principes du RGPD dans le domaine de la santé mobile sont les suivants :

– le traitement des **données concernant la santé est strictement interdit sous réserve d'avoir été expressément autorisé**. Toute opération de traitement doit donc être motivée ; le consentement explicite de la personne concernée peut constituer un motif ;

– le principe de la ***privacy by design*** (protection des données dès la conception) implique l'obligation de prévoir les mesures nécessaires pour garantir la protection des données non pas au moment de traiter ces dernières mais à un stade antérieur ;

– le principe de la ***privacy by default*** (protection des données par défaut) prévoit, pour l'essentiel, qu'un produit ou un service doit être paramétré de manière à garantir au mieux la protection des données dès la première utilisation par la personne concernée ;

– la **sécurité des données** doit être garantie. Tout responsable du traitement de données est tenu de prendre des mesures techniques et organisationnelles pour garantir un niveau de protection adapté au risque. Ainsi, la sécurité des données ne revêt pas uniquement un caractère technique, mais doit être comprise dans sa dimension globale.

6 Les principes les plus importants (protection des données dès la conception, protection des données par défaut et sécurité des données) ne sont toutefois

pas applicables aux **fabricants** de systèmes (par exemple, développeurs de logiciels pour applications) s'ils ne sont pas eux-mêmes responsables du traitement des données. Le code de conduite UE entend combler cette lacune en incitant les fabricants à faire **certifier que leurs produits sont conformes aux règles de protection des données**.

1.2.2. Cadre juridique appliqué aux États-Unis

7 Aux États-Unis, tant la communauté scientifique que des autorités publiques comme la *Food and Drug Administration* (**FDA**) encouragent le développement et l'intégration de la santé mobile. Le pays met l'accent sur la réglementation des dispositifs médicaux, sans pour autant négliger la protection des données.

8 Par rapport à l'Europe, les États-Unis interprètent cette dernière notion de façon diamétralement opposée. La libre exploitation des données en tant que bien économique prend le pas sur la protection de leur caractère personnel. Cela étant, il existe aux États-Unis une multitude de prescriptions sur la protection des données applicables à des secteurs ou à des évènements particuliers, au niveau national et dans les différents États. Dans le domaine de la santé, le *Health Insurance Portability and Accountability Act* (**HIPAA**) et le *Health Information Technology for Economic and Clinical Health Act* (**HITECH**) constituent les textes de référence. Ils réglementent la protection des données de santé non-anonymisées (informations médicales protégées) et fixent les sanctions correspondantes. Trois principes priment :

- la ***privacy rule*** fixe les prescriptions minimales encadrant la protection des données, l'utilisation et la publication d'informations médicales protégées ;
- la ***security rule*** vise à garantir la sécurité des données de santé électroniques à quatre niveaux (mesures de protection au niveau administratif, physique, organisationnel ainsi qu'au niveau des directives et des processus) ;
- la ***breach notification rule*** impose que les patients concernés et l'organe de surveillance compétent soient informés des cas de violation des obligations en matière de sécurité des données.

9 Les obligations susmentionnées ne valent pas pour l'ensemble des applications mHealth, mais uniquement pour celles traitant des informations médicales protégées. Il s'agit exclusivement des cas où des employés de services de santé ont

accès à l'application en question ou communiquent des informations au patient via ce canal. Ainsi, les applications ne servant qu'à alimenter le système de santé de données concernant un patient ne sont pas soumises aux strictes prescriptions du HIPAA ni du HITECH. Dans la pratique, toutefois, la *Federal Trade Commission* recourt également à des **normes similaires** pour examiner les infractions à la sécurité des données commises **dans d'autres secteurs**.

1.2.3. Appréciation générale

10 Aussi bien dans l'UE qu'aux États-Unis, **la protection des données de santé revêt une importance majeure**. Aux États-Unis, le champ d'application du HIPAA et du HITECH ne concerne certes directement qu'un nombre limité d'applications mHealth, mais des normes de sécurité comparables sont aussi appliquées dans les secteurs où le traitement de données sensibles est répandu.

11 Dans l'UE, le traitement des données concernant la santé est soumis à un cadre général strict. L'avenir dira si le RGPD peut être appliqué efficacement dans le contexte international. Dans le domaine de la santé mobile, il faut s'attendre à ce que les fournisseurs d'applications soient désormais plus attentifs à la protection des données. La conformité en matière de protection des données devrait constituer un atout concurrentiel, d'autant plus si les fournisseurs d'applications sérieux adoptent le code de conduite européen.

1.3. Adaptations nécessaires du droit suisse

1.3.1. Cadre suisse en matière de protection des données pour les applications mHealth

12 Même si les fournisseurs d'applications mHealth évoluent dans un contexte mondial et que très peu ont installé leur siège social en Suisse, les prescriptions suisses sur la protection des données sont applicables à toutes les données personnelles traitées sur le territoire.

13 La loi fédérale sur la protection des données (**LPD**) fait actuellement l'objet d'une révision visant à garantir sa compatibilité avec le RGPD. L'avis de droit tient compte de cette révision dans la suite du développement.

14 La LPD poursuit une autre approche que son pendant européen. Cette loi n'autorise pas le traitement des données exclusivement sur autorisation expresse mais impose **un principe de transparence sous réserve d'interdiction**.

En règle générale, le traitement des données n'est pas subordonné au consentement de la personne concernée. Les **principes fondamentaux** suivants doivent cependant être respectés :

– principe de la transparence ;

– principe de l'affectation ;

– principe de la proportionnalité ;

– principe de l'intégrité des données ;

– principe de la sécurité des données.

15 Les données de santé sont des **données sensibles**, raison pour laquelle leur traitement est régi par des prescriptions spécifiques sur le plan de la transparence. En outre, il est interdit de communiquer des données de santé à des tiers, sous réserve du consentement de la personne concernée ou d'un autre motif justificatif.

16 L'approche suisse est donc plus libérale que l'approche européenne, **le niveau de protection n'en reste pas moins élevé**. Si l'opération de traitement dépasse le but primaire fixé dans le cadre de l'application, elle ne respecte plus le principe de proportionnalité ou, dans le cas où des données de santé sont portées à la connaissance de tiers, elle est interdite. Ainsi, au sens du droit suisse également, le traitement de données dérogeant au but primaire requiert le consentement de la personne concernée. Il n'y a donc pas lieu d'adapter la législation à ce niveau.

1.3.2. Exigences de la LDEP

17 Il n'existe pas de règle particulière spécifiant les modalités pour relier des applications mHealth au DEP. Dans les solutions actuelles, l'intégration de ces applications au DEP est généralement moins poussée que pour les **systèmes primaires**, où le niveau d'interaction est plus important ; partant, **les exigences** pour raccorder les systèmes en question (inventaire, garantie de la protection et de la sécurité des données) **ne peuvent être reprises en l'état pour les applications mHealth**. Par contre, il est indispensable que les applications mHealth qui sont reliées au DEP via un dispositif mobile respectent des exigences minimales de protection et de sécurité des données.

18 Pour l'heure, il est prévu que les données collectées par de telles applications ne puissent être converties et classées dans le DEP que si le patient a consenti au transfert de données, et ce, au cas par cas. Ce mode de fonctionnement n'est pas particulièrement convivial. Toutefois, si une **solution de transmission automatique de données** depuis une application directement dans le DEP via le portail d'accès du patient devait être mise en place (authentification entre appareils), il faudrait, **au préalable, recueillir le consentement général du patient**. En outre, cette opération impliquerait que les applications mHealth concernées répondent à des exigences de sécurité et de protection élevées. À l'heure actuelle, l'art. 23, let. b et c, de l'ordonnance sur le dossier électronique du patient (ODEP) fait obstacle à une telle solution dans la mesure où il y est précisé que le moyen d'identification doit être conçu de manière à ce que seule la personne autorisée puisse l'utiliser et qu'une procédure d'authentification comportant au moins deux facteurs d'authentification soit utilisée.

19 Enfin, les communautés de référence sont tenues de recommander aux patients des mesures de protection et de sécurité des données. Cette **obligation d'information et de renseignement** s'étend à l'utilisation d'applications mHealth.

1.3.3. Comparaison

20 La comparaison entre le cadre législatif suisse (en tenant compte de la révision de la LPD) et celui applicable dans l'UE et aux États-Unis en matière de protection des données est résumée dans le tableau ci-après :

Thème	UE (RGPD)	USA (HIPAA)	CH (P-LPD)
Approche réglementaire	réglementation de portée générale fondée sur une combinaison de normes et de principes ; nombreuses initiatives de santé mobile	fondée sur des normes et sectorielle ; sécurité de l'information en général : également une approche fondée sur le principe du caractère raisonnable (*reasonableness*), encadrée par des lignes	fondée sur des principes et de portée générale

Thème	UE (RGPD)	USA (HIPAA)	CH (P-LPD)
		directrices relativement concrètes surveillées par la FTC	
Principes pour le traitement des données de santé	interdiction expresse de traitement assorti d'une réserve d'autorisation	impératif de transparence et interdiction de communiquer	impératif exprès de transparence et interdiction de communiquer
Protection des données dès la conception / par défaut	oui	les prescriptions du HIPAA doivent être applicables	oui
Sécurité des données	réglementation fondée sur des principes, pas de normes contraignantes ; analyse d'impact relative à la protection des données en tant qu'instrument de la prévention des risques	prescriptions spécifiques ; *Information Security Standard* du NIST (non contraignant)	réglementation fondée sur des principes, pas de normes contraignantes ; analyse d'impact relative à la protection des données en tant qu'instrument de la prévention des risques
Obligation de déclarer les cas de violation de la sécurité des données	à l'autorité compétente et, le cas échéant, aux personnes concernées	aux personnes concernées et à l'autorité compétente (si le seuil minimal d'individus concernés n'est pas atteint : déclaration annuelle)	à l'autorité compétente et, le cas échéant, aux personnes concernées

Thème	UE (RGPD)	USA (HIPAA)	CH (P-LPD)
Procédure de certification pour les produits (par exemple applications mHealth)	prévue mais rarement utilisée code de conduite UE	pas prévue	prévue, mais non appliquée jusqu'ici

1.4. Mécanismes de mise en œuvre

1.4.1. Mesures de protection préventives

21 Le contrôle préventif constitue le mécanisme de mise en œuvre le plus efficace. En tant que **contrôleurs des accès**, les **communautés de référence** jouent un rôle crucial dans le cadre du raccordement des applications mHealth au DEP. Il leur revient fondamentalement d'appliquer et d'imposer les critères pour relier ces applications.

22 Les instruments ci-après peuvent être utilisés :

– **Mesures de droit administratif** (critères de vérification et normes pour le raccordement des applications mHealth) ;

– **Mesures contractuelles** (réglementer l'intégration des applications dans le DEP par voie de contrat) ;

– **Mesures techniques et organisationnelles** (audits, monitorage des solutions de santé mobile).

23 La question se pose toutefois de savoir si les communautés de référence peuvent et veulent assumer ces **tâches exigeantes** ; la gestion des accès à plusieurs niveaux pourrait, de surcroît, segmenter davantage le marché déjà restreint de la santé mobile en Suisse. Il serait possible de surmonter cette difficulté :

– en autorisant les **portails d'accès externes**, dans la loi et le droit d'exécution, avec droit d'écriture pour les patients, et/ou

– si l'Office fédéral de la santé publique (**OFSP**) se voyait confier une **fonction de soutien** dépassant la mission de mettre en place des conditions de certification.

Dans les deux cas, il faudrait **adapter la loi et le droit d'exécution**.

1.4.2. Recours de l'utilisateur final

24 La protection des données repose en premier lieu sur le principe selon lequel toute personne assujettie au droit respecte les dispositions juridiques. L'effet dissuasif des sanctions et la dénonciation publique des infractions poussent également les personnes à suivre les règles. L'utilisateur final dispose certes de voies de recours lui permettant de défendre ses intérêts personnels, mais la **procédure civile** notamment est **onéreuse**, et le fardeau de la preuve incombant dans une large mesure au demandeur, cette procédure n'est pas sans **risque**. Selon le cas, l'utilisateur peut également recourir à la **voie pénale** ou déposer une **plainte auprès de l'autorité de surveillance**.

1.5. Mesures recommandées

25 Les mesures recommandées figurent dans le tableau ci-après :

N°	Mesure	Base légale
1	Réfléchir à la mise en place décentralisée, par les communautés de référence, des portails d'accès pour les patients ; évaluer la possibilité d'autoriser les portails d'accès externes donnant aux patients un droit de lecture et leur permettant également de mettre des données à disposition au sens de l'art. 8, al. 2, LDEP (sous réserve de modification de la loi)	LDEP 1 IV LDEP 10 II LDEP 11 (b) ODEP 30 s.
2	Éviter de raccorder l'application mHealth à l'identité électronique du patient (numéro d'identification du patient)	ODEP 10 III ODEP 12 IV
3	Permettre un transfert automatique des données par les applications mHealth (entre appareils) uniquement à des	ODEP 23 (b) ODEP 23 (c)

N°	Mesure	Base légale
	conditions strictes en matière de protection et de sécurité des données (sous réserve de modification de l'ordonnance)	
4	Sensibiliser les patients et les professionnels de la santé aux risques liés à la protection des données dans le cadre d'applications mHealth ; élaborer une fiche d'information à l'intention des communautés de référence	ODEP 15 II
5	Élaborer un catalogue de critères pour imposer des exigences minimales en matière de protection des données auxquelles doivent répondre les applications mHealth à raccorder, y compris obligation de contrôler (due diligence) que les applications satisfont auxdites exigences	LDEP 12 I (b)
	Confier au DFI (OFSP) la responsabilité d'établir le catalogue de critères	LDEP 12 II
	Confier la due diligence à l'OFSP (et non aux communautés de référence ; sous réserve de modification de la loi et de l'ordonnance), réalisation de ce contrôle par un portail d'accès externe également envisageable (cf. mesure 1)	LDEP 30 III
6	Édicter des prescriptions pour déterminer le raccordement d'applications mHealth par voie contractuelle	LDEP 12 I (b) ODEP 12
	Élaborer un modèle (librement utilisable) de contrat d'intégration régissant le raccordement d'applications mHealth à l'interface du DEP en conformité avec le droit suisse.	n/a