Lundi 14 décembre 2015

Dossier électronique du patient: quo vadis? Dulcius ex asperis!

Sébastien Fanti | Avocat et Notaire | Préposé à la protection des données et à la transparence | sebastien.fanti@admin.vs.ch

Sommaire

- Prolégomènes confessoires
- Définition du Big Data (données massives)
- Référentiel légal
- L’exemple du dossier électronique du patient
- Safe Harbor, what else?
- Droit à l’oubli
- Conclusions
- Q & A

Prolégomènes confessoires

Nécessité absolue de formation permanente:

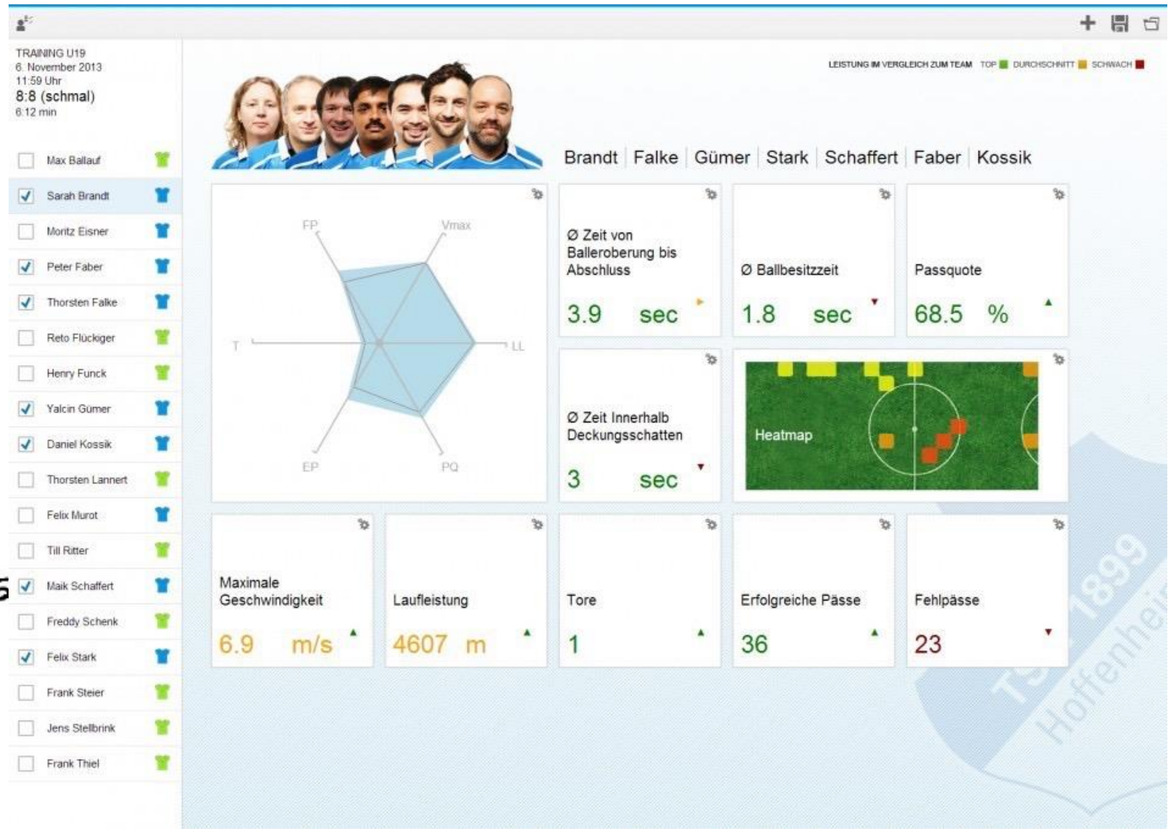
- Conseiller en protection des données HEIG-VD (2014)
- Information Security Lead Auditor ISO 27001 :2013 (2015)
- Security Management Lead Implementer ISO 27001 :2013 (2015)
- Certified Lead Privacy Implementer ISO 29100 (2015)
- Doctorat en droit (2016?)
- MBA Media Leadership (2016?)

Fanti est incompétent car il a dû faire appel à un auxiliaire, soit à un expert en intrusion!

Sur 330’000 sociétés suisses combien sont certifiées ISO 27001?

Définition du Big Data (données massives)

"Your recent Amazon purchases, Tweet score and location history makes you 23.5% welcome here."



Définition du Big Data (données massives)

assuré SF - management du risque

sources de données alpha:
FB, instagram, withings (applicatif), Runkeeper, GPS, Internet (courses…)
sources de données bêta:
balance connectée, montre connectée, web, GPS
sources de données omega: dossier patient, tests génétiques

Référentiel légal incomplet et discrépant

Les normes actuelles sur le plan fédéral et cantonal permettent d'appréhender le Big Data (art. 3 al. 1 LPD).

Un argument souvent invoqué dans le contexte des données massives est que, dans la plupart des cas, seules des données factuelles ou anonymisées sont collectées et que les dispositions relatives à la protection des données ne s'appliquent donc pas.

La difficulté que présentent les données « factuelles » ou « anonymisées » dans le cadre des données massives est qu'on ne peut pas exclure que le rapprochement de plusieurs collections de données n'entraîne une désanonymisation. Dans de nombreux cas, l'anonymisation des identificateurs particuliers évidents ne suffit pas à exclure toute ré-identification.

Référentiel légal incomplet et discrépant

Transparence: chacun a le droit de savoir quelles sont les données le concernant qui sont traitées, par qui et dans quel but: traitement et la connexion de données provenant de différentes sources est très opaque et difficilement vérifiable par les personnes concernées.

Consentement: nécessite de connaître le but! antinomique ave le principe des données massives, celles-ci impliquant la constitution de stocks de données qui serviront ultérieurement à un but non encore déterminé

Précision: les procédures d'analyse créent de nouvelles informations liées à des personnes, sans qu'il soit possible de les qualifier d'exactes ou de fausses, puisqu'elles ne constituent que des probabilités ou des interprétations.

Référentiel légal incomplet et discrépant

Nécessité de tenir compte de la protection des données lors de la conception: privacy by design ou privacy by default; problème: aucune norme en CH ne l'impose; deux postulats acceptés par le Conseil fédéral (J.-C. Schwaab).

Une révision législative du droit fédéral s'impose! Le problème : coordonner nos actions avec l'UE qui a adopté une nouvelle Directive qui sanctionne lourdement les manquements aux incombances légales.

Quid des normes de sécurité à respecter?

Multiplicité de défis protéiformes

1. **Minimisez la collecte des données** : la proposition de loi de l'UE comporte des exigences strictes en ce qui concerne la limitation des données recueillies auprès des consommateurs. Les acteurs du marketing et de l'informatique doivent prendre le temps d'examiner les données demandées sur tous les formulaires Web orientés vers l'extérieur.

2. **Signalez rapidement** : la notification des atteintes à la protection des données constitue une nouvelle exigence que les entreprises européennes devront respecter. Pour les données non structurées, cela signifie que vous devrez mettre en place une supervision des fichiers en temps réel pour détecter les accès non autorisés et enregistrer ce qui a été exposé.

3. **Conservez les données avec précaution** : les règles de minimisation de la nouvelle loi concernent non seulement l'étendue des données collectées, mais aussi leur durée de rétention. Vous ne devez pas stocker les données plus longtemps que « nécessaire aux fins prévues ». Si vous n'avez pas consulté votre stratégie de rétention des données récemment, il est temps de l'examiner. Et de vous assurer que vous disposez des outils d'automatisation appropriés pour appliquer votre stratégie.

4. **Attention à la nouvelle définition des identifiants personnels** : l'UE a étendu la définition des identifiants personnels et ce changement s'avère important parce que la loi européenne met l'accent sur leur protection. Possédez-vous la liste de tous les fichiers contenant ces identifiants personnels et savez-vous si leurs accès sont appropriés ?

5. **Employez un langage clair dans votre politique de confidentialité** : il vous faudra le consentement préalable et explicite des consommateurs lors de la collecte de leurs données.

6. **Trouvez votre bouton d'effacement** : le « droit d'effacement » signifie qu'en cas de retrait du consentement accordé par les consommateurs, les sociétés devront supprimer les données concernées de tous les endroits où elles se situent. Et cela comprend aussi toutes les données non structurées des consommateurs présentes dans votre système de fichiers.

7. **N'oubliez pas le cloud** : il n'échappe pas à la nouvelle loi de l'UE ! En effet, les règles suivent les données. Vous devrez vous assurer que vous disposez des langues appropriées dans vos contrats avec le fournisseur de cloud et les autres processeurs de données tiers.

L'exemple du dossier du patient

Base légale fédérale exsangue et génératrice de problèmes: loi fédérale sur le dossier électronique du patient!

10 La sécurité des données est-elle garantie dans le dossier électronique du patient ?

La sûreté de l'information et la protection des données sont considérés comme des priorités absolues dans le cadre du dossier électronique du patient. Pour les garantir, la loi fédérale sur le dossier électronique du patient prévoit les mesures suivantes :

- les données sont enregistrées de manière décentralisée ;
- les professionnels de la santé et les patients doivent se connecter avec une identité électronique sécurisée ;
- les accès aux données sont consignés dans des historiques que peuvent consulter les patients ;
- les communautés et les portails d'accès font l'objet de certifications qui doivent être renouvelées régulièrement ;
- en outre, tout accès non autorisé au dossier électronique du patient est puni.

L'exemple du dossier du patient

Base légale fédérale exsangue et génératrice de problèmes: loi fédérale sur le dossier électronique du patient!

Art. 8 Critères de certification

[1] Le Conseil fédéral fixe les critères de certification en tenant compte des normes internationales en la matière et des progrès techniques, en particulier en ce qui concerne:

a. les normes, les standards et les profils d'intégration applicables;

b. les critères de protection et de sécurité des données;

c. les prescriptions organisationnelles et les prestations à fournir;

d. l'obligation d'historiser tous les accès au dossier électronique du patient.

[2] Il peut charger l'Office fédéral de la santé publique d'adapter aux progrès techniques les critères visés à l'al. 1, let. a.

L’exemple du dossier du patient

Base légale fédérale exsangue et génératrice de problèmes: loi fédérale sur le dossier électronique du patient!

Section 5 Dispositions pénales

Art. 17

[1] Est puni d’une amende de 100 000 francs au plus, pour autant que le code pénal[4] ne prévoie pas de sanction plus grave, quiconque accède intentionnellement et sans droit à un dossier électronique.

[2] Si l’auteur agit par négligence, l’amende est de 10 000 francs au plus.

L’exemple du dossier du patient

Base légale cantonale:

Section 6: Protection des données

Art. 17 Confidentialité des données

[1]Les données récoltées sont traitées confidentiellement, dans le respect des normes imposant le secret professionnel ou le secret de fonction et de la législation sur la protection des données.

[2]Le comité de direction dans la phase de développement puis l'organisme responsable du système d'échange d'information dans la phase d'exploitation collaborent avec l'autorité cantonale chargée de la protection des données pour assurer le respect des normes en vigueur.

Art. 18 Utilisation des données à des fins statistiques

L'utilisation à des fins statistiques de données anonymes ne permettant pas d'identifier les patients concernés est autorisée.

Art. 19 Mesures organisationnelles et techniques

[1]Des mesures appropriées sont prises pour la protection des données enregistrées contre les risques de falsifications, de destruction, de vol, de perte, de copies et autres traitements illicites.

[2]Ces mesures doivent notamment permettre la traçabilité du traitement (création, modification et accès) des données enregistrées au sein du système d'échange d'information.

Ordonnance concernant le système d'échange d'information sanitaire (Ordonnance «Infomed»)

du 18 septembre 2013

Safe Harbor, what else?

Ce régime offre l'avantage de ne pas devoir négocier un contrat avec un partenaire américain enregistré.

Nonobstant les réticences de la Commission européenne (http://europa.eu/rapid/press-release_MEMO-13-1059_fr.htm), dès lors que le Préposé fédéral maintient sa confiance au processus, il suffit que l'entreprise américaine ait intégré le programme pour que l'on considère que le niveau adéquat de protection des données soit atteint. Tel est le cas en l'occurrence. Il peut donc être considéré sur le principe que les conditions figurant dans la LIPDA (cf. article 25 LIPDA notamment) en termes de protection des données sont remplies (articles et que le formulaire peut être utilisé **pour l'instant.** La situation pourrait s'avérer différente, notamment au terme de l'assesment conduit par la Commission européenne.

Après discussion avec le Préposé fédéral, il s'avère que celui-ci attend la décision de la Commission européenne (des négociations sont en cours en avec les États-Unis en sus de l'assessment précité), ainsi qu'une décision de la Cour de justice de l'Union européenne devant laquelle une procédure est en cours s'agissant spécifiquement de la garantie du niveau adéquat de l'accord Safe Harbor (cf. http://bakerxchange.com/cv/b23f91d3e436568a4954bff45049448a6486b4da/p=2460666).

Si au terme de l'assessment ou de la procédure devant la Cour le niveau adéquat devait être nié, l'article 25 alinéa 2 LIPDA trouverait alors application.

Droit à l'oubli: en matière médicale

Les données qui ne sont plus nécessaires au maître du fichier doivent être détruites.

Le médecin doit détruire ou rendre au patient les dossiers médicaux à l'échéance du dossier du conservation. Il peut devoir détruire les données avant l'échéance du délai de conservation des données à la demande du patient.

Quid en cas de dossier électronique du patient détenu par une assurance, un Canton ou une société privée?

Il y a une impérieuse nécessité de déterminer dans la loi les conditions d'exercice d'un droit à l'oubli s'agissant des données médicales.

Conclusions:

Le système de santé a besoin de données pour agir

L'analyse prédictive fondée sur le Big Data permettra dans quelques années de déterminer, avec précision, le niveau de risque intrinsèque pour une personne de développer une maladie et de chiffrer les coût prévisibles (Health Rating Risk). Y aura-t-il encore une place pour l'imperfection qui ne soit l'objet d'une appréhension informatique?

La question n'est pas de savoir quand et comment cela sera possible, mais de déterminer quelle part intangible de l'individu nous voulons soustraire à la capacité d'analyse (eHealth-Habeas Corpus). Et vous quelles données médiales êtes-vous prêts à partager?

Merci de votre attention
suivez nous sur

Twitter: @preposeVS
Facebook: https://www.facebook.com/preposeVS