

# Protection des données et dispositifs médicaux dans le domaine de la consultation en ligne sur les addictions - quo vadis ?

**Dr. iur. Barbara Widmer LL.M.,  
CIA (Certified Internal Auditor)**

# **Tout va bien, parce que...**

2

**je n'ai rien à cacher...**

**nous n'avons rien à cacher...**

# Tout va bien, mais...

3

**vous ne pensez pas que...**

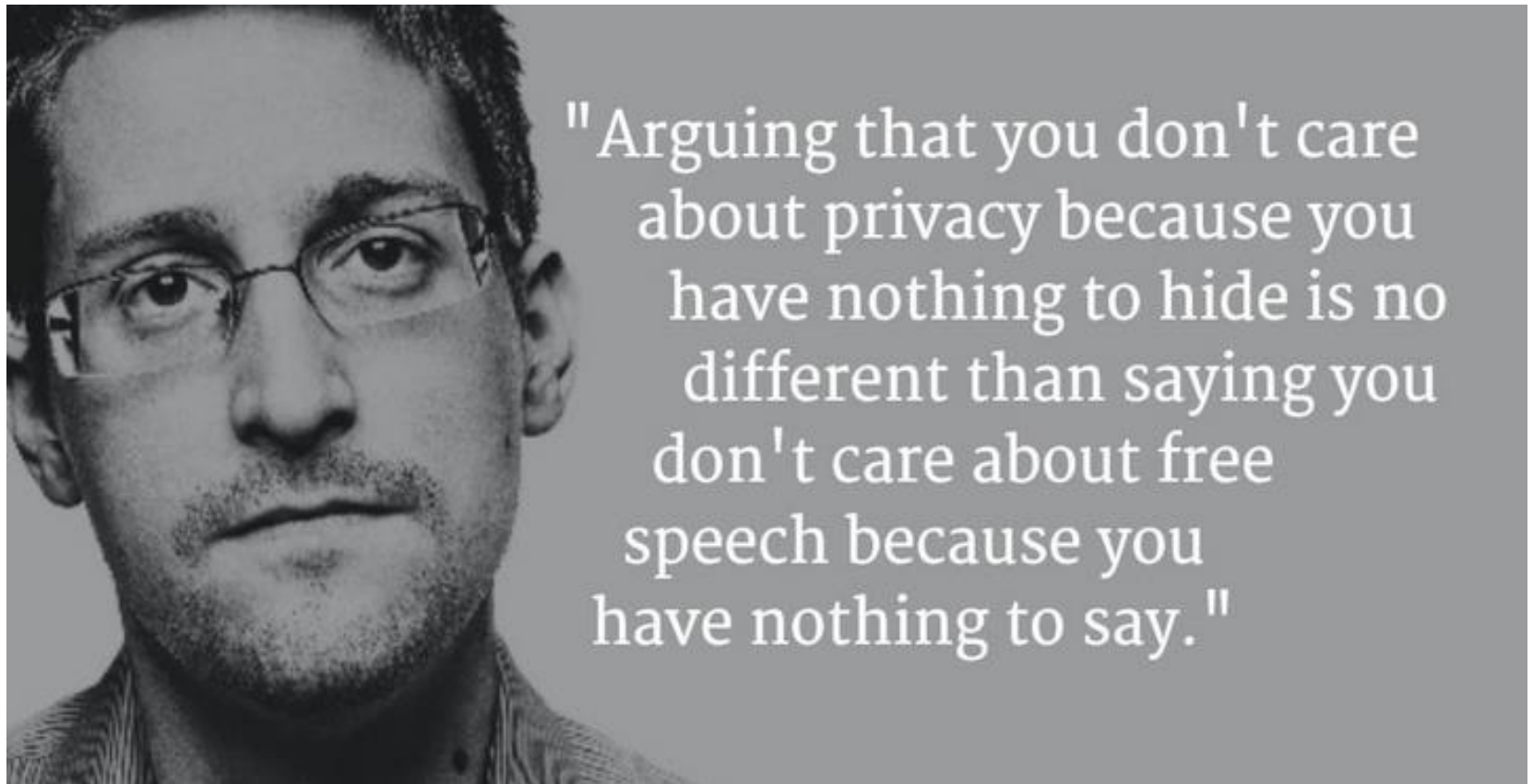
# Rien ne va, parce que...

4

## Exemple

# Rien ne va, parce que...

5



# Sommaire

6

**I. Bases**

**II. Application de la législation européenne sur la protection des données**

**III. Anonymat des données personnelles**

**IV. Applications de santé = dispositif médical ?**

**V. Résumé**

# I. Bases

# Bases

## Application de la législation sur la protection des données

8

La **législation sur la protection des données** s'applique uniquement en cas de **traitement de données personnelles**.

**Deux notions** à clarifier :

- Traitement
- Données personnelles

⇒ **Conditions identiques** en CH et dans l'UE



# Bases

## Notion de « traitement »

9

- = **toute** utilisation de données personnelles
  - **que ce soit par voie numérique ou sur papier**
- ⇒ p. ex. obtention, conservation, communication, modification, suppression

⇒ **La notion est très vaste.**

# Bases

## Notion de « données personnelles »

10

**Données personnelles** = toutes les informations qui concernent une personne (1) **identifiée** ou (2) **identifiable**

- (1) Personne **identifiée** : l'identité de la personne peut être déterminée grâce aux données ⇒ p. ex. documents d'identité, carte de membre
- (2) Personne **identifiable** : l'identité de la personne peut être déterminée grâce au contexte des données ⇒ p. ex. adresse IP, données sur l'emplacement

# Bases

## Types de données personnelles

11

### Données personnelles « normales »

= p. ex. nom, adresse, date de naissance

**Données personnelles particulières** ⇒  
particulièrement adaptées pour porter atteinte à la personnalité

⇒ p. ex. données concernant la santé, la religion, l'appartenance raciale, les mesures d'aide sociale

# Bases

## Conditions relatives au traitement des données personnelles

12

Les **conditions varient** – en fonction de l'institution qui traite les données :

- (1) organe public ou organe privé qui assume des tâches publiques

**ou**

- (2) personne physique ou morale relevant du droit privé (p. ex. entreprise, SA)

# Bases

## Conditions relatives au traitement des données personnelles

13

(1) Organe public / institution privée qui assume des tâches publiques :

⇒ Existence d'une **base légale**

Ne se trouve pas dans la loi sur la protection des données, mais dans une **loi spéciale** :

- Autorités fiscales : législation fiscale
- Registres fonciers : CC, ordonnance sur le registre foncier

# Bases

## Conditions relatives au traitement des données personnelles

14

### (2) Personne physique ou morale :

Existence de l'une des **justifications** suivantes :

- **Autorisation** de la personne concernée
- **Intérêt public** ou **privé prépondérant** de l'institution qui traite les données
- Base légale

## **II. Application de la législation européenne sur la protection des données**

# Question initiale

16

**Quand la législation européenne sur  
la protection des données  
s'applique-t-elle aux institutions  
suisses qui traitent des données ?**



# Nouvelle législation européenne sur la protection des données

17

Sujet	Règlement sur la protection des données (RGPD)	Règlement ePrivacy
Entrée en vigueur	Mai 2018	Vraisemblablement 2020
Étendue	88 pages, 99 articles	Ebauche : 40 pages, 29 articles
Contenu	Règle comment et à quelles conditions les données personnelles peuvent être traitées et comporte une liste de sanctions	Règle l'utilisation des données personnelles dans le cadre de la communication électronique, de la publicité en ligne et du suivi par Internet

# Champ d'application du RGPD

## Bases

18

### Cas normal :

Un acte législatif s'applique exclusivement **au sein d'un territoire.**

⇒ pour le territoire de l'État qui édicte l'acte.

**= *effet territorial***

# Champ d'application du RGPD

## Bases

19

### Exception :

Certains actes législatifs s'appliquent aussi **en dehors d'un territoire.**

⇒ en dehors du territoire de l'État qui édicte l'acte

**= *effet extraterritorial***

# Champ d'application du RGPD

## Bases

20

La législation européenne sur la protection des données comporte des règles qui peuvent entraîner une **application extraterritoriale**.

**Objectifs** de cette réglementation :

- **Mêmes conditions du marché** pour les entreprises au sein et en dehors de l'UE
- **Mêmes droits** pour les personnes au sein de l'UE – que l'institution qui traite les données se trouve au sein ou en dehors de l'UE

# Champ d'application du RGPD

Conditions (art. 3, par. 2, RGPD)

21

La législation européenne s'applique **en dehors du territoire de l'UE** lorsque

- des **données concernant des personnes** qui se trouvent dans l'UE sont **traitées**
- par une **institution** qui n'est pas sise dans l'UE

**POUR**

# Champ d'application du RGPD

Conditions (art. 3, par. 2, RGPD)

22

- **proposer des** <sup>(1)</sup> **marchandises** ou **des prestations** <sup>(2)</sup> à des personnes qui se trouvent dans l'UE  
**(première situation)**
- ou**
- <sup>(3)</sup> **observer** le comportement de personnes qui se trouvent dans l'UE  
**(seconde situation)**

# Première situation

23

...proposer des (1) **marchandises** ou des **services** (2) à des **personnes qui se trouvent dans l'UE**

# Première situation

## Notion de « marchandises et services »

24

### (1) Marchandises et services

**Marchandise** = tout bien meuble corporel qui a une valeur monétaire et qui peut faire l'objet d'un commerce

**Service** = notion moins claire mais qui doit se comprendre au sens **large** ⇒ couvre tous les types de **services Internet**



# Première situation

## Notion de « proposer »

25

### (2) Proposer

- ⇒ Peut avoir lieu **contre rémunération ou à titre gratuit**
- ⇒ Ne requiert **PAS** de comportement actif – **MAIS** il ne suffit pas de simplement mettre un site Internet à disposition – des éléments complémentaires sont nécessaires, p. ex.

# Première situation

## Notion de « proposer »

26

- Site Internet disponible dans la langue d'un pays membre de l'UE (ne s'applique pas aux langues officielles de la Suisse)
- Offres en EURO
- Avis de clients qui se trouvent en dehors de l'UE
- Caractère international de l'activité

# Première situation

## Conséquences

27

⇒ Le seul fait que **des personnes qui se trouvent dans l'UE** peuvent acheter des marchandises ou des services

≠

**Application** de la législation européenne sur la protection des données

⇒ Une **combinaison d'autres éléments** est toujours nécessaire

# Seconde situation

28

... **(3) observer** le comportement de personnes qui se trouvent dans l'UE

# Seconde situation

## Notion d'« observer »

29

(3) **Observer** = toute forme de **suivi et de profilage sur Internet** grâce à des outils d'analyse...

- À des fins de **traçabilité** des utilisateurs,
- À des fins de **publicité individuelle** (publicité ciblée)

# Seconde situation

## Notion d'« observer »

30

### Notions de suivi et de profilage :

**Suivi** = suivre et enregistrer les activités d'une personne sur Internet

**Profilage** = relier à un **profil de personnalité** les données sur une personne qui ont été récoltées grâce au suivi

# Seconde situation

## Notion d'« observer »

31

**Tout prestataire de site Internet** qui utilise des outils de suivi et de profilage est concerné

⇒ que le site Internet s'adresse ou non à des personnes qui se trouvent au sein de l'UE...

**Mais il existe des échappatoires :**

# Seconde situation

## Echappatoires

32

- **Ne pas** utiliser des outils de suivi et de profilage ⇒ p. ex. bouton Like de Facebook
- Le suivi et le profilage sont **anonymes**  
⇒ p. ex. utilisation de Google Analytics
- **Outil de géolocalisation** qui exclut du suivi et du profilage les utilisateurs ayant une adresse IP européenne



# Conclusions

## Application extraterritoriale

33

Pour déterminer si la législation européenne sur la protection des données **s'applique en dehors du territoire de l'UE**, il convient d'**analyser le cas en détail**.

⇒ Si la première situation ne s'applique pas, il existe des **échappatoires** relativement simples pour la seconde.

# III.

## Anonymat des données personnelles

# Question initiale

35

**Quand les données personnelles  
sont-elles anonymes et que se  
passe-t-il alors ?**

# Notion de l'anonymat

36

**Pas de définition** dans la législation sur la protection des données

⇒ Le **message** relatif à l'ébauche de la nouvelle loi sur la protection des données comporte des indications :

Les données personnelles sont **anonymes** lorsqu'une...

# Notion de l'anonymat

37

## ...identification

- par des tiers est exclue

**ou**

- n'est possible **QU'**au prix d'**efforts considérables** que nul ne serait prêt à consentir.

⇒ **Efforts considérables** en termes de temps, de finances et de ressources humaines

# Faux anonymat

38

Les données personnelles ne sont **pas véritablement anonymes** lorsque

- des **déductions** peuvent être faites sur les personnes concernées **à partir du contexte**  
**ou**
- les données personnelles ne sont que **pseudonymisées.**

# Faux anonymat

## Déductions à partir du contexte

39

Les données personnelles sont régulièrement présentes dans le **même contexte que d'autres données**

⇒ Des **déductions** peuvent être faites grâce aux **données contextuelles** et à leur lien avec **d'autres sources de données**

**Problème** : il est difficile de reconnaître les autres sources de données qui, combinées aux données originales, permettent de faire des déductions sur la personne concernée.

# Faux anonymat

## Déductions à partir du contexte

40

### La transformation numérique

- a nettement accru l'incertitude quant à l'existence d'autres sources de données  
**et**
  - facilite la création de liens avec les autres sources de données.
- ⇒ Il est devenu **beaucoup plus difficile d'anonymiser** les données personnelles.



# Faux anonymat

## Données pseudonymisées

41

Les données personnelles sont **pseudonymisées** lorsque

- l'information personnelle (p. ex. nom) est remplacée par un **indicateur** (p. ex. numéro)
- des efforts ont été délibérément menés pour rendre toute **déduction plus difficile** à faire.

# Faux anonymat

## Données pseudonymisées

42

⇒ Il existe toujours une **règle d'affectation** pour les données pseudonymisées.

### Ont accès à la règle d'affectation

- les personnes responsables de l'affectation
- des tiers qui accèdent **de façon injustifiée** à la règle d'affectation (par hasard, par malveillance)

# Faux anonymat

## Données pseudonymisées

43

- ⇒ **Toutes les personnes** qui ont accès à la règle d'affectation peuvent consulter des **données personnelles**.
- ⇒ La qualité de **protection de la règle d'affectation** contre les accès injustifiés est déterminante pour la qualité de la pseudonymisation.
- ⇒ En tous les cas, les données pseudonymisées ne sont **JAMAIS** des données anonymes.

# Vrai anonymat

44

**Données anonymes ≠ données personnelles**

⇒ La législation sur la protection des données  
**ne s'applique plus!**

L'anonymisation doit toujours faire l'objet d'**un examen minutieux** – toute **erreur** peut avoir des **conséquences considérables** !

# IV. Applications de santé = dispositif médical ?

# Question initiale

46

**Les applications de santé peuvent-elles être un dispositif médical ?**

# Situation actuelle

47

**Plusieurs incidents et scandales** impliquant des dispositifs médicaux ont entraîné

- ⇒ **des doutes concernant le système de contrôle européen** pour les dispositifs médicaux
- ⇒ **l'élaboration d'une nouvelle législation européenne sur les dispositifs médicaux**

# Nouvelle législation européenne sur les dispositifs médicaux

## Aperçu

48

Sujet	Règlement relatif aux dispositifs médicaux (RDM)	Règlement relatif aux dispositifs médicaux de diagnostic in vitro
Entrée en vigueur	Mai 2017	Mai 2017
Prise de validité	Échelonnée jusqu'en mai 2020	Échelonnée jusqu'en mai 2022
Étendue	92 pages, 123 articles, plus 17 annexes	82 pages, 113 articles, plus 15 annexes
Contenu	Règle la mise en circulation, la mise sur le marché et l'exploitation au sein de l'UE de <b>dispositifs médicaux</b> destinés à un usage humain ainsi que de leurs accessoires	Règle la mise en circulation, la mise sur le marché et l'exploitation au sein de l'UE de <b>dispositifs médicaux de diagnostic in vitro</b> destinés à un usage humain ainsi que de leurs accessoires



# Nouvelle législation suisse sur les dispositifs médicaux

## Aperçu

49

Le caractère **international** du marché des dispositifs médicaux est **très prononcé**.

- ⇒ **Commerce international** de dispositifs médicaux
- ⇒ Si la Suisse souhaite rester compatible avec le **marché européen intérieur des dispositifs médicaux**, elle doit largement reprendre la législation européenne à ce sujet.

# Nouvelle législation suisse sur les dispositifs médicaux

## Aperçu

50

La révision du droit suisse sur les dispositifs médicaux est en cours :

- ⇒ **Les modifications** sont **échelonnées** à l'instar de celles au niveau européen.
- ⇒ **L'entrée en vigueur** est prévue pour 2020 ou 2022 – à l'instar de la législation européenne

# Notions

## Dispositif médical

51

**Définition complexe** – pour simplifier :

**Objet, matière ou logiciel** qui

- est utilisé *à des fins thérapeutiques ou diagnostiques* sur des êtres humains,
- dont les *principaux effets conformes à l'usage prévu* sont de nature physique ou psychosomatique.

(psychosomatique = relevant de la chimie physique)

# Notions

## Diagnostic in vitro en tant que dispositif médical

52

### Type particulier de dispositif médical

⇒ sert aux **analyses de laboratoire**  
d'échantillons prélevés sur des corps humains  
(p. ex. sang, sécrétion ou tissu)

**Exemples** : tests rapides, matériel pour frottis,  
appareils d'analyse

# Notions

## Logiciels en tant que dispositifs médicaux

53

Logiciel	Exemple	Description
<b>Logiciels autonomes</b>  = PAS intégrés à un produit	Applications de santé	Si le logiciel poursuit un <u>but spécifiquement médical</u> , il s'agit d'un dispositif médical.  <b>MAIS</b> : si le logiciel poursuit des buts généraux ou des buts relatifs au mode de vie ou au bien-être tout en pouvant être utilisé dans le domaine de la santé, ce n'est pas un dispositif médical.
<b>Logiciels faisant partie d'un produit</b>  = logiciels qui commandent un produit ou influencent son utilisation	Tensiomètre numérique	Si le produit peut être qualifié de dispositif médical, le logiciel est considéré comme étant une partie d'un dispositif médical et traité de la sorte. Le fait que le logiciel soit intégré au dispositif médical ou non (p. ex. stocké dans un cloud) n'a aucune importance.

# Classification en général

## Situation initiale

54

**Catégories de risque : 4 différentes – I, IIa, IIb, III**

**Base risque : corps humain**

**Facteurs de risque : durée et lieu de l'utilisation du dispositif médical (durée = temps d'utilisation, lieu = profondeur dans le corps)**

**Certification : en général nécessaire ⇒ plus le risque est élevé, plus les exigences en matière de certification le sont.**

# Classification en général

## Vue d'ensemble

55

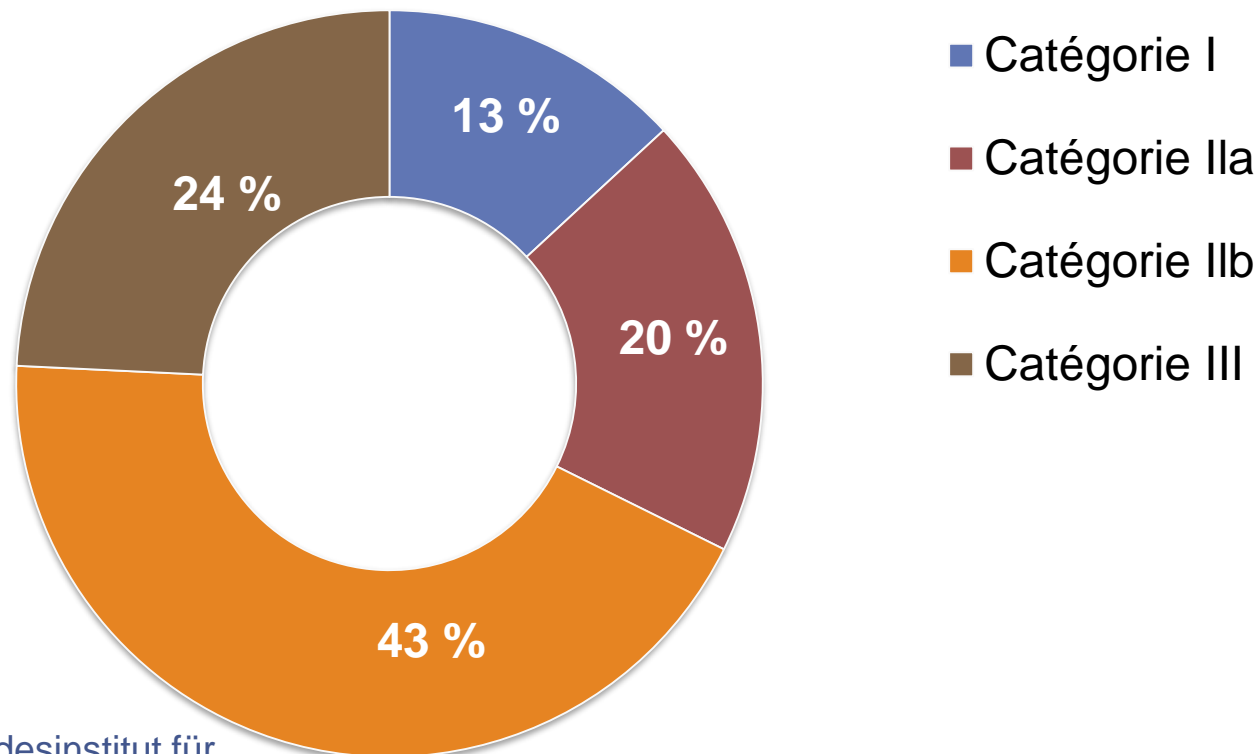
Catégorie	Potentiel de risque	Exemples	Certification nécessaire
<b>I</b>	faible	pansements, colliers cervicaux, chaises roulantes, cannes	en général non
<b>IIa</b>	moyen	appareils à ultrasons, canules, appareils auditifs externes	oui
<b>IIb</b>	élevé	lasers chirurgicaux, appareils de radiographie, endoprothèses, défibrillateurs	oui
<b>III</b>	très élevé	valves cardiaques, prothèses articulaires, implants mammaires, stimulateurs cardiaques	oui

# Classification en général

## Parts des catégories de dispositifs médicaux

56

### Parts des catégories de dispositifs médicaux en Allemagne en 2015



**Source :** Deutsches Bundesinstitut für  
Arzneimittel und Medizinprodukte

Rencontre de SafeZone.ch du 31.1.2019



# Classification des logiciels

57

**Base légale : règle 11, annexe VIII, RDM :**

- ⇒ À l'avenir, la plupart des **logiciels** relèveront vraisemblablement de la **catégorie IIa** – voire de la catégorie IIb ou III dans certains cas.
- ⇒ **Conséquence** : exigences **plus élevées** en matière de certification et moins de **logiciels** de la **catégorie I**

**MAIS** : la règle 11 est **contestée** dans les milieux spécialisés !

# Développement d'applications de santé

58

En cas de développement **d'applications de santé**, il convient de prendre contact suffisamment tôt avec les **autorités de certification** pour clarifier les points suivants :

1. Distinction entre ce qui relève d'un dispositif médical et ce qui ne relève pas d'un tel dispositif – **si dispositif médical** :
2. Diffusion géographique
3. Classification
4. Exigences en matière de certification
5. Étapes ultérieures

# Résumé

59

- ⇒ **La législation européenne sur la protection des données** peut s'appliquer aux institutions en Suisse qui traitent des données concernant des personnes dans l'UE – il existe toutefois des **échappatoires** dans certaines situations.
- ⇒ Souvent, les données sont **faussement anonymisées**. La **transformation numérique a compliqué** l'anonymisation sûre. Un **examen minutieux** est toujours nécessaire.

# Résumé

60

- ⇒ **Le droit relatif aux dispositifs médicaux est exigeant.** La Suisse va largement reprendre la nouvelle législation européenne.
- ⇒ Les **logiciels** peuvent être des dispositifs médicaux dans certaines circonstances. En raison de la **nouvelle règle de classification**, ils devraient être affectés aux catégories supérieures → **conséquence** : exigences plus élevées en matière de certification.

**Merci de votre attention**

**Des questions ?**