3+6 IDÉES & 0 TRACASSERIE

pour mettre une clinique en conformité

LIVRE BLANC

SOMMAIRE

DE QUOI EST-CE QU'IL S'AGIT ?

LES DONNÉES À CARACTÈRE PERSONNEL, c'est toute information de quelque nature que ce soit et indépendamment de son support, y compris le son et l'image, relative à une personne physique identifiée ou identifiable.

Aux termes du Code, deux grandes catégories de données à caractère personnel peuvent ainsi être distinguées : les données à caractère personnel ordinaires et les données à caractère personnel soumis à un régime particulier dont les données concernant la santé.

Les données concernant la santé sont définies comme toute information concernant l'état physique et mental d'une personne concernée, y compris les données génétiques et la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne.

Cette courte définition et brève d'apparence appelle pourtant à une conception élargie des données concernant la santé.

Si la **séropositivité**, la **présence de plasmodium**, des **troubles de vision**, des **troubles de démence** renvoient à l'état physique et mental d'une personne et que la **biométrie**, la **sérologie**, le **groupe sanguin**, renvoient aux données génétiques qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne physique en question, la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne est également perçue comme une donnée concernant la santé.

A titre illustratif, la Commission Européenne a considéré que la simple information qu'une personne se soit blessée au pied et qu'elle est en congé maladie constitue une donnée de santé tandis que la Commission Nationale Informatique et Libertés française a considéré que les données sur les addictions et la dépendance sont des données de santé. Autre exemple, le simple fait qu'une personne soit en arrêt maladie, sans en connaître la raison, constitue une donnée de santé.

C’est dire que la notion de données concernant la santé ne couvre plus la seule hypothèse d’une information en lien direct avec une pathologie, mais plus largement avec tout l’environnement lié à la prestation de santé.

Concrètement, les données concernant la santé font référence aux :

Informations relatives à une personne physique collectées lors de son inscription en vue de bénéficier de services de soins de santé ou lors de la prestation de ces services : un numéro, un symbole ou un élément spécifique attribué à une personne physique pour l’identifier de manière unique à des fins de santé ;

Informations obtenues lors du test ou de l’examen d’une partie du corps ou d’une substance corporelle, y compris à partir des données génétiques et d’échantillons biologiques ;

Informations concernant une maladie, un handicap, un risque de maladie, les antécédents médicaux, un traitement clinique ou l’état physiologique ou biomédical de la personne concernée (indépendamment de sa source, qu’elle provienne par exemple d’un médecin ou d’un autre professionnel de santé, d’un hôpital, d’un dispositif médical ou d’un test de diagnostic in vitro).

Les renseignements peuvent ainsi concerner la santé présente, passée ou future d'une personne et tout élément informant sur l'état de santé d'une personne. Il peut en effet s'agir, non seulement, des informations relatives à une éventuelle maladie ou pathologie mais aussi celles obtenues lors d'un test ou examen d'une partie du corps.

Ainsi, les objets connectés et autres dispositifs technologiques qui collectent, par exemple, des données brutes relèvent désormais du régime des données de santé.

En revanche, n'entrent pas dans la notion de données concernant la santé celles à partir desquelles aucune conséquence ne peut être tirée au regard de l'état de santé de la personne concernée.

EXEMPLE :

une application collectant un nombre de pas au cours d'une promenade sans croisement de ces données avec d'autres.

ET LA CONFORMITÉ DONC ?

Les données à caractère personnel concernées par la conformité dans le domaine de la santé sont celles qualifiées par le Code du numérique comme des données sensibles.

Il est en principe interdit de traiter les données sensibles. Ce n'est que par le contournement de la profession que le corps médical pourra en traiter.

Logiquement, la sensibilité de ces données fait accroître les obligations qui pèsent sur les professionnels de la santé. D'abord, les professionnels de la santé doivent respecter les principes cardinaux de traitement des données à caractère personnel. Ensuite, ils doivent se soumettre aux régimes de traitements indiqués par la loi et enfin, ils doivent démontrer leur **«accountability»**, sens de responsabilité tel qu'exigé par l'**article 387 de la loi 2020-35 portant Code du numérique révisé en République du Bénin**, à travers la mise en place d'un cadre de traitement conforme aux exigences de la loi.

Mieux que les responsables qui traitent des données courantes, les responsables de traitement des données de santé, les promoteurs ou responsables de centres de santé privés doivent donc protéger, la confidentialité, l'intégrité et la disponibilité des données qu'ils recueillent.

Toutefois, même si ces professionnels ont reçu une doctrine déontologique qu'ils essaient de mettre en pratique, les exigences du Code du numérique semblent lourd à porter pour eux et ils ont parfois du mal à s'y faire. Pourtant, la conformité est une opportunité d'amélioration continue plutôt qu'une contrainte. Elle peut être abordée de manière proactive et pragmatique.

En adoptant les idées que nous partageons ici et en les adaptant aux besoins spécifiques de votre clinique, vous pouvez garantir des soins de qualité et la sécurité des données tout en évitant les tracas inutiles.

LES 3 PILIERS DE LA FONDATION :

1. METTRE SOUS CONFIDENTIALITÉ RENFORCÉE TOUS LES INTERVENANTS DANS LE CENTRE :

si les médecins prêtent serment, ce n'est pas le cas des aides-soignants(e)s, des infirmier(e)s, des garde-malades etc. Or tous représentent des sources de risques potentiels. En leur faisant prendre des engagements de confidentialité, éventuellement assortis de clauses pénales, le responsable de traitement pose un premier grand pas vers sa conformité au Code du numérique.

2. SENSIBILISER, ÉDUQUER, FORMER TOUT LE MONDE :

lorsqu'il s'agit de la protection des données et de la vie privée, le maillon faible est le maillon de plus dangereux. De la personne chargée de nettoyer les bureaux, les salles d'hospitalisation, il faut amener tout le monde à développer une conscience aigue des enjeux liés à la protection des données.

De plus, tout ce qui est mis en place à l'interne pour assurer la sécurité des données doit être connu et maîtrisé de tous. C'est cohérent et une question d'efficacité. Un outil comme Codnumlab vous permet de satisfaire à cette exigence sans vous prendre des journées entières de travail.

3. INSONORISER LES SALLES DE CONSULTATIONS ET D'OPÉRATIONS ET TOUTES LES PIÈCES CLÉS :

une fuite de donnée banale et récurrente, c'est le mur qui a des oreilles. La discussion entre le médecin et son patient doit rester entre eux. Sauf cas spécifiques rares, même l'époux n'est pas censé savoir ce qui s'est dit entre son épouse et son médecin. A plus forte raison, l'amie.

LES 6 POTEAUX DE L'ÉDIFICE

4.

ELOIGNER LE HALL D'ATTENTES

Une technique de base pour garder confidentielle la donnée personnelle des personnes est d'appliquer la distanciation. Dans une file d'attente, la personne suivante ne doit pas être en mesure de savoir les détails de l'opération de la personne avant. Un hall d'attente espacé et suffisamment éloignée des secteurs opérationnels permet ainsi de limiter les risques de fuites de l'information. C'est définitivement un précepte à mettre en place si l'on a à cœur la sécurité des données de ses patients.

5.

PSEUDONYMISER LES DONNÉES DES CLIENTS :

Un code, une lettre ou un chiffre sont tous préférable aux nom et prénoms des personnes qu'on scande pour leur annoncer leurs tours ou leur remettre un document dans un espace partagé. La pseudonymisation des données de vos patients vous garantis d'être les seuls à pouvoir savoir à qui correspond telle ou telle autre donnée.

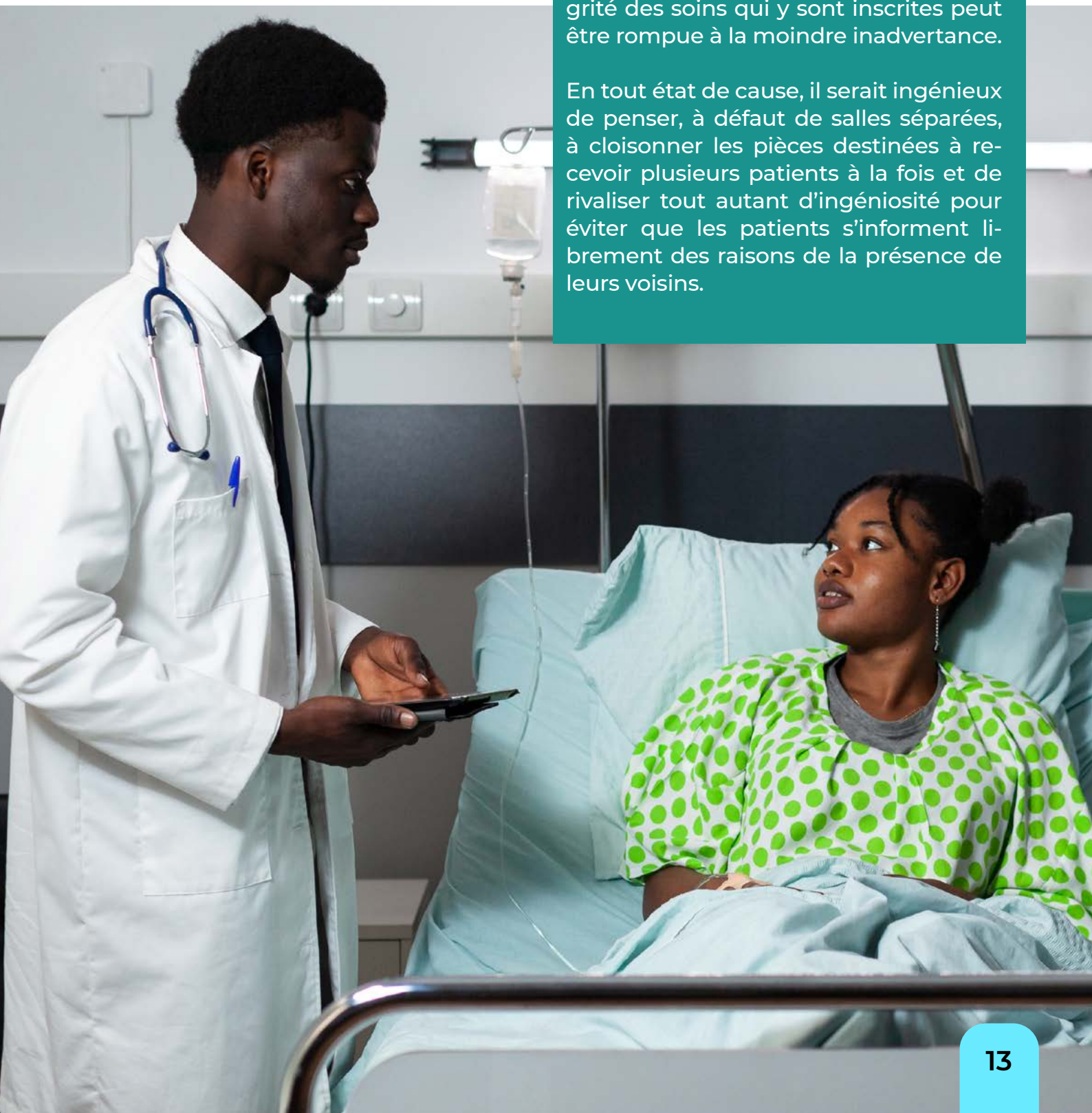
Elle vous permet de vous assurer que seules les personnes autorisées ont connaissance des données qui vous sont confiées. Allez-y à l'envie et n'hésitez pas à faire preuve de créativité et de générosité dans l'effort de pseudonymisation des données de vos patients. «**Loulou**» pourrait ravir un sourire à «**M. Donné**» et rendre plus agréable son expérience « patient».

6. CLOISONNER LA SALLE D'HOSPITALISATION :

Une chose courante dans vos établissements de santé est la communautarisation dans les salles d'hospitalisation. Comme si le fait d'être admis en soin créé d'office un lien de familiarité entre toutes les personnes qui y sont présentes.

Les personnes alitées sont alignées côte à côte et chacun connait ce dont souffre son compagnon d'infortune. C'est une pratique violatrice des données à caractère personnel mais également de la vie privée. Mieux, elle peut s'avérer attentatoire. Si tout le monde avait accès à la fiche de soin de tous les patients, l'intégrité des soins qui y sont inscrites peut être rompue à la moindre inadvertance.

En tout état de cause, il serait ingénieux de penser, à défaut de salles séparées, à cloisonner les pièces destinées à recevoir plusieurs patients à la fois et de rivaliser tout autant d'ingéniosité pour éviter que les patients s'informent librement des raisons de la présence de leurs voisins.



7.

INFORMER LES PATIENTS :

Un responsable de traitement responsable est celui qui met tout en œuvre pour que les personnes concernées par ses traitements soient suffisamment informées de ces derniers. Les patients ont un droit fondamental à la protection de leur vie privée et de leurs données personnelles.

Ils doivent être informés sur la manière dont leurs données seront collectées, utilisées, stockées et partagées et comprendre comment leurs données seront utilisées dans le cadre de leur traitement médical. C'est seulement en comprenant cela qu'ils peuvent donner un consentement éclairé chaque fois que c'est nécessaire.

Les sachant informés, vous êtes aussi plus enclin à faire attention à ce que leurs données soient traitées de la meilleure manière et dans les meilleures conditions. L'information préalable permet aux patients de signaler tout comportement abusif ou inapproprié concernant leurs données, ce qui contribue à prévenir les violations de la vie privée. Affiches permanentes dans la salle d'accueil, le bureau du médecin, formulaires, informations orales, centres d'écoutes, aucun effort n'est négligeable pour s'assurer que les patients sont bien informés.

8. CHOISIR LES BONS PARTENAIRES

Ambulanciers privés, laboratoires d'analyses, équipementiers, les personnes qui agissent pour votre compte sur les données d vos patients doivent démontrer leur conformité au Code du numérique. Tout comme vous. Sauf que, c'est pour vous, une obligation légale de veiller à ce qu'il le soit. Au-delà, le choix d'un sous-traitant st une question d'efficacité et peut-être d'économie. Un sous-traitant qualifié doit posséder l'expertise technique nécessaire pour gérer les données de santé de manière appropriée.

Cela inclut la mise en œuvre de mesures de sécurité, la gestion des risques et la prévention des incidents de sécurité. En choisissant un sous-traitant compétent, vous réduisez les risques potentiels liés à la sécurité des données et aux violations de la confidentialité. Un sous-traitant expérimenté est mieux équipé pour anticiper et gérer les problèmes potentiels. Les exigences de conformité sont transférées au sous-traitant tandis que vos seules diligences restantes sont celles de vous assurer de leur conformité et d'auditer cette conformité de temps à autre.

9. DÉSIGNER UN DÉLÉGUÉ À LA PROTECTION DES DONNÉES

La désignation du délégué est un acte de conformité obligatoire pour les personnes traitant des données concernant la santé. Cette désignation va témoigner de la volonté du responsable de traitement d'opérer ses traitements dans le respect des prescriptions légales.

En se dotant d'un délégué à la protection des données à caractère personnel ou **DPO**, le responsable du traitement, s' « équipe » d'un « œil » du Code et de l'Autorité dans son organisme. C'est une présomption suffisante de son engagement à être responsable.

Vous pouvez avoir un délégué interne ou externaliser ce service. La mission principale d'un **DPO** est de faire en sorte que l'organisme qui l'a désigné soit en conformité avec le cadre légal relatif aux données personnelles.

VOTRE MANTRA

Premièrement, ne pas nuire !

Aux informations identifiantes directement ou indirectement un patient, **ne pas nuire !**
En salle d'attente ou de consultation, au laboratoire ou au bloc opératoire, **ne pas nuire !**
Soi-même, ses collaborateurs ou ses prestataires, **ne pas nuire !**
Comprenant que la nuisance n'emporte pas nécessairement perte de vie ou de capacité, **ne pas nuire !**
Comprenant que toute personne a droit au respect de son intégrité et de sa vie privée, **ne pas nuire !**
Comprenant que le traitement des données à caractère personnel peut conduire à la nuisance, **ne pas nuire !**

360 CONSEILS

LE CABINET

Nous sommes **360 Conseils S.A.S**, des ingénieurs juridiques des affaires et du numérique. Nous accompagnons les organisations à s'adapter et à se réinventer face aux enjeux juridiques, économiques, sociétaux, réglementaires et technologiques en République du Bénin.

NOS EXPERIENCES

Conseils s'appuie sur une expertise acquise depuis la première législation sur la question de protection des données à caractère personnel au travers de plus d'une cinquantaine de missions de conformité dans divers secteurs d'activités et de plusieurs publications.

NOS MARQUEURS

NOS RÉFÉRENCES

APDP

IFDC
Developing Agriculture from the Ground Up

SÈMÈ CITY

TechnoServe
L'Entreprise, Solution à la Pauvreté

Enabel

VITAL FINANCE

GO AFRICA online

ORDRE DES AVOCATS DU BENIN

SLI AFRIKA

NOS PUBLICATIONS

Envie d'approfondir ces points ou des questions restées en suspens,

360 Conseils SAS

vous accompagne sur votre chantier de mise et de maintien en conformité.

360conseils www.360conseils.com

+229 67 96 72 72 infos@360conseils.com