DÉMARCHE SFSO QUALITÉ
Spécialistes en orthodontie

Données personnelles
Déploiement du RGPD dans les cabinets

V1 – Juin 2018

Ce guide ne prétend bien entendu pas à l'exhaustivité sur l'ensemble des thématiques associées au RGPD, qui sont très étendues. Il se veut une aide à la compréhension des thèmes principaux et au passage à l'acte dans les cabinets. Il évoluera avec la réglementation, les interprétations qui en seront données dans le temps et le retours constatés sur le terrain

Le RGPD ?

- Le Règlement Général sur la Protection des Données (RGPD - *Règlement UE 2016/679 du Parlement européen et du Conseil du 27 avril 2016*) entré en vigueur le 25/05/18 harmonise et encadre le traitement des données personnelles sur tout le territoire de l'Union européenne.
- Il s'inscrit dans la continuité de la Loi française « Informatique et Libertés » de 1978 et renforce les principes de **protection du citoyen et les obligations des entreprises traitant des données personnelles**. Il s'impose à toutes les entreprises établies en UE ou proposant des produits et services au résidents européens

- Pour l'entreprise, le principe de conformité préalable jusqu'ici en vigueur dans le cadre de déclarations simplifiées CNIL est remplacé, entre autres, par :
  - une obligation de conformité documentée en continue dans l'entreprise (les formalités préalables actuelles, comme les déclarations simplifiées, sont amenées à disparaître)
  - une garantie d'information des particuliers
  - une responsabilité élargie des professionnels et sous-traitants

Définitions

Données personnelles. Toute information se rapportant à une personne physique identifiée ou identifiable directement (nom, prénom…) ou indirectement (par un identifiant, une donnée biométrique, des éléments propres à son physique, numéro de sécurité sociale,…)

Données personnelles « sensibles » : origine raciale ou ethnique, opinions politiques ou religieuses, appartenance syndicale, **concernant la santé** ou l'orientation sexuelle, génétiques ou biométriques → Le Cabinet est donc concerné par la nature des données santé, « à risque », qu'il manipule quotidiennement dans le cadre de ses activités.

Traitement de données personnelles. Ce sont les opérations réalisées portant sur des données personnelles, quel que soit le procédé utilisé (collecte, enregistrement, consultation, modification, communication par tout moyens…). Le scanne des cartes mutuelles est un exemple de traitement de données personnelles par collecte.

Rappelons qu'un traitement de données personnelle n'est pas nécessairement informatisé : **les fichiers papiers sont également concernés !**

RGPD : une opportunité plus qu'un « risque » pour les cabinets

- L'émission du RGPD européen après des années de débat porte une ambition très importante : **contribuer à la protection des citoyens dans une économie digitale mondialisée**. **Son objectif est clairement tourné vers les acteurs clés du digital et des données,** les acteurs technologiques mobilisant des données à grande échelle et porteurs de risques.

- La CNIL est rassurante : ses contrôles (dont le cadre reste à fixer) prioriseront les **acteurs à risque, dont le cœur d'activité tourne autour du traitement de données, et dans une logique d'accompagnement plus que de sanction**

- Pour le cabinet, le RGPD ne doit donc pas être vu sous l'angle de la contrainte et de la sanction, mais comme **une opportunité d'évaluer et reprendre en main ses pratiques de sécurité informatique et de renforcer la gestion globale des risques de l'entreprise**

« Si les données personnelles ne sont pas au cœur de votre activité, les moyens à déployer pour vous mettre en conformité au RGPD ne seront pas très importants ! (…) Ce règlement dans votre entreprise n'est donc pas obligatoirement un projet technique ou juridique, il s'agit avant tout de bon sens et d'organisation. »

CNIL – BPI – Guide pratique de sensibilisation au RGPD pour les PME.

RGPD : Faire son « audit » des pratiques internes en matière de protection des accès et des données

Faire son audit apparait indispensable au regard des obligations de moyens qui pèsent sur la structure.

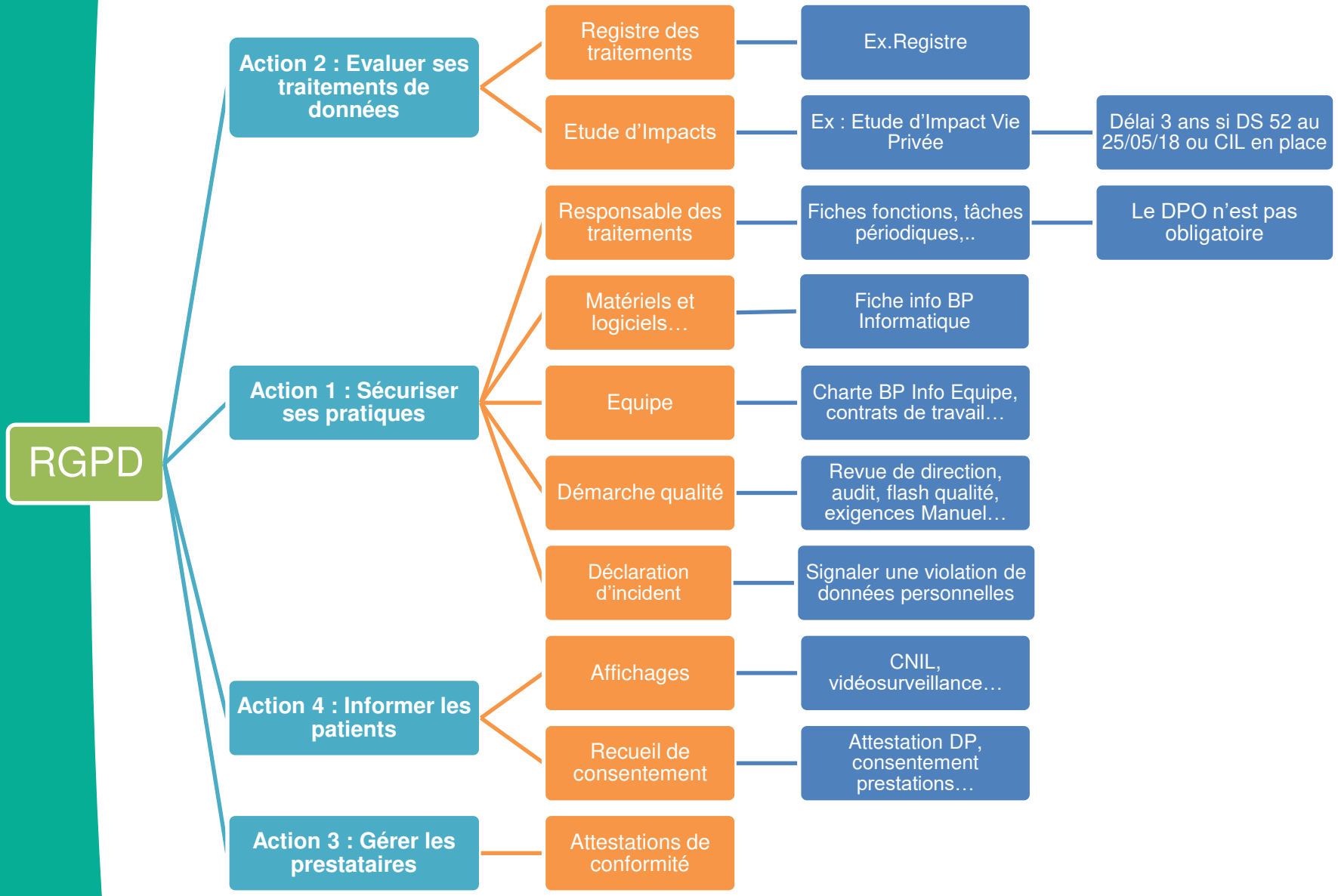
Exemple de grille « d'audit »

ÉVALUER LE NIVEAU DE SÉCURITÉ DES DONNÉES PERSONNELLES DE VOTRE ORGANISME

Avez-vous pensé à ?

	FICHES	MESURE	
1	Sensibiliser les utilisateurs	Informez et sensibilisez les personnes manipulant les données	☐
		Rédigez une charte informatique et donnez lui une force contraignante	☐
2	Authentifier les utilisateurs	Définissez un identifiant (login) unique à chaque utilisateur	☐
		Adoptez une politique de mot de passe utilisateur conforme à nos recommandations	☐
		Obligez l'utilisateur à changer son mot de passe après réinitialisation	☐
		Limitez le nombre de tentatives d'accès à un compte	☐
3	Gérer les habilitations	Définissez des profils d'habilitation	☐
		Supprimez les permissions d'accès obsolètes	☐
		Réalisez une revue annuelle des habilitations	☐
4	Tracer les accès et gérer les incidents	Prévoyez un système de journalisation	☐
		Informez les utilisateurs de la mise en place du système de journalisation	☐
		Protégez les équipements de journalisation et les informations journalisées	☐
		Prévoyez les procédures pour les notifications de violation de données à caractère personnel	☐
5	Sécuriser les postes de travail	Prévoyez une procédure de verrouillage automatique de session	☐
		Utilisez des antivirus régulièrement mis à jour	☐
		Installez un « pare-feu » (firewall) logiciel	☐
		Recueillez l'accord de l'utilisateur avant toute intervention sur son poste	☐
6	Sécuriser l'informatique mobile	Prévoyez des moyens de chiffrement des équipements mobiles	☐
		Faites des sauvegardes ou des synchronisations régulières des données	☐
		Exigez un secret pour le déverrouillage des smartphones	☐
7	Protéger le réseau informatique interne	Limitez les flux réseau au strict nécessaire	☐
		Sécurisez les accès distants des appareils informatiques nomades par VPN	☐
		Mettez en œuvre le protocole WPA2 ou WPA2-PSK pour les réseaux Wi-Fi	☐
8	Sécuriser les serveurs	Limitez l'accès aux outils et interfaces d'administration aux seules personnes habilitées	☐
		Installez sans délai les mises à jour critiques	☐
		Assurez une disponibilité des données	☐

Tour d'horizon du RGPD au Cabinet…



Thèmes à prendre en compte dans les cabinets

Pourquoi le cabinet est-il concerné par le RGPD et les données personnelles ?

Mobilisation de données sensibles des patients

Risques de défaillance technique ou de malveillance informatique

Partenaires SSII centralisateurs et exploitants de données sensibles « à grande échelle »

Les datas, outils indispensables de l'évolution des cabinets, de ses missions, de l'interprofessionnalité,…

1.
Sécuriser ses pratiques

Désigner un pilote

Un pilote sur la gestion des données personnelles, qui sera identifié en tant que « **Responsable de traitement** », et sera souvent par défaut le praticien. Il s'assurera périodiquement des bonnes pratiques mises en place au cabinet concernant les données personnelles.

A noter : la nomination d'un DPO au cabinet (délégué à la protection des données) est une possibilité **mais n'est pas obligatoire** : le cabinet ne gère pas de données sensibles « à grande échelle ». Le cas échéant, la fonction de DPO peut être mutualisé entre différentes structures.

Sensibiliser votre équipe

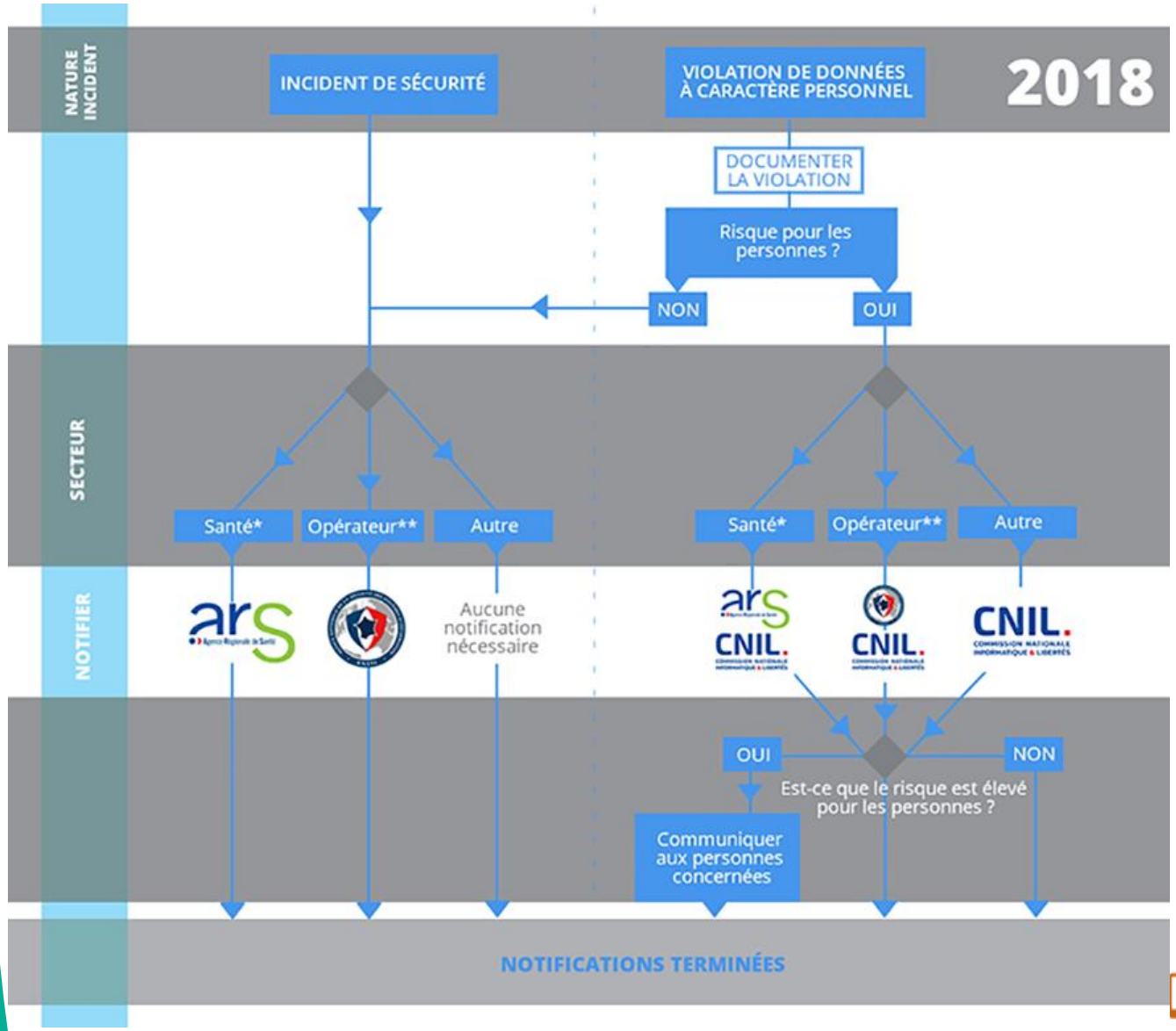
Le respect des bons réflexes au quotidien dépendent largement de l'équipe et il est impératif de la **sensibiliser à l'importance des données manipulées chaque jour**, à leur confidentialité et plus généralement, aux bonnes pratiques informatiques à avoir en tête. Enfin, les salariés du cabinet doivent être informés de la gestion directe de données personnelles les concernant aux fins de gestion administrative interne.

A noter : cette sensibilisation peut se concrétiser par une charte de bonnes pratiques informatiques au sein du cabinet et à destination de l'équipe, une clause dans le contrat de travail ou la fiche de fonction…

Evaluez votre sécurité informatique

- Assurez-vous que seules les données strictement nécessaires à la poursuite de vos objectifs sont collectées et traitées.
- Identifiez la base juridique sur laquelle se fonde votre traitement (par exemple : consentement de la personne, intérêt légitime, contrat, obligation légale).
- Révisez vos mentions d'information afin qu'elles soient conformes aux exigences du règlement.
- Vérifiez que vos sous-traitants connaissent leurs nouvelles obligations et leurs responsabilités, assurez-vous de l'existence de clauses contractuelles rappelant les obligations du sous-traitant en matière de sécurité, de confidentialité et de protection des données personnelles traitées.
- Prévoyez les modalités d'exercice des droits des personnes concernées (droit d'accès, de rectification, droit à la portabilité, retrait du consentement...).
- Vérifiez les mesures de sécurité mises en place.

Savoir gérer les incidents



** Établissements de santé, hôpitaux des armées, laboratoires de biologie médicale et centres de radiothérapie*

*** Opérateur d'importance vitale (OIV), opérateur de service essentiel (OSE) ou opérateur de service numérique (OSN) mettant à disposition des places de marché et les moteurs de recherche en ligne et des services d'informatique en nuage, service de confiance (SDC), ou opérateurs Télécom*

2.
Evaluer ses traitements de données personnelles

1. Le registre de traitement des données : identifiez vos traitements de données personnelles

Voir outils - exemple :
Registre des traitement et Risques

- La première démarche à accomplir est de **lister les principales activités** du cabinet mobilisant des données personnelles, en précisant quelques points clés de bon sens : quelle est la finalité de ce traitement ? (ex – dossier patient du logiciel : sécuriser les actes…) quelles sont les données collectées ? qui y a accès ? quelle est la durée de conservation prévue ?...

RGPD

Registre des traitements de données personnelles

TRAITEMENTS de données personnelles	Finalité du traitement	Données concernées	Responsable du traitement	Accès Qui?	Durée de conservation	Transfert éventuel
Dossier patient	Assurer la traçabilité et sécurité des actes	Etat-civil patient, prescripteurs, actes, traçabilité des DM	Praticien	Tous	10 ans	

2. L'Etude d'Impacts sur la Vie Privée (EIVP) : évaluez les risques associés à vos traitements de données personnelles

Voir outils - exemple :
Registre des traitement et Risques

- La sécurisation des données personnelles mobilisées par l'entreprise est un objectif central du RGPD. Il est donc logique, après avoir recensé ses données, de procéder à **l'évaluation des risques liés à la dégradation des données personnelles mobilisées par le cabinet** : consultation non désirée des données, vol et disparition…les impacts ne sont pas les mêmes pour les particuliers concernés, et votre exposition au risque non plus !
- A vous d'identifier les risques possibles et surtout, d'éventuelles actions d'amélioration à mettre en place !

RGPD

Etude d'Impacts : gestion des risques

TRAITEMENTS de données personnelles	Natures du risques potentiels (accès illégitime, disparition des données…)	Risques			Précautions existantes	Exemple : Actions à mettre en œuvre (juridique, organisation, technique, physique…)
		Faibles	Moyens	Forts		
Gestion des salariés du cabinet (et ex salariés)	Exemple de risques : Accès illégitime Modification non désirée Disparition des données Divulgation Information patients Autres	X			Accès protégées des données scannées	Mettre sous clés les données personnelles salariés Destructeur de documents Code d'accès aux postes informatiques et boites mails

L'informatique, un des thèmes de votre démarche qualité !

Les « systèmes informatiques » sont traités dans votre Manuel qualité et font déjà l'objet de plusieurs exigences. Elles évolueront dans les prochaines versions du Manuel pour intégrer des points complémentaires (ex : disponibilité d'une messagerie sécurisée…).

3.
Gérer ses prestataires

Conservez toutes les attestations de conformité RGPD reçues des prestataires concernés

- De nombreuses données personnelles mobilisées au cabinet sont susceptibles de transfert vers des prestataires, destinataires externes variés – exemples :
  - Sauvegardes externes automatisées vers la SSII
  - Données transitant vers un autre professionnel de santé ou un prothésiste sous-traitant

- Le RGPD prévoit une responsabilité élargie des sous-traitants de données personnelles : l'intégralité des exigences du RGPD leur sont opposables et ceux-ci doivent être en capacité de le démontrer.

- Pour le cabinet, l'essentiel consiste donc à s'assurer que le **contrat avec son sous-traitant intègre une clause ou un avenant spécifique sur la gestion des données personnelles**. Il convient donc de conserver dans vos dossiers fournisseurs tout support apparenté à une « attestation de conformité au RGPD» reçu de ces derniers.

- *SSII du Logiciel de gestion*
- *Concentrateur de données*
- *Sous-traitants*
- *Hébergeur*
- *Webmaster*
- *…*

4.
Informer les patients

Consentement éclairé

Vous avez l'obligation de démontrer que la personne a bien donné son consentement pour l'utilisation que vous faîtes de ses données personnelles. Cela revient à associer à chaque personne enregistrée dans vos bases de données le contenu de son consentement à l'utilisation de ses données personnelles.

Selon les documents de la CNIL, « La preuve du consentement nécessite trois éléments :

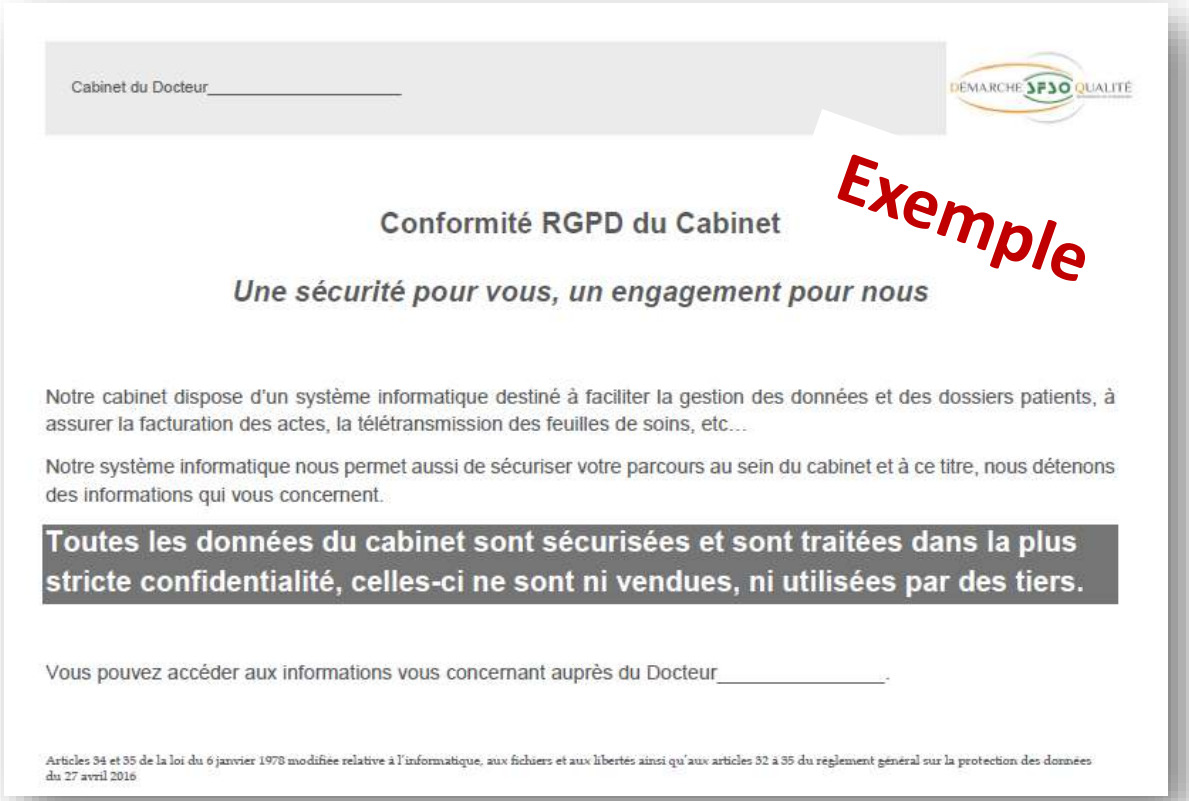
- ce à quoi la personne a consenti,
- le moment où elle a consenti,
- qui a consenti.

Ainsi et en attendant sans doute une proposition d'ajout plus officielle émanant du Syndicat ou de l'Ordre, l'Association vous propose d'ajouter la mention suivante :

Je, soussigné,…….. déclare donner mon consentement au cabinet du Dr…… en ce qui concerne le traitement de mes données de santé et/ou celles de mon enfant…… à des fins purement médicales, dans le cadre du traitement envisagé (photos, empreintes, radios, antécédents, historiques des soins,…). A ce titre, toutes les données du cabinet sont sécurisées et sont traitées dans la plus stricte confidentialité, celles-ci ne sont ni vendues, ni utilisées par des tiers.

Informer les patients

- Un affichage obligatoire dans la salle d'attente



Cabinet du Docteur_____

DÉMARCHE SFSO QUALITÉ

Exemple

Conformité RGPD du Cabinet

Une sécurité pour vous, un engagement pour nous

Notre cabinet dispose d'un système informatique destiné à faciliter la gestion des données et des dossiers patients, à assurer la facturation des actes, la télétransmission des feuilles de soins, etc…

Notre système informatique nous permet aussi de sécuriser votre parcours au sein du cabinet et à ce titre, nous détenons des informations qui vous concernent.

Toutes les données du cabinet sont sécurisées et sont traitées dans la plus stricte confidentialité, celles-ci ne sont ni vendues, ni utilisées par des tiers.

Vous pouvez accéder aux informations vous concernant auprès du Docteur_____.

Articles 34 et 35 de la loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ainsi qu'aux articles 32 à 35 du règlement général sur la protection des données du 27 avril 2016

Accès aux données par les patients

Le délai de réponse passe de 8 jours à un mois maximum à compter de la réception de la demande. Il est possible de prolonger de deux mois ce délai, « compte tenu de la complexité et du nombre de demandes», à condition d'en informer le patient dans le délai d'un mois suivant la réception de sa demande.
En outre, le RGPD prévoit la gratuité des copies fournies dans le cadre d'une demande d'accès.
Si le patient présente sa demande par voie électronique, les informations demandées sont communiquées sous une forme électronique d'usage courant, à moins que le patient ne demande qu'il en soit autrement.

Des droits des patients renforcés

Les droits déjà existants sont renforcés (consentement, transparence). Le patient doit être informé de manière claire, intelligible et facilement accessible sur ses droits :

- droit d'accès et de rectification,
- droit à l'oubli,
- droit à la portabilité des données,
- droit de réparation des dommages, matériels ou moral,
- droit d'effacement,
- droit à la limitation du traitement,
- droit d'opposition,
- principe des actions collectives,
- conditions particulières du traitement des données pour les mineurs de moins de 16 ans (le tuteur légal prime dans le recueil du consentement).

Boîte à outils Qualité

Le RGPD, élargi dans le cadre de la démarche qualité à l'attention portée à la sécurité informatique, fait l'objet de plusieurs traductions dans le cadre de votre démarche :

- Manuel qualité de l'Association SFSO Démarche Qualité : mention d'un plan d'action RGPD identifié
- Outils :
  - Guide RGPD V1 – Juin 2018
  - Registre de traitement + Etude D'impacts – exemple

Annexes et sources – supports utiles pour aller plus loin

[Retrouvez toutes les informations utiles sur : https://www.cnil.fr/fr/rgpd-et-professionnels-de-sante-liberaux-ce-que-vous-devez-savoir]