Union Régionale des Professionnels de Santé des Chirurgiens-Dentistes Auvergne Rhône-Alpes

Guide pratique du Règlement Général sur la Protection des Données (RGPD*)

Réalisé par l'Union Régionale des Professionnels de Santé des Chirurgiens-Dentistes Auvergne-Rhône-Alpes

**Le RGPD s'applique à tous les supports qu'ils soient papiers ou numériques.*

URPS CD Auvergne – Rhône-Alpes
15, Avenue des Frères Montgolfier - 63170 Aubière
04.73.14.62.27 - contact@urps-cd-ara.fr

20260120-VF
Réalisation : URPS CD ARA

Table des matières

URPS CD Auvergne – Rhône-Alpes
15, Avenue des Frères Montgolfier - 63170 Aubière
04.73.14.62.27 - contact@urps-cd-ara.fr

20260120-VF
Réalisation : URPS CD ARA

1. INTRODUCTION : QU'EST-CE QUE LE RGPD ?

Le Règlement Général sur la Protection des Données personnelles du 27 avril 2016 (RGPD), entré en vigueur le 25 mai 2018, s'inscrit dans la continuité des principes déjà établis par la loi Informatique et Libertés du 6 janvier 1978.

Il modifie cependant la logique en vigueur. Nous passons d'un contrôle a priori, reposant sur des formalités préalables auprès de la CNIL (déclarations, autorisations, engagements de conformité, etc.), à un régime de responsabilisation des acteurs traitant des données personnelles, comme les pharmaciens.

Qu'est-ce qu'une donnée personnelle ou donnée à caractère personnel ?

Toute information permettant d'identifier directement ou indirectement une personne.

Qu'est-ce qu'une donnée de santé ?

Toute information liée à la santé physique ou mentale, passée, présente ou future, d'une personne physique (y compris les prestations de soins de santé) qui révèle des éléments sur l'état de santé de cette personne.

Liens utiles :

- Sécurité (URPS CD ARA) : le replay du webinaire sur le RGPD - URPS (urps-cd-ara.fr)
- Accueil - Ordre National des Chirurgiens-Dentistes (ordre-chirurgiens-dentistes.fr)

20260120-VF
Réalisation : URPS CD ARA

2. LE RESPONSABLE DE TRAITEMENT

Le responsable de traitement est la personne morale (entreprise, commune, etc.) ou physique qui détermine les finalités et les moyens d'un traitement, c'est à dire l'objectif et la façon de le réaliser. En pratique et en général, il s'agit de la personne morale incarnée par son représentant légal.

⇒ **Dans une SCM, les praticiens associés ont une patientèle distincte :**

- Les dossiers médicaux (papier et informatique) sont donc parfaitement séparés ;
- En cas de départ, l'associé a le droit d'emmener uniquement les dossiers correspondant à sa base patientèle ;
- Chaque praticien est responsable des traitements de sa patientèle.

⇒ **Dans une société d'exercice, c'est la société qui est titulaire de la patientèle :**

- En cas de départ, il est recommandé au praticien de conserver une copie des dossiers de ses patients ou de prévoir contractuellement un droit d'accès en cas de mise en jeu de sa responsabilité.

⇒ **Dans une collaboration libérale, en cas de départ, il faut distinguer :**

- Les patients du titulaire, dont le collaborateur doit garder une copie pour des raisons de responsabilité professionnelle ;
- Les patients du collaborateur, dont le collaborateur garde l'intégralité des dossiers ;
- Chaque praticien est responsable des traitements de sa patientèle.

**Une patientèle = un registre des traitements*

URPS CD Auvergne – Rhône-Alpes
15, Avenue des Frères Montgolfier - 63170 Aubière
04.73.14.62.27 - contact@urps-cd-ara.fr

20260120-VF
Réalisation : URPS CD ARA

3. LE REGISTRE DES TRAITEMENTS

Le registre des activités de traitement est prévu par l'article 30 du RGPD ( ). Il constitue un élément essentiel de la documentation nécessaire au pilotage et à la démonstration de sa conformité au RGPD.

CHAPITRE IV -
Resp Une fiche correspond à un usage précis : le dossier médical ; les contrats de travail ; les recherches médicales, formations, etc.

Chaque fiche comporte les informations obligatoires :

- ⇒ La désignation de l'activité de traitement ;
- ⇒ L'identification du responsable de traitement (la CNIL) ;
- ⇒ Les finalités (objectifs du traitement de données) ;
- ⇒ Les catégories de personnes concernées (acteurs internes ou externes, professionnels ou particuliers) ;
- ⇒ Les catégories de données traitées (comme l'identité, les coordonnées, les informations de connexion ou les données sensibles) ;
- ⇒ Les catégories de destinataires des données (services de la CNIL, tiers) ;
- ⇒ La liste des sous-traitants ;
- ⇒ L'existence de transferts de données en dehors de l'Union Européenne ;
- ⇒ La durée de conservation des données ;
- ⇒ Une description générale des mesures de sécurité prises.

Liens utiles :

- Affichages réglementaires & RGPD – Ordre National des Chirurgiens-Dentistes (ordre-chirurgiens-dentistes.fr)
- Guide pratique RGPD le pharmacien d'officine et la protection des données (cnil.fr)

Nota bene :

Les registres proposés en annexe sont une synthèse du registre proposé par le Conseil National de l'Ordre des chirurgiens-dentistes et le guide pratique de la CNIL dans les officines. Il convient de l'adapter à vos pratiques.

URPS CD Auvergne – Rhône-Alpes
15, Avenue des Frères Montgolfier - 63170 Aubière
04.73.14.62.27 - contact@urps-cd-ara.fr

20260120-VF
Réalisation : URPS CD ARA

4. LA CHARTE INFORMATIQUE

Les utilisateurs ont un usage souvent quotidien de l'outil informatique. Leurs pratiques peuvent avoir un impact direct sur la sécurité des données personnelles et doivent donc être encadrées.

Pour respecter le RGPD, toutes les entreprises qui traitent des données personnelles doivent mettre en place une charte informatique. Cette charte fixe les règles d'utilisation des outils informatiques d'une entreprise, mis à la disposition de ses employés.

La charte informatique définit également les risques encourus dans le cas du non-respect de ces règles et des obligations liées au RGPD.

Pour la mettre en place, voici les étapes à suivre :

1. Information au personnel (fiche CSE à venir) ;
2. Fixation d'une date d'entrée en vigueur de la charte ;
3. Annexe de cette charte :
   ⇒ Au contrat de travail (avenant) ;
   ⇒ Au règlement intérieur (avis CSE art L2312-8 / exemplaire au greffe des Prud'hommes R1321-2 code du travail / exemplaire inspection travail).

En annexe numéro 2, vous trouverez un modèle de charte informatique.

5. LES CONTRATS DE SOUS-TRAITANTS

Le responsable de traitement et le sous-traitant doivent conclure un contrat incluant plusieurs mentions obligatoires listées à l'article 28.3 du RGPD.

Cela doit permettre aux parties :

⇒ D'organiser leurs rapports et leurs obligations respectives au regard de la protection des données personnelles ;

⇒ D'intégrer l'ensemble des mentions listées à l'article 28.3 du RGPD, en les adaptant à leur situation, et mettre en œuvre les obligations ainsi définies.

20260120-VF
Réalisation : URPS CD ARA

Nota bene :

Pour tout nouveau contrat *: compléter et intégrer le modèle en annexe 7.*

Pour les contrats en cours *: s'assurer que les contrats comportent déjà les mentions obligatoires prévues par l'article 28 du RGPD et figurant dans l'annexe 7. Dans le cas contraire, pensez à mettre à jour vos contrats en signant un avenant.*

En cas de transferts hors UE dans un pays dont le niveau de sécurité n'est pas jugé adéquat, il convient d'adopter en sus, des clauses contractuelles types.

Pour connaître le nom du tribunal compétent et les procédures possibles, renseignez-vous auprès de votre protection juridique.

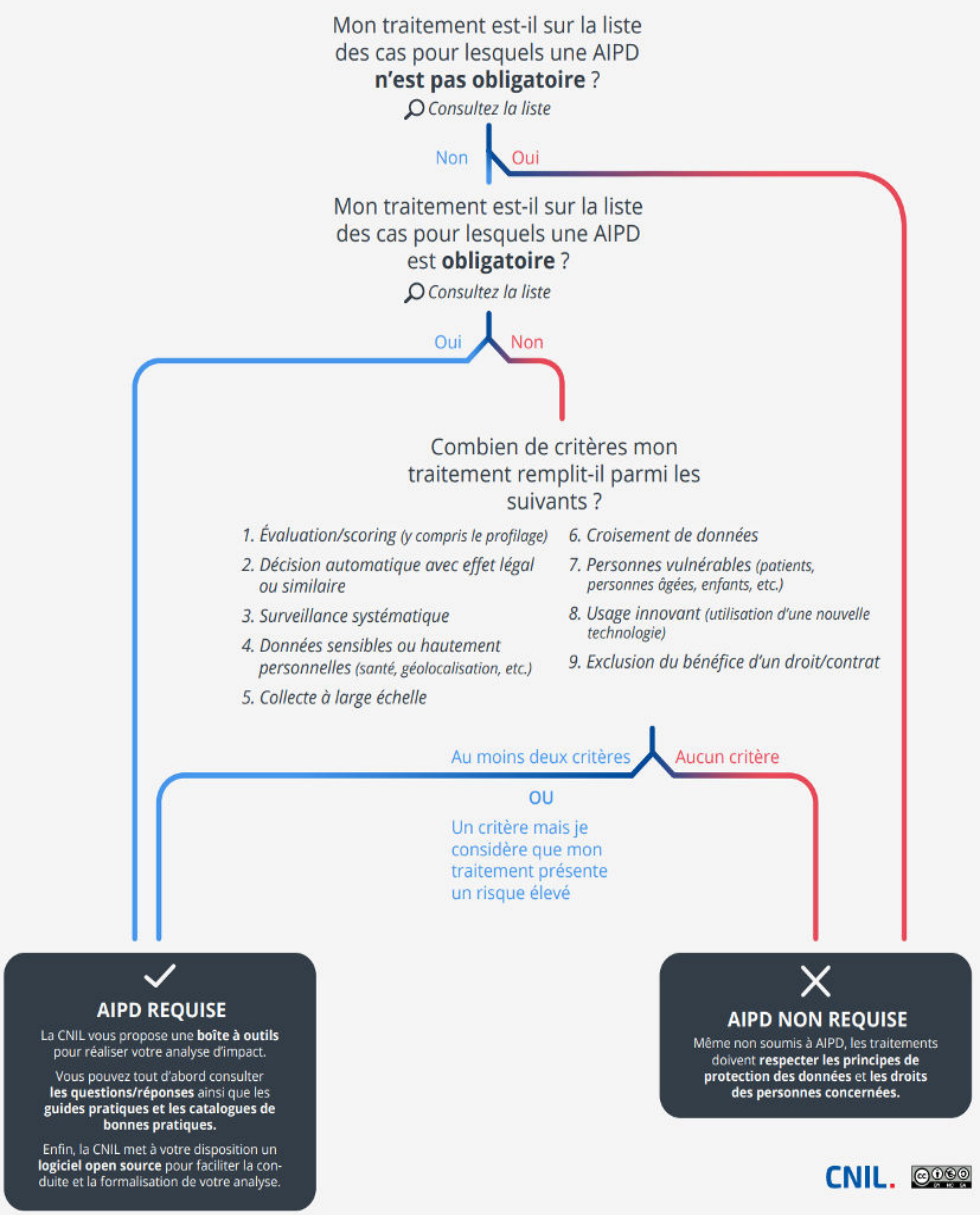
Liste de contrats à réunir :

Contrats de sous-traitants	Finalité
Comptable	RH
Logiciel métier	Dossier médical
Agenda en ligne	Dossier médical
Secrétariat	Dossier médical
Laboratoire de prothèse	Dispositif médical
Empreinte optique	Dispositif médical
Logiciel cone beam	Dossier médical
….	….

URPS CD Auvergne – Rhône-Alpes
15, Avenue des Frères Montgolfier - 63170 Aubière
04.73.14.62.27 - contact@urps-cd-ara.fr

20260120-VF
Réalisation : URPS CD ARA

6. L'ANALYSE D'IMPACT SUR LA PROTECTION DES DONNEES



URPS CD Auvergne – Rhône-Alpes
15, Avenue des Frères Montgolfier - 63170 Aubière
04.73.14.62.27 - contact@urps-cd-ara.fr

20260120-VF
Réalisation : URPS CD ARA

Elle se décompose en 4 parties :

⇒ Description détaillée du traitement mis en œuvre ;

⇒ Une évaluation de la nécessité et de la proportionnalité concernant les principes et les droits fondamentaux ;

⇒ Une étude des risques sur la sécurité des données et de leur impact potentiel sur la vie privée des personnes concernées ;

⇒ Une description des mesures envisagées pour faire face à ces risques.

Liens utiles :

- Logiciel gratuit mis à disposition par la CNIL : PIA https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil
- Guides AIPD de la CNIL :https://www.cnil.fr/fr/guides-aipd

7. QU'EST-CE QU'UN DPO ?

Le délégué à la protection des données (Data Protection Officer - DPO) a une mission d'information, de conseil, de contrôle et d'intermédiaire de l'organisme et de ses collaborateurs. Il contrôle le respect du RGPD et des règles internes.

Il est requis en ligne s'il y a plus de 10 000 dossiers patients (ex. : cabinet de groupe).

Le DPO peut être interne, externe ou mutualisé. Il faut néanmoins vérifier que :

1. **Le DPO détient les compétences requises :**

⇒ Une expertise juridique et technique en matière de protection des données personnelles ;

⇒ Une bonne connaissance du secteur d'activité, de l'organisation interne, en particulier des opérations de traitements, des systèmes d'information, des besoins en matière de protection et de sécurité des données.

20260120-VF
Réalisation : URPS CD ARA

2. **Le DPO ait des moyens suffisants :**

   ⇒ Temps suffisant pour exercer ses missions ;

   ⇒ Moyens matériels et humains adéquats ;

   ⇒ Accès aux informations utiles ;

   ⇒ Association en amont des projets impliquant des données personnelles ;

   ⇒ Facilement joignable.

3. **Le DPO ait la capacité d'agir en toute indépendance :**

   ⇒ Ne pas être en situation de conflit d'intérêt en cas de cumul de sa fonction de DPO avec une autre fonction ;

   ⇒ Pouvoir rendre compte de son action au plus haut niveau de la direction de l'organisme ;

   ⇒ Ne pas être sanctionné pour l'exercice de ses missions de DPO ;

   ⇒ Ne pas recevoir d'instruction dans le cadre de l'exercice de ses missions de DPO.

Outre le DPO, il est conseillé de désigner dans votre structure un référent RGPD et un référent SSI (Sécurité des Systèmes d'Information).

Le référent RGPD assure la conformité aux normes de protection des données et supervise les procédures RGPD en entreprise. Il fait le lien entre l'entreprise et le DPO.

Le Référent de la Sécurité des Systèmes d'Information (RSSI) définit et développe la politique de sécurité de l'information de son entreprise. Il est garant de sa mise en œuvre et en assure le suivi. Le RSSI doit également informer le personnel sur les questions et les normes de sécurité par la mise en œuvre d'outils (chartes numériques, guidelines de sécurité) ou d'activités de communication.

Un MOOC est disponible sur ANSSI ou cybermalveillance.fr.

Lien utile :

- Le délégué à la protection des données (DPO) | CNIL

URPS CD Auvergne – Rhône-Alpes
15, Avenue des Frères Montgolfier - 63170 Aubière
04.73.14.62.27 - contact@urps-cd-ara.fr

20260120-VF
Réalisation : URPS CD ARA

8. LES NOTICES D'INFORMATION

Information des personnes concernées par ces traitements :

Les personnes (patients, salariés, etc.) dont vous traitez les données doivent être informées de l'existence des traitements de leurs données et de leurs droits (tels que droits d'accès, rectification, opposition, effacement, etc.).

Il convient d'informer les personnes concernées de façon claire, simple, concise et facilement accessible.

Nota bene :

Cette mention d'information peut être complétée par d'autres documents distincts afin d'informer vos patients de tout autre traitement ou transmission de leurs données personnelles à des tiers.

Mise en place d'une procédure de traitement des demandes d'exercice de droits :

Les personnes (patients, salariés, etc.) dont vous traitez les données disposent de droits sur leurs données qu'elles peuvent exercer directement auprès du cabinet :

- ⇒ Droit d'accès à toutes les données les concernant ;
- ⇒ Droit de rectification ;
- ⇒ Droit d'effacement ;
- ⇒ Droit à la limitation du traitement ;
- ⇒ Droit de s'opposer au traitement de leurs données, selon les conditions prévues par le RGPD et le cas échéant, d'autres textes applicables.

Nota bene :

Pour vos patients : *vous pouvez mettre cette note d'information à leur disposition au niveau des comptoirs par exemple.*

Pour votre personnel : *vous pouvez leur remettre en main propre.*

20260120-VF
Réalisation : URPS CD ARA

Notices à prévoir	
Information collecte de données de santé	
Vidéoprotection	
Enregistrement communication lors d'appel secrétariat (mention oral)	

9. L'EMPLOI DE L'INTELLIGENCE ARTIFICIEL

C'est parce que le développement de l'intelligence artificielle met en tension des libertés fondamentales qu'elle impose une réflexion éthique, pas pour brider cette technologie mais pour que la promesse qu'elle porte d'amplifier l'intelligence humaine se réalise.

Marie-Laure Denis, présidente de la CNIL

Avant l'utilisation d'une application reliée à l'intelligence artificielle (par exemple ChatGPT), il convient de vérifier son contrat de sous-traitance :

Le responsable du traitement et ses sous-traitants (s'il en a) doivent mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque (*article 32 du RGPD*).

La transparence et l'éthique numérique doivent être vérifiées.

Le fournisseur doit fixer une durée de conservation des données utilisées pour le développement du système d'IA, conformément au principe de limitation de la conservation des données (*article 5.1.d du RGPD*).

Il convient également d'informer de l'emploi de l'Intelligence Artificielle (courrier par exemple).

URPS CD Auvergne – Rhône-Alpes
15, Avenue des Frères Montgolfier - 63170 Aubière
04.73.14.62.27 - contact@urps-cd-ara.fr

20260120-VF
Réalisation : URPS CD ARA

Pour aller plus loin :

En mai 2024, l'Union européenne a adopté définitivement l'IA Act, première législation mondiale visant à encadrer le développement de l'intelligence artificielle.

En classant les systèmes d'IA par niveau de risque, avec des règles proportionnées, l'Europe entend à la fois stimuler l'essor d'une IA « digne de confiance » sur son marché unique et protéger ses citoyens contre les potentiels abus et dérives.

Cette législation impactera les créateurs de logiciels métiers et nous aidera dans la sécurité des données.

10. LA RECHERCHE MÉDICALE

Les traitements de données de santé mis en œuvre à des fins de recherches, études ou évaluations dans le domaine de la santé sont strictement encadrés et nécessitent l'accomplissement de démarches spécifiques :

1. Identifier le traitement : recherche, étude ou évaluation dans le domaine de la santé

Tout d'abord, il convient d'identifier si le traitement répond aux trois critères cumulatifs suivants, définissant une recherche, étude ou évaluation dans le domaine de la santé :

⇒ Il doit s'agir d'une recherche scientifique, c'est-à-dire un projet de recherche établi conformément aux normes méthodologiques et éthiques du secteur et conformément aux bonnes pratiques ;

⇒ Des données de santé doivent être collectées, c'est-à-dire des données personnelles relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne ;

⇒ La recherche doit relever d'un questionnement en matière de santé (médical, paramédical, sanitaire, etc.).

20260120-VF
Réalisation : URPS CD ARA

Les recherches, études ou évaluations dans le domaine de la santé ne sont pas des :

⇒ Entrepôts de données de santé qui, même s'ils sont constitués pour la mise en œuvre de projets de recherche ultérieurs, obéissent à un régime juridique distinct ;

⇒ Recherches scientifiques qui ne poursuivent pas une finalité en lien avec le domaine de la santé et/ou qui ne nécessitent pas le traitement de données relatives à la santé.

2. Identifier le type de recherche et les formalités nécessaires

3. Effectuer les démarches nécessaires auprès de la CNIL

Les formalités requises **consistent en une déclaration de conformité à une méthodologie de référence ou, à défaut de conformité en tout point à ce référentiel, en une autorisation préalable de la CNIL.**

Liens utiles :

- Recherches dans le cadre de la santé : quelles sont les formalités ? | CNIL
- Créer son entrepôt de données de santé (EDS) | Health Data Hub (health-data-hub.fr)

20260120-VF
Réalisation : URPS CD ARA

11. COMMENT RÉAGIR EN CAS DE VIOLATION DES DONNÉES

Malgré les mesures de sécurité mises en place dans votre officine, il se peut que vous constatiez une violation des données personnelles que vous traitez.
Dans ce cas, le RGPD vous impose certaines obligations :

1. Identifier la violation de données personnelles

Constitue une violation de données personnelles tout incident de sécurité ayant comme conséquence de compromettre :

⇒ L'intégrité ;

⇒ La confidentialité ;

⇒ La disponibilité des données (destruction ou perte des données rendant impossible leur consultation pour les personnes autorisées).

Peu importe que cet incident soit d'origine accidentelle ou non, ou encore qu'il se produise dans vos locaux ou chez votre prestataire.

2. Tenir un registre des violations (logiciel métier)

Toute violation de données personnelles doit être documentée en interne. Cela peut prendre la forme d'un registre comportant au minimum les informations suivantes :

⇒ La nature de la violation (exemples : atteinte à l'intégrité, la disponibilité ou la confidentialité des données) ;

⇒ Les catégories et le nombre approximatif des personnes concernées (exemples : 200 patients, 5 employés, etc.) ;

⇒ Les catégories et le nombre approximatif d'enregistrements de données personnelles concernées (exemples : 200 pages de l'ordonnancier, 120 minutes d'images vidéo du mois de septembre, etc.) ;

⇒ Les conséquences probables de la violation (exemples : risque d'usurpation d'identité, risque d'interactions médicamenteuses ou de redondances de traitements, etc.) ;

⇒ Les mesures prises pour remédier à la violation et, le cas échéant, pour limiter les conséquences négatives de la violation (exemples : modifications des droits d'accès, chiffrement des données, etc.) ;

20260120-VF
Réalisation : URPS CD ARA

⇒ Coordonnées personne à contacter.

3. Notifier la violation à la CNIL

Dans quels cas notifier à la CNIL ?

Lorsque cette violation fait peser un risque sur les droits et libertés des personnes dont les données ont été impactées.

Comment notifier à la CNIL ?

Il suffit de compléter le formulaire de téléservice mis à votre disposition sur le site internet de la CNIL, en y indiquant les informations que vous avez consignées à ce titre dans votre registre. La CNIL pourra vous demander des informations complémentaires si besoin.

Dans quel délai notifier ?

Si vous ne disposez pas de toutes les informations lors de votre notification initiale, vous pouvez la compléter par la suite à l'aide d'une notification complémentaire. Cette notification complémentaire doit intervenir si possible dans un délai maximal de 72 h. Si le délai de 72 h est dépassé, les raisons de ce retard seront à justifier auprès de la CNIL.

4. Communiquer la violation aux personnes concernées

Dans quels cas informer les personnes concernées ?

Lorsque le risque sur les droits et les libertés de ces personnes est élevé.

Comment communiquer auprès des personnes ?

La communication doit se faire directement auprès de la personne et peut se faire par tout moyen permettant de s'assurer que la personne a bien été informée (e-mail, SMS …). Si cette information individuelle exige des efforts disproportionnés, il sera alors procédé à une communication plus générale (message sur site web …).

URPS CD Auvergne – Rhône-Alpes
15, Avenue des Frères Montgolfier - 63170 Aubière
04.73.14.62.27 - contact@urps-cd-ara.fr

20260120-VF
Réalisation : URPS CD ARA

12. COMMENT RÉAGIR EN CAS DE CONTROLE DE LA CNIL ?

Qui est la CNIL ?

La Commission Nationale de l'Informatique et des Libertés (CNIL) est le régulateur français des données personnelles. La CNIL accompagne les acteurs privés et publics dans la mise en œuvre de leur conformité en matière de protection des données personnelles.

Dans le cadre de ses missions, elle dispose également de pouvoirs de contrôle sur les organismes. Ces contrôles peuvent faire suite à une réclamation ou au signalement d'un particulier, lorsqu'un organisme ne répond pas à une demande d'exercice des droits, par exemple.

Quel est le déroulement d'un contrôle de la CNIL ?

La CNIL peut procéder à différents types de contrôles :

- **Contrôle sur place :** les agents de la CNIL se rendent directement sur site. Ils peuvent prendre copie de tout document papier ou numérique (contenu d'un ordinateur ou d'un serveur, contenu d'une messagerie, extraction d'enregistrements de caméras de vidéosurveillance, copie des notes d'information, copie des contrats, …) et s'entretenir avec tout membre du personnel.

- **IMPORTANT :** au titre de la loi Informatique et Libertés, l'accès aux données médicales individuelles couvertes par le secret médical ne peut se faire « *que sous l'autorité et en présence d'un médecin* ».

- **Audition du responsable de traitement :** le titulaire de l'officine est convoqué dans les locaux de la CNIL à la date indiquée sur la convocation pour répondre aux questions de la CNIL.

- **Contrôle en ligne :** les agents de la CNIL effectuent des vérifications en consultant toute donnée librement accessible (par exemple : le site internet de l'officine), y compris par négligence ou du fait d'un tiers.

URPS CD Auvergne – Rhône-Alpes
15, Avenue des Frères Montgolfier - 63170 Aubière
04.73.14.62.27 - contact@urps-cd-ara.fr

20260120-VF
Réalisation : URPS CD ARA

- **Contrôle sur pièces :** la CNIL peut adresser un courrier au titulaire de l'officine pour lui demander de répondre à des questions par écrit, et d'y joindre tout document utile.

- **La présidente de la CNIL peut notamment décider de :**
  - ⇒ **Clore la procédure de contrôle avec ou sans observation ;**
  - ⇒ **Mettre en demeure le responsable du traitement** d'adopter des mesures nécessaires pour remédier aux manquements constatés dans un délai imparti et, éventuellement, de justifier des mesures prises et décider de rendre publique cette mise en demeure ;
  - ⇒ **Prononcer un rappel aux obligations légales** à l'encontre du responsable de traitement ;
  - ⇒ **Transmettre le dossier à la formation restreinte de la CNIL qui pourra prononcer des sanctions à l'encontre du responsable du traitement** (allant du rappel à l'ordre au paiement d'une amende administrative pouvant atteindre jusqu'à 20 000 000 € ou 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent) et qui pourra **rendre publique sa décision** en la publiant sur son site internet.

URPS CD Auvergne – Rhône-Alpes
15, Avenue des Frères Montgolfier - 63170 Aubière
04.73.14.62.27 - contact@urps-cd-ara.fr

20260120-VF
Réalisation : URPS CD ARA

13. ANNEXES

1- Registres des activités de traitement (modèle prérempli, à adapter et à compléter)

Docteur :
Coordonnées du titulaire du cabinet et tampon :

Nom et coordonnées du délégué à la protection des données (praticien exerçant seul ou au sein d'un « petit » cabinet de groupe, il n'est pas obligatoire de procéder à la désignation d'un délégué à la protection des données) :

Liste des activités (une fiche par activité) pour lesquelles il existe un traitement de données personnelles :

Liste des activités	**Désignation des activités**
Activité 1	Suivi des patients
Activité 2	Gestion du personnel
…	…

20260120-VF
Réalisation : URPS CD ARA

2- Registre de l'activité de suivi des patients (modèle prérempli, à adapter et à compléter)

Date de création de la fiche :
Date de la dernière mise à jour de la fiche :
Nom du logiciel utilisé pour le suivi des patients :

Objectifs poursuivis :

Objet du traitement :	Suivi des patients du cabinet.
Fonctionnalités du traitement :	Gestion des dossiers médicaux, gestion des rendez-vous, édition des ordonnances, établissement et télétransmission des feuilles de soins.

Catégories de personnes concernées :

Catégorie 1 :	Patients
Catégorie 2 :	Titulaires de l'autorité parentale, tuteur, curateur
Catégorie 3 :	Professionnels de santé
…	…

Catégories de données collectées* :

Etat civil, identité, données d'identification, image :	Nom, prénom, adresse, photo, date et lieu de naissance …
Vie personnelle :	Habitudes de vie, situation familiale…
Vie professionnelle :	Profession ou conditions de travail…

Information d'ordre économique et financier :	Revenus, situation financière, données bancaires…
Données de connexion :	Eventuellement : adresses IP, logs, identifiants des terminaux, identifiants de connexion, informations d'horodatage, etc…
Données de localisation :	Eventuellement : déplacements, données GPS, GSM…
Internet :	Eventuellement : cookies, traceurs, données de navigation, mesures d'audience…
…	…

** Ne peuvent être collectées que les données nécessaires à la prise en charge du patient.*

Données sensibles :

Des données sensibles sont-elles traitées ? OUI : ☐ NON : ☐

Si oui, lesquelles ?

Données sensibles 1 :	Données personnelles de santé
Données sensibles 2 :	NIR
Données sensibles 3 :	Empreintes dentaires

Durées de conservation des catégories de données :

Données personnelles de santé	20 ans à compter de la dernière consultation (et *a minima* jusqu'au 28ème anniversaire)
…	40 ans si dérivés sang

URPS CD Auvergne – Rhône-Alpes
15, Avenue des Frères Montgolfier - 63170 Aubière
04.73.14.62.27 - contact@urps-cd-ara.fr

20260120-VF
Réalisation : URPS CD ARA

Catégories de destinataires de données*

Destinataires internes :	Assistant dentaire, réceptionniste, autre professionnel de santé de la structure
Destinataires externes :	Autre professionnel de santé, organismes de sécurité sociale

** Le secret professionnel et les règles d'échange et de partage d'information des données personnelles de santé devant être respectées.*

Sous-traitants :

Sous-traitant 1 :	Par exemple, prestataire de maintenance informatique.
Sous-traitant 2 :	Par exemple, hébergeurs externes de données de santé personnelles.
…	Logiciel métier
	Télésecrétariat
	Agenda en ligne

Transfert des données hors UE*

Des données personnelles sont-elles transmises hors de l'Union Européenne ?

OUI : ☐ NON : ☐

Si oui, lesquels ?

** En cas de transfert de données hors UE, des précautions particulières doivent être prises. Il est vivement conseiller de se rapprocher de la CNIL.*

URPS CD Auvergne – Rhône-Alpes
15, Avenue des Frères Montgolfier - 63170 Aubière
04.73.14.62.27 - contact@urps-cd-ara.fr

20260120-VF
Réalisation : URPS CD ARA

Mesures de sécurité :

Description des mesures de sécurité organisationnelles et techniques prévues pour préserver la confidentialité des données – le niveau de sécurité étant adapté aux risques soulevés par le traitement.

Catégories	Mesures
Sensibiliser les utilisateurs	Informer et sensibiliser le personnel accédant aux données
	Rédiger une charte informatique et lui donner force contraignante
Authentifier les utilisateurs	Définir un authentifiant à chaque utilisateur
	Adopter une politique de mot de passe conforme aux recommandations CNIL
	Pour les données de santé, privilégier les solutions d'authentification forte avec carte CPS
Gérer les habilitations, **Tracer les accès et gérer les incidents**	Adapter le profil d'habilitation à chaque utilisateur (administratif, soignant)
	Supprimer les permissions d'accès obsolètes (trace registre)
	Mettre en place un système de journalisation d'accès aux données de santé (paramètres logiciel métier)
	Informer les utilisateurs du journal d'accès
	Prévoir les procédures pour les notifications de données à caractère personnel

Sécuriser les postes informatiques et l'informatique mobile.	Prévoir un verrouillage automatique des postes au bout d'un délai d'inactivité de 5 min dans les zones ouvertes au public
	Protéger les postes susceptibles d'être facilement emportés à l'aide d'un câble physique de sécurité (ordinateur portable)
	Chiffrement de tous les ordinateurs et supports amovibles
	Mise à jour automatique des antivirus
	Activer le pare feu (physique ou logiciel)
	Recueillir accord utilisateur avant toute intervention sur le poste
	Limiter le stockage des données de santé sur les tablettes, ordiphone et prévoir une sécurité équivalente à celui des autres équipements (chiffrement, code d'accès...)
	Exiger un code secret pour le déverrouillage des tablettes
	Protéger les écrans des regards indiscrets (filtre, orientation)
	Prévoir une zone de confidentialité
	Répertorier les supports de sauvegarde amovibles et prévoir leur stockage sécurisé et leur chiffrement
	Aucun usage personnel avec les outils informatiques professionnels

URPS CD Auvergne – Rhône-Alpes
15, Avenue des Frères Montgolfier - 63170 Aubière
04.73.14.62.27 - contact@urps-cd-ara.fr

20260120-VF
Réalisation : URPS CD ARA

Protéger le réseau informatique interne	Interdire la connexion d'appareils non professionnels sur le réseau WIFI
	En cas de fourniture d'un accès WIFI public aux patients, cloisonner les accès afin que le WIFI interne soit inaccessible
	Informer des risques du WIFI public (passeport du voyageur ANSSI)
Sécuriser les serveurs	Hiérarchiser le réseau avec un compte administrateur, des comptes utilisateurs (droit adapté aux postes) et un compte invité
	Mise à jour automatique
Sauvegarder et prévoir continuité d'activité	Effectuer des sauvegardes régulières
	Stocker les supports de sauvegarde dans un endroit sûr avec accès restreint
	Prévoir et tester régulièrement les sauvegardes
	Cloud certifié HDS ou Secnumcloud
Archiver de manière sécurisée	Mettre en œuvre des modalités d'accès spécifiques aux données archivées
	Détruire les archives obsolètes de manière sécurisée
Encadrer la maintenance et la destruction des données	Registre des maintenances
	Effacer les données de tout matériel avant recyclage (procédure ANSSI) ou prévoir sa destruction
	Anticiper le remplacement du matériel obsolète

URPS CD Auvergne – Rhône-Alpes
15, Avenue des Frères Montgolfier - 63170 Aubière
04.73.14.62.27 - contact@urps-cd-ara.fr

20260120-VF
Réalisation : URPS CD ARA

Gérer la sous-traitance (logiciel métier, agenda en ligne, télésecrétariat) :	Lister les logiciels métiers nécessaires à la finalité et documenter en annexe.
	Clauses spécifiques en cas de transferts de données hors UE
	Clauses de transparence et de garantie humaine si usage d IA
	Garantie de sécurité
Sécuriser les échanges avec d'autres organismes	Utiliser des mails à usage professionnel qui utilisent un **protocole sécurisé** HTTPS, IMAPS, POPS
	Authentifier les mails avec création d'une messagerie professionnelle par utilisateur
	Pour les données de santé, canal sécurisé
	Vérifier qu'il s'agit du bon destinataire
	Clause de confidentialité en bas des mails
	Transmettre le code secret lors d'un envoi distinct et via un canal différent
Protéger les locaux	Restreindre les accès aux locaux au moyen de portes verrouillées
	Alarme anti-intrusion
	Coffre-fort pour les cartes CPS
Encadrer les développements informatiques	Designer un référent Sécurité des Systèmes d'Information
	Activer la navigation privée

URPS CD Auvergne – Rhône-Alpes
15, Avenue des Frères Montgolfier - 63170 Aubière
04.73.14.62.27 - contact@urps-cd-ara.fr

20260120-VF
Réalisation : URPS CD ARA

3- Registre de l'activité de gestion du personnel (modèle prérempli, à adapter et à compléter)

Date de création de la fiche :
Date de la dernière mise à jour de la fiche :
Nom du logiciel utilisé pour le suivi des patients :

Objectifs poursuivis :

Objet du traitement :	Suivi de la gestion du personnel.
Fonctionnalités du traitement :	Gestion administrative du personnel, gestion de la paie, gestion des horaires...

Catégories de personnes concernées :

Catégorie 1 :	Assistant dentaire
Catégorie 2 :	Réceptionniste
Catégorie 3 :	Chirurgien-dentiste salarié

Catégories de données collectées* :

Etat civil, identité, données d'identification, image :	Nom, prénom, adresse, nationalité, date de naissance, sexe, emploi, qualification, dates d'entrée et de sortie de l'établissement.
Vie professionnelle :	Type de contrat.
Vie personnelle :	Situation familiale…
Information d'ordre économique et financier :	Revenus, situation financière, données bancaires…

Données de connexion :	Eventuellement : adresses IP, logs, identifiants des terminaux, identifiants de connexion, informations d'horodatage, etc…
Données de localisation :	Eventuellement : déplacements, données GPS, GSM…
Internet :	Eventuellement : cookies, traceurs, données de navigation, mesures d'audience…
…	…

** Ne peuvent être collectées que les données nécessaires à la gestion du personnel (principe de collecte de données pertinentes).*

Données sensibles :

Des données sensibles sont-elles traitées ? OUI : ☐ NON : ☐

Si oui, lesquelles ?

Données sensibles 1 :	NIR
…	…

Durées de conservation des catégories de données :

5 ans	Bulletin de paie
	Registre unique du personnel.
	Document concernant les contrats de travail, salaires, primes, indemnités, soldes de tout compte, régimes de retraite.
	Comptabilisation des horaires des salariés, des heures d'astreinte et de leur compensation

5 ans	Déclaration d'accident du travail auprès de la caisse primaire d'assurance maladie
1 an	Document relatif aux charges sociales et à la taxe sur les salaires

Catégories de destinataires de données* :

Destinataires externes :	Organismes sociaux, médecine du travail, IRSN.

Sous-traitants :

Sous-traitant 1 :	Par exemple, service de gestion de paie.
…	…

Transfert des données hors UE*
Des données personnelles sont-elles transmises hors de l'Union Européenne ?

OUI : ☐ NON : ☐

Si oui, lesquels ?

** En cas de transfert de données hors UE, des précautions particulières doivent être prises. Il est vivement conseiller de se rapprocher de la CNIL.*

Mesures de sécurité :

Description des mesures de sécurité organisationnelles et techniques prévues pour préserver la confidentialité des données – le niveau de sécurité étant adapté aux risques soulevés par le traitement.

Catégories	Mesures
Sensibiliser les utilisateurs	Informer et sensibiliser le personnel accédant aux données
	Rédiger une charte informatique et lui donner force contraignante
Authentifier les utilisateurs	Définir un authentifiant à chaque utilisateur
	Adopter une politique de mot de passe conforme aux recommandations CNIL
	Pour les données de santé, privilégier les solutions d'authentification forte avec carte CPS
Gérer les habilitations, **Tracer les accès et gérer les incidents**	Adapter le profil d'habilitation à chaque utilisateur (administratif, soignant)
	Supprimer les permissions d'accès obsolètes (trace registre)
	Mettre en place un système de journalisation d'accès aux données de santé (paramètres logiciel métier)
	Informer les utilisateurs du journal d'accès
	Prévoir les procédures pour les notifications de données à caractère personnel

Sécuriser les postes informatiques et l'informatique mobile.	Prévoir un verrouillage automatique des postes au bout d'un délai d'inactivité de 5 min dans les zones ouvertes au public
	Protéger les postes susceptibles d'être facilement emportés à l'aide d'un câble physique de sécurité (ordinateur portable)
	Chiffrement de tous les ordinateurs et supports amovibles
	Mise à jour automatique des antivirus
	Activer le pare-feu (physique ou logiciel)
	Recueillir accord utilisateur avant toute intervention sur le poste
	Limiter le stockage des données de santé sur les tablettes, ordiphone et prévoir une sécurité équivalente à celui des autres équipements (chiffrement, code d'accès, etc.)
	Exiger un code secret pour le déverrouillage des tablettes
	Protéger les écrans des regards indiscrets (filtre, orientation)
	Prévoir une zone de confidentialité
	Répertorier les supports de sauvegarde amovibles et prévoir leur stockage sécurisé et leur chiffrement
	Aucun usage personnel avec les outils informatiques professionnels

URPS CD Auvergne – Rhône-Alpes
15, Avenue des Frères Montgolfier - 63170 Aubière
04.73.14.62.27 - contact@urps-cd-ara.fr

20260120-VF
Réalisation : URPS CD ARA

Protéger le réseau informatique interne	Interdire la connexion d'appareils non professionnels sur le réseau WIFI
	En cas de fourniture d'un accès WIFI public aux patients, cloisonner les accès afin que le WIFI interne soit inaccessible
	Informer des risques du WIFI public (passeport du voyageur ANSSI)
Sécuriser les serveurs	Hiérarchiser le réseau avec un compte administrateur, des comptes utilisateurs (droit adapté aux postes) et un compte invité
	Mise à jour automatique
Sauvegarder et prévoir continuité d'activité	Effectuer des sauvegardes régulières
	Stocker les supports de sauvegarde dans un endroit sûr avec accès restreint
	Prévoir et tester régulièrement les sauvegardes
	Cloud certifié HDS ou Secnumcloud
Archiver de manière sécurisée	Mettre en œuvre des modalités d'accès spécifiques aux données archivées
	Détruire les archives obsolètes de manière sécurisée
Encadrer la maintenance et la destruction des données	Registre des maintenances
	Effacer les données de tout matériel avant recyclage (procédure ANSSI) ou prévoir sa destruction
	Anticiper le remplacement du matériel obsolète

URPS CD Auvergne – Rhône-Alpes
15, Avenue des Frères Montgolfier - 63170 Aubière
04.73.14.62.27 - contact@urps-cd-ara.fr

20260120-VF
Réalisation : URPS CD ARA

Gérer la sous-traitance (comptable, avocat) :	Lister les logiciels métiers nécessaires à la finalité et documenter en annexe.
	Clauses spécifiques en cas de transferts de données hors UE
	Clauses de transparence et de garantie humaine si usage d'IA
	Garantie de sécurité
Sécuriser les échanges avec d'autres organismes	Utiliser des mails qui utilisent un **protocole sécurisé** HTTPS, IMAPS, POPS
	Authentifier les mails avec création d'une messagerie professionnelle par utilisateur
	Pour les données de santé, canal sécurisé
	Vérifier qu'il s'agit du bon destinataire
	Clause de confidentialité en bas des mails
	Transmettre le code secret lors d'un envoi distinct et via un canal différent
Protéger les locaux	Restreindre les accès aux locaux au moyen de portes verrouillées
	Alarme anti-intrusion
	Coffre-fort pour les cartes CPS
Encadrer les développements informatiques	Designer un référent Sécurité des Systèmes d'Information
	Activer la navigation privée

URPS CD Auvergne – Rhône-Alpes
15, Avenue des Frères Montgolfier - 63170 Aubière
04.73.14.62.27 - contact@urps-cd-ara.fr

20260120-VF
Réalisation : URPS CD ARA

4- Registre de l'activité de gestion des fournisseurs (modèle prérempli, à adapter et à compléter)

Date de création de la fiche :
Date de la dernière mise à jour de la fiche :
Nom du logiciel utilisé pour le suivi des patients :

Objectifs poursuivis :

Objet du traitement :	Suivi de la gestion des fournisseurs.
Fonctionnalités du traitement :	Suivi des commandes, réceptions, paiements.

Catégories de personnes concernées :

Catégorie 1 :	Fournisseurs
Catégorie 2 :	…

Catégories de données collectées* :

Etat civil, identité, données d'identification, image :	Nom, prénom ou dénomination sociale, adresse, numéro d'inscription au registre du commerce et des sociétés
Information d'ordre économique et financier :	Données bancaires
Données de connexion :	Eventuellement : adresses IP, logs, identifiants des terminaux, identifiants de connexion, informations d'horodatage, etc…
Données de localisation :	Eventuellement : déplacements, données GPS, GSM…

Internet :	Eventuellement : cookies, traceurs, données de navigation, mesures d'audience…
…	…

** Ne peuvent être collectées que les données nécessaires à la gestion des fournisseurs (principe de collecte de données pertinentes).*

Données sensibles :

Des données sensibles sont-elles traitées ? OUI : ☐ NON : ☐

Si oui, lesquelles ?

Données sensibles 1 :	
…	…

** Pour mémoire, les dispositions relatives au secret professionnel s'opposent à ce que les fournisseurs connaissent l'identité des patients (y compris les laboratoires de prothèse dentaire – le patient devant être identifié par un numéro).*

Durées de conservation des catégories de données :

Documents versés au dossier médical du patient (traçabilité des produits et dispositifs utilisés) :	20 ans à compter de la dernière consultation du patient
Eléments strictement comptables (factures) :	10 ans

20260120-VF
Réalisation : URPS CD ARA

Catégories de destinataires de données :

Destinataires externes 1 :	Patient (certificat de conformité aux exigences essentielles…).
Destinataires externes 2 :	Comptable
Destinataires externes 3 :	…

Sous-traitants :

Sous-traitant 1 :	Par exemple, service de comptabilité.
…	…

Transfert des données hors UE*

Des données personnelles sont-elles transmises hors de l'Union Européenne ?

OUI : ☐ NON : ☐

Si oui, lesquels ?

** En cas de transfert de données hors UE, des précautions particulières doivent être prises. Il est vivement conseiller de se rapprocher de la CNIL.*

Mesures de sécurité :

Description des mesures de sécurité organisationnelles et techniques prévues pour préserver la confidentialité des données – le niveau de sécurité étant adapté aux risques soulevés par le traitement.

Catégories	Mesures
Sensibiliser les utilisateurs	Informer et sensibiliser le personnel accédant aux données
	Rédiger une charte informatique et lui donner force contraignante
Authentifier les utilisateurs	Définir un authentifiant à chaque utilisateur
	Adopter une politique de mot de passe conforme aux recommandations CNIL
	Pour les données de santé, privilégier les solutions d'authentification forte avec carte CPS
Gérer les habilitations, **Tracer les accès et gérer les incidents**	Adapter le profil d'habilitation à chaque utilisateur (administratif, soignant)
	Supprimer les permissions d'accès obsolètes (trace registre)
	Mettre en place un système de journalisation d'accès aux données de santé (paramètres logiciel métier)
	Informer les utilisateurs du journal d'accès

	Prévoir les procédures pour les notifications de données à caractère personnel
Sécuriser les postes informatiques et l'informatique mobile.	Prévoir un verrouillage automatique des postes au bout d'un délai d'inactivité de 5 min dans les zones ouvertes au public
	Protéger les postes susceptibles d'être facilement emportés à l'aide d'un câble physique de sécurité (ordinateur portable)
	Chiffrement de tous les ordinateurs et supports amovibles
	Mise à jour automatique des antivirus
	Activer le pare feu (physique ou logiciel)
	Recueillir l'accord de l'utilisateur avant toute intervention sur le poste
	Limiter le stockage des données de santé sur les tablettes, ordiphone et prévoir une sécurité équivalente à celui des autres équipements (chiffrement, code d'accès, etc.)
	Exiger un code secret pour le déverrouillage des tablettes

URPS CD Auvergne – Rhône-Alpes
15, Avenue des Frères Montgolfier - 63170 Aubière
04.73.14.62.27 - contact@urps-cd-ara.fr

20260120-VF
Réalisation : URPS CD ARA

Protéger les écrans des regards indiscrets (filtre, orientation)	
Prévoir une zone de confidentialité	
Répertorier les supports de sauvegarde amovibles et prévoir leur stockage sécurisé et leur chiffrement	
Aucun usage personnel avec les outils informatiques professionnels	
Protéger le réseau informatique interne	Interdire la connexion d'appareils non professionnels sur le réseau WIFI
	En cas de fourniture d'un accès WIFI public aux patients, cloisonner les accès afin que le WIFI interne soit inaccessible
	Informer des risques du WIFI public (passeport du voyageur ANSSI)
Sécuriser les serveurs	Hiérarchiser le réseau avec un compte administrateur, des comptes utilisateurs (droit adapté aux postes) et un compte invité
	Mise à jour automatique
Sauvegarder et prévoir continuité d'activité	Effectuer des sauvegardes régulières
	Stocker les supports de sauvegarde dans un endroit sûr avec accès restreint

URPS CD Auvergne – Rhône-Alpes
15, Avenue des Frères Montgolfier - 63170 Aubière
04.73.14.62.27 - contact@urps-cd-ara.fr

20260120-VF
Réalisation : URPS CD ARA

	Prévoir et tester régulièrement les sauvegardes
	Cloud certifié HDS ou Secnumcloud
Archiver de manière sécurisée	Mettre en œuvre des modalités d'accès spécifiques aux données archivées
	Détruire les archives obsolètes de manière sécurisée
Encadrer la maintenance et la destruction des données	Registre des maintenances
	Effacer les données de tout matériel avant recyclage (procédure ANSSI) ou prévoir sa destruction
	Anticiper le remplacement du matériel obsolète
Gérer la sous-traitance (comptable, avocat) :	Lister les logiciels métiers nécessaires à la finalité et documenter en annexe.
	Clauses spécifiques en cas de transferts de données hors UE
	Clauses de transparence et de garantie humaine si usage d IA
	Garantie de sécurité
Sécuriser les échanges avec d'autres organismes	Utiliser des mails qui utilise un **protocole sécurisé** HTTPS, IMAPS, POPS
	Authentifier les mails avec création d'une messagerie professionnelle par utilisateur
	Pour les données de santé, canal sécurisé
	Vérifier qu'il s'agit du bon destinataire

URPS CD Auvergne – Rhône-Alpes
15, Avenue des Frères Montgolfier - 63170 Aubière
04.73.14.62.27 - contact@urps-cd-ara.fr

20260120-VF
Réalisation : URPS CD ARA

	Clause de confidentialité en bas des mails
	Transmettre le code secret lors d'un envoi distinct et via un canal différent
Protéger les locaux	Restreindre les accès aux locaux au moyen de portes verrouillées
	Alarme anti-intrusion
	Coffre-fort pour les cartes CPS
Encadrer les développements informatiques	Designer un référent Sécurité des Systèmes d'Information
	Activer la navigation privée

URPS CD Auvergne – Rhône-Alpes
15, Avenue des Frères Montgolfier - 63170 Aubière
04.73.14.62.27 - contact@urps-cd-ara.fr

20260120-VF
Réalisation : URPS CD ARA

5- Registre de l'activité prothétique (modèle prérempli, à adapter et à compléter)

Date de création de la fiche :
Date de la dernière mise à jour de la fiche :
Nom du logiciel utilisé pour le suivi des patients :

Objectifs poursuivis :

Objet du traitement :	Prescription de prothèses dentaires
Fonctionnalités du traitement :	Confection dispositif médical

Catégories de personnes concernées :

Catégorie 1 :	Laboratoire dentaire
Catégorie 2 :	…

Catégories de données collectées* :

Etat civil, identité, données d'identification, image :	Fiche pseudo anonymisé
	Données biométriques : empreinte dentaire
	Image 3D
	Photos labiodentaires
Données de connexion :	Logiciel empreinte optique
Données de localisation :	Eventuellement : déplacements, données GPS, GSM…
Internet :	
…	…

URPS CD Auvergne – Rhône-Alpes
15, Avenue des Frères Montgolfier - 63170 Aubière
04.73.14.62.27 - contact@urps-cd-ara.fr

20260120-VF
Réalisation : URPS CD ARA

** Ne peuvent être collectées que les données nécessaires à la gestion des fournisseurs (principe de collecte de données pertinentes).*

Données sensibles :

Des données sensibles sont-elles traitées ? OUI : ☐ NON : ☐

Si oui, lesquelles ?

Données sensibles 1 :	Données biométriques : empreinte dentaire
	Prescription médicale
…	…

** Pour mémoire, les dispositions relatives au secret professionnel s'opposent à ce que les fournisseurs connaissent l'identité des patients (y compris les laboratoires de prothèse dentaire – le patient devant être identifié par un numéro).*

Durées de conservation des catégories de données :

Documents versés au dossier médical du patient (traçabilité des produits et dispositifs utilisés) :	20 ans à compter de la dernière consultation du patient
Eléments strictement comptables (factures) :	10 ans

Catégories de destinataires de données* :

Destinataires externes 1 :	Patient (certificat de conformité aux exigences essentielles…).
Destinataires externes 2 :	Laboratoire

Transfert des données hors UE*

Des données personnelles sont-elles transmises hors de l'Union Européenne ?

OUI : ☐ NON : ☐

Si oui, lesquels ?

** En cas de transfert de données hors UE, des précautions particulières doivent être prises. Il est vivement conseiller de se rapprocher de la CNIL.*

Mesures de sécurité :

Description des mesures de sécurité organisationnelles et techniques prévues pour préserver la confidentialité des données – le niveau de sécurité étant adapté aux risques soulevés par le traitement.

Catégories	Mesures
Sensibiliser les utilisateurs	Informer et sensibiliser le personnel accédant aux données
	Rédiger une charte informatique et lui donner force contraignante
Authentifier les utilisateurs	Définir un authentifiant à chaque utilisateur
	Adopter une politique de mot de passe conforme aux recommandations CNIL
	Pour les données de santé, privilégier les solutions d'authentification forte avec carte CPS
Sauvegarder et prévoir continuité d'activité	Effectuer des sauvegardes régulières
	Stocker les supports de sauvegarde dans un endroit sur avec accès restreint

	Prévoir et tester régulièrement les sauvegardes
	Cloud certifié HDS ou Secnumcloud
Archiver de manière sécurisée	Mettre en œuvre des modalités d'accès spécifiques aux données archivées
	Détruire les archives obsolètes de manière sécurisée
Encadrer la maintenance et la destruction des données	Registre des maintenances
	Effacer les données de tout matériel avant recyclage (procédure ANSSI) ou prévoir sa destruction
	Anticiper le remplacement du matériel obsolète
Gérer la sous-traitance (labo de prothèse, caméra optique) :	Lister les logiciels métiers nécessaires à la finalité et documenter en annexe.
	Clauses spécifiques en cas de transferts de données hors UE
	Clauses de transparence et de garantie humaine si usage d IA
	Garantie de sécurité
Sécuriser les échanges avec d'autres organismes	Utiliser des mails qui utilisent un **protocole sécurisé** HTTPS, IMAPS, POPS
	Authentifier les mails avec création d'une messagerie professionnelle par utilisateur
	Pour les données de santé, canal sécurisé
	Vérifier qu'il s'agit du bon destinataire

URPS CD Auvergne – Rhône-Alpes
15, Avenue des Frères Montgolfier - 63170 Aubière
04.73.14.62.27 - contact@urps-cd-ara.fr

20260120-VF
Réalisation : URPS CD ARA

	Clause de confidentialité en bas des mails
	Transmettre le code secret lors d'un envoi distinct et via un canal différent

URPS CD Auvergne – Rhône-Alpes
15, Avenue des Frères Montgolfier - 63170 Aubière
04.73.14.62.27 - contact@urps-cd-ara.fr

20260120-VF
Réalisation : URPS CD ARA

6- Modèle de charte informatique (modèle prérempli, à adapter et à compléter)

Je soussigné(e) Docteur ……., étant à ce titre amené(e) à accéder à des données à caractère personnel ou des pièces juridiques, déclare reconnaître la confidentialité desdites données.
Je m'engage par conséquent, conformément aux art 121 et 122 de la loi du 06 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ainsi qu'aux art 32 et 35 du règlement général sur la protection des données du 27 avril 2016, à prendre toutes précautions conformes aux usages et à l'état de l'art dans le cadre de mes attributions afin de protéger la confidentialité des informations auxquelles j'ai accès, et en particulier d'empêcher qu'elles ne soient communiquées à des personnes non expressément autorisées à recevoir ces informations.

Je m'engage en particulier à :

- Ne pas utiliser les données auxquelles je peux accéder à des fins autres que celles prévues à mes attributions ;
- Ne divulguer ces données qu'aux personnes dument autorisées ;
- Ne faire aucune copie de ces données sauf à ce que cela soit nécessaire à l'exécution de mes fonctions ;
- Prendre toutes les mesures conformes aux usages et à l'état de l'art dans le cadre de mes attributions afin d'éviter l'utilisation détournée ou frauduleuse de ces données ;
- Prendre toutes précautions conformes aux usages et à l'état de l'art pour préserver la sécurité physique et logique de ces données :
- M'assurer, dans la limite de mes attributions, que seuls des moyens de communications sécurisés seront utilisés pour transférer ces données ;
- Prendre connaissance des process de sauvegarde et de sécurité mises en place.

Cet engagement de confidentialité, en vigueur pendant toute la durée de mes fonctions, demeurera effectif, sans limitation de durée après cessation de mes fonctions, quelle qu'en soit la cause, dès lors que cet engagement concerne l'utilisation et la communication de données à caractère personnel.

J'ai été informé que toute violation du présent engagement m'expose à des sanctions disciplinaires et pénales conformément à la réglementation en vigueur, notamment au regard des art 226-16 à 226-24 du code pénal.

Fait à , le

Signature :

URPS CD Auvergne – Rhône-Alpes
15, Avenue des Frères Montgolfier - 63170 Aubière
04.73.14.62.27 - contact@urps-cd-ara.fr

20260120-VF
Réalisation : URPS CD ARA

7- Modèle de contrat de sous-traitant (modèle prérempli, à adapter et à compléter)

La présente annexe « protection des données personnelles » est partie intégrante du contrat.
Les parties acceptent de se conformer à la règlementation applicable à la protection des données personnelles et en particulier le règlement européen sur la protection des données du 27/04/2016 (l RGPD) et la loi informatique et libertés du 06/01/1978 modifiée.
Préambule,

Pour les besoins de gestion du cabinet, l'entreprise a souhaité le recours de :
……
……
……

Pour la finalité suivante :
……
……
……

Dans ce cadre, la société ……. pourra être amenée à traiter des données personnelles pour le compte du cabinet dentaire.

Objet :

Les présentes clauses ont pour objet de définir les conditions dans lesquelles le sous-traitant s'engage à effectuer pour le compte du Responsable du traitement les opérations de traitement de données personnelles définies ci-après.

Description du traitement faisant l'objet de la sous traitance :

Dans le cadre du présent contrat, le sous-traitant traite les données personnelles suivantes :

Données sensibles 1 :	
	…

Pour répondre à la ou les finalités suivantes :

Objet du traitement :	
Fonctionnalités du traitement :	

A la suite de quoi, il a été décidé ce qui suit :

Article 1 : Obligations de confidentialité

Chaque partie s'engage à garder strictement confidentielles et à ne pas divulguer à des tiers, par quelque moyen que ce soit, les informations qui lui sont transmises ou auxquelles elle aura accès à l'occasion de l'exécution du présent contrat.

Article 2 : Obligations du sous-traitant

Le sous-traitant s'engage à :

- Ne traiter les données que pour les finalités définies par le Responsable du traitement et conformément à ses instructions. Il informera le Responsable du traitement en cas d'instruction qui apparaitrait contraire à la Réglementation applicable à la protection des données personnelles ;
- Prendre toutes mesures techniques et organisationnelles appropriées afin de garantir la confidentialité des données personnelles traitées et un niveau de sécurité conforme au RGPD. A ce titre, il s'engage à ce que les personnes autorisées à traiter les données personnelles pour le compte du Responsable du traitement soient soumises à une obligation de confidentialité ;
- Ne pas transférer les données personnelles hors de l'Union Européenne ;
- Informer le Responsable du traitement de toute violation de données à caractère personnelles dans les meilleurs délais et au plus tard dans les 48h après en avoir eu connaissance ;
- Informer le Responsable du traitement, dans le cas où il ferait appel à un sous-traitant ultérieur pour traiter les données personnelles confiées par le Responsable du traitement. A ce titre, il s'engage à ce que le sous-traitant ultérieur soit soumis à des obligations au moins équivalentes à celles fixées par le présent contrat et demeure pleinement responsable vis-à-vis du Responsable du traitement de l'exécution par ce sous-traitant ultérieur de ses obligations ;

- Mettre à la disposition du Responsable du traitement toute information nécessaire pour démontrer le respect des obligations décrites dans le présent contrat et pour permettre la réalisation d'audits de conformité ;
- Assister le responsable du traitement dans la mise en œuvre de l'exercice des droits des personnes concernées ;
- Les parties s'engagent à coopérer avec l'autorité de contrôle en matière de protection des données personnelles en cas de demande d'information qui pourrait être adressée ou cas de contrôle effectué.

Article 3 : Durée de conservation et restitution des données

Le sous-traitant s'engage à retourner au responsable du traitement l'intégralité des données personnelles des personnes concernées collectées pour le compte du Responsable du traitement et à supprimer définitivement toute copie restante de ces données personnelles **dans les 15 jours au terme du contrat**.

Il s'engage à communiquer, sur simple demande du Responsable du traitement, toute attestation de destruction de ces données.

Article 4 : Responsabilité

Le sous-traitant s'engage à indemniser le Responsable du traitement de tous dommages liés à l'atteinte à la sécurité, l'intégrité ou la confidentialité des données personnelles résultant du manquement de ses obligations au titre du présent contrat, à toute violation de la réglementation applicable à la protection des données personnelles et à tout préjudice d'image ou de réputation lié à un manquement du sous-traitant et à ses obligations au titre du présent contrat.

Article 5 : Juridiction compétente et loi applicable

Le présent contrat est soumis à la loi française et tout litige de ce contrat relève de la compétence des juridictions de ……

Fait à …….

Le…….

20260120-VF
Réalisation : URPS CD ARA

8- Modèles de notices d'informations (modèle prérempli, à adapter et à compléter)

RAPPEL :

Votre cabinet médical est considéré comme un lieu ouvert au public, au sens du code de la sécurité intérieure. Pour installer un système de vidéosurveillance, vous devez obtenir une autorisation de la préfecture valable cinq ans. La demande d'autorisation peut être effectuée en ligne sur le site du ministère de l'Intérieur.

Ensuite, vous devez déclarer votre système de vidéoprotection en complétant le formulaire CERFA n°13806*03.

NIVEAU 1 DE L'INFORMATION :

PANNEAU D'INFORMATION AFFICHÉ DANS LES LOCAUX - ETABLISSEMENT SOUS SURVEILLANCE VIDEO

Etablissement placé sous vidéosurveillance par …….. pour la sécurité des personnes et des biens.

Les images sont conservées pendant un mois et peuvent être visionnées, en cas d'incident, par le personnel habilité du cabinet …….. et par les forces de l'ordre.

Conformément à la réglementation applicable à la protection des données, vous pouvez exercer votre droit d'accès aux images qui vous concernent ou demander toute information sur ce dispositif en écrivant à l'adresse e-mail suivante:

…….ou à l'adresse postale suivante :

……

……

Vous pouvez également, si vous l'estimez nécessaire, introduire une réclamation auprès de la Commission Nationale de l'Informatique et des Libertés (CNIL).

Pour plus d'informations, nous vous invitons à consulter notre note d'information disponible ……

IMPORTANT :

Ce panneau doit être placé à une distance raisonnable des lieux surveillés de manière à ce que la personne puisse facilement reconnaître la zone surveillée.

NIVEAU 2 DE L'INFORMATION :

NOTE D'INFORMATION DESTINEE À VOS PATIENTS ET À VOTRE PERSONNEL

La société……..située à ……. a placé ses locaux sous vidéosurveillance afin d'assurer la sécurité des personnes et de ses biens et lutter, ainsi, contre les vols et les agressions.

En tant que responsable du traitement, la société ……..collecte des images de son personnel, des patients et des visiteurs. Ces images ne sont pas utilisées à des fins de surveillance du personnel, ni de contrôle des horaires.

*Les images peuvent être visionnées, **en cas d'incident**, par le personnel habilité du cabinet …… et par les forces de l'ordre, ainsi que le personnel de la société en charge de la maintenance du matériel agissant en qualité de sous-traitant.*

Ces images sont conservées pendant un mois à compter de leur enregistrement. En cas d'incident lié à la sécurité des personnes et des biens, les images de vidéosurveillance peuvent néanmoins être extraites du dispositif.

Elles sont alors conservées sur un support distinct le temps du règlement des procédures liées à cet incident et accessibles aux seules personnes habilitées dans ce cadre.

Vous pouvez accéder aux données vous concernant ou demander leur effacement. Vous disposez également d'un droit d'opposition et d'un droit à la limitation du traitement de vos données. Pour exercer ces droits ou pour toute question sur le traitement de vos données, vous pouvez nous contacter par voie électronique :

……ou à l'adresse postale suivante :
……
……

Vous pouvez également, si vous l'estimez nécessaire, introduire une réclamation auprès de la Commission Nationale de l'Informatique et des Llibertés (CNIL).

URPS CD Auvergne – Rhône-Alpes
15, Avenue des Frères Montgolfier - 63170 Aubière
04.73.14.62.27 - contact@urps-cd-ara.fr

20260120-VF
Réalisation : URPS CD ARA

NIVEAU 3 DE L'INFORMATION : LORS D'UN MAIL DE RAPPEL DE RENDEZ-VOUS EN PIECE JOINTE

Notice d'information protection des données

Votre chirurgien-dentiste, est amené à recueillir et à conserver dans un dossier, des informations sur votre état de santé.

Pourquoi ?

La tenue du dossier « patient » est obligatoire. Ce dossier a pour finalité d'assurer votre suivi médical et de vous garantir la prise en charge la plus adaptée à votre état de santé. Il garantit la continuité de la prise en charge sanitaire et répond à l'exigence de délivrer des soins appropriés.

Quelle est la durée de conservation ?

Il est conservé en principe 20 ans à compter de la date de votre dernière consultation, par référence aux dispositions de l'art R.1112-7 du code de santé publique applicables aux établissements de santé.

Quels sont les destinataires des informations figurant dans votre dossier ?

Seul votre chirurgien-dentiste a accès à vos informations et, dans une certaine mesure, au regard de la nature des missions qu'il exerce, son personnel. Votre médecin, avec votre consentement pourra également transmettre à d'autres professionnels de santé des informations concernant votre état de santé. Enfin afin de permettre la facturation des actes qu'il réalise, votre médecin est amené à télé transmettre des feuilles de soins à votre caisse de sécurité sociale.

Votre médecin ne communique pas avec votre assureur santé.

Vos dossiers sont traités par un logiciel de gestion de cabinet dentaire XXXXXX porteur de l'agrément DMP v2 et répondant aux cahiers des charges sesam-vitale1.40 Addendum 8.

L'agenda est externalisé sur l'application XXXXXXX certifiée par le label hébergeur de données de santé.

Le télésecrétariat a été confié à la société XXXXXXXXXXXXXXX, composée d'assistant(e)s dentaires qualifié(e)s. Pour des raisons de formations, les communications sont enregistrées et conservées XXX mois.

Le cabinet a placé ses locaux sous vidéosurveillance afin d'assurer la sécurité des personnes et de ses biens et lutter, ainsi, contre les vols et les agressions. Les images sont conservées XXXXXXXXXXX mois.

Pour sécuriser nos échanges, le cabinet préconise l'emploi de la messagerie MS Santé (recommandation du ministère de la santé)

Quels sont vos droits ?

Vous pouvez accéder aux informations figurant dans votre dossier.

Vous disposez par ailleurs, sous certaines conditions, d'un droit de rectification, d'effacement de ces informations ou du droit de vous opposer ou de limiter leur utilisation.

Pour toute question relative à la protection des données ou pour exercer vos droits, vous pouvez vous adresser directement à votre médecin.

9- Check liste de la documentation RGPD

La documentation portant sur vos traitements de données personnelles

☐ Le registre des traitements de données à caractère personnel
☐ Les analyses d'impact réalisées
☐ Si transfert de données hors de l'Union Européenne : les garanties apportées pour encadrer ces transferts *(exemples : clauses contractuelles types)*

La documentation relative à l'information et aux droits des personnes concernées

☐ Les mentions d'information
☐ Les modèles de recueil du consentement des personnes concernées, le cas échéant
☐ La procédure mise en place pour l'exercice des droits des personnes concernées, ou à défaut un document démontrant la sensibilisation de votre personnel sur cette thématique

La documentation relative aux contrats conclus avec vos sous-traitants

☐ Les contrats conclus avec vos sous-traitants conformes au RGPD
☐ La documentation démontrant la conformité de vos sous-traitants *(exemples : documentation relative à leurs mesures de sécurité, certificat pour un hébergeur de données de santé, etc.)*

La documentation relative à la sécurité de vos traitements

☐ La procédure de violation de données personnelles, ou à défaut un document démontrant la sensibilisation de votre personnel sur cette thématique
☐ Le registre des violations de données personnelles

URPS CD Auvergne – Rhône-Alpes
15, Avenue des Frères Montgolfier - 63170 Aubière
04.73.14.62.27 - contact@urps-cd-ara.fr

20260120-VF
Réalisation : URPS CD ARA

14. BIBLIOGRAPHIE

Affichages réglementaires & RGPD – Ordre National des Chirurgiens-Dentistes (ordre-chirurgiens-dentistes.fr)

Guide pratique RGPD le pharmacien d'officine et la protection des données (cnil.fr)

Sécurité (URPS CD ARA) : le replay du webinaire sur le RGPD - URPS (urps-cd-ara.fr)

Assistance aux victimes de cybermalveillance

La CNIL adopte un référentiel sur la gestion des officines de pharmacie | CNIL

Accueil - Ordre National des Chirurgiens-Dentistes (ordre-chirurgiens-dentistes.fr)

URPS CD Auvergne – Rhône-Alpes
15, Avenue des Frères Montgolfier - 63170 Aubière
04.73.14.62.27 - contact@urps-cd-ara.fr