

MEDISSIMO

POLITIQUE DE CONFIDENTIALITE PATIENTS ET AIDANTS

MEDISSIMO a pour priorité absolue la protection de vos données personnelles, collectées et traitées dans le respect de la loi Informatique et Libertés du 6 janvier 1978 et du Règlement Européen (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (« **RGPD** »).

1. Responsable de traitement et sous-traitant

MEDISSIMO a la qualité de responsable de traitement concernant les données collectées sur le site **medissimo.fr**, **medissimo.com** (les « **Sites** »).

Toutefois, MEDISSIMO est conjointement responsable avec les professionnels de santé, lorsqu'ils insèrent vos données personnelles dans les applications web Medissimo Pharmacien et Medissimo Etablissement, ainsi que dans l'application mobile Medissimo Infirmière. C'est également le cas lorsque vous entrez vos données personnelles dans les applications mobiles Medissimo Aidant et Kimed (les « **Applications** »).

2. Données personnelles traitées et moyens de collectes

Données personnelles traitées par Medissimo	Identification	Nom, prénom, date de naissance
	Coordonnées	Adresse postale, email, numéro de téléphone
	Données sensibles	Numéro de sécurité sociale, données de santé (prescriptions et observance)
Moyens de collecte	Collecte directe	Cookies – lors de la navigation sur les Sites et les Applications, des cookies peuvent être installés sur votre terminal (cf. Annexe cookies pour en savoir plus)
	Collecte indirecte	Prescriptions saisies par le pharmacien
		Données d'observance saisies par le patient, les aidants, les pharmaciens et les infirmiers

3. Finalités poursuivies par les traitements de vos données personnelles et bases légales

MEDISSIMO traite vos données personnelles pour des finalités déterminées, suivant différents types de fondements. Les durées de conservation de vos données personnelles dépendent de la finalité poursuivie par le traitement.

FONDEMENTS	FINALITES	DUREE DE CONSERVATION
Exécution des mesures précontractuelles	Création de votre compte sur les Applications Medissimo Aidant et Kimed	3 ans après le dernier contact
Exécution du contrat (service) ou consentement	Partage de données de santé sur les Applications entre vos professionnels de santé : médecins, pharmaciens, infirmiers, établissement médico-social	Les données des Applications Medissimo sont conservées 4 mois en base active, c'est à dire accessible en ligne, et 32 mois en base archive, c'est à dire accessible uniquement sur demande tracée et justifiée.
Exécution du contrat (service)	Traçabilité du circuit médicamenteux	
	Suivi de l'observance	3 ans après le dernier contact
	Envoi de vos documents d'information par communication électronique (email, sms etc.)	
Intérêt légitime	Etudes statistiques destinées aux professionnels de santé	3 ans pour les données personnelles ; durée illimitée pour les données anonymisées
	Gestion des éventuelles procédures amiables ou contentieuses et établissement de la preuve de nos obligations	5 ans après le dernier contact
	Utilisation de cookies ou traceurs pour le bon fonctionnement de nos Sites et Applications	13 mois maximum

Intérêt légitime (obligation déontologique)	Bon fonctionnement des Applications et notamment la traçabilité des opérations	10 ans
Obligation légale	Gestion de l'exercice de vos droits sur le traitement de vos données personnelles	Temps de l'utilisation du dossier en base active 10 ans en base intermédiaire
	Exécution des règles comptables, fiscales et sociales et lutte contre la fraude	6 à 10 ans selon la réglementation applicable

4. Destinataires de vos données personnelles

Les données personnelles sont traitées au sein de l'entreprise.

Les Applications Medissimo peuvent permettre un échange de données avec d'autres applications utilisées par les Professionnels de santé (logiciels de gestion de soins en EHPAD, logiciels de gestion d'officine en pharmacie, etc.). Ces échanges de données sont déclenchés par le Professionnel de santé dans l'Application Medissimo pertinente, et sous sa seule responsabilité. Les informations issues de logiciels tiers et importées dans les Applications Medissimo doivent être contrôlées par les Professionnels de santé qui les utilisent. De la même manière, les Professionnels de santé qui utilisent les Applications Medissimo sont responsables des données qu'ils valident dans ces Applications et qu'ils envoient vers les logiciels tiers.

Vos données peuvent également être transmises à des destinataires externes, uniquement pour les finalités précédemment mentionnées et dans la limite strictement nécessaire à l'accomplissement des tâches qui leurs sont confiées et/ou des dispositions législatives et réglementaires.

Il s'agit notamment :

- Des professionnels de santé constituant votre équipe de soins ;
- De sous-traitants, en particulier des catégories suivantes : prestataires techniques de systèmes d'information, éditeurs de cookies (sur ce point, veuillez consultez l'Annexe cookies) ;
- Des autorités légalement compétentes : Tracfin, organismes sociaux et fiscaux et toutes autorités judiciaires autorisées par les dispositions législatives et réglementaires.

Les données sont hébergées en France par la société OSPI, certifiée Hébergeur de Données de Santé (HDS), conformément à l'article L. 1111-8 du code de la santé publique.

5. Transfert hors UE

Vos données sont traitées sur le territoire de l'Union Européenne. Elles ne font en aucun cas l'objet de transferts dans des pays situés hors de ce territoire.

6. Vos droits

Vous disposez de plusieurs droits sur les données vous concernant et traitées par MEDISSIMO :

- Droit d'effacement ;
- Droit d'accès ;
- Droit de rectification ;
- Droit d'opposition ;
- Droit de limitation du traitement ;
- Droit à la portabilité ;
- Droit de retirer votre consentement à tout moment pour le traitement de vos données de santé ;
- Droit de définir des directives post-mortem relatives à la conservation, l'effacement et la communication de vos données.

7. Contact MEDISSIMO

Vos droits peuvent être exercés auprès de vos professionnels de santé, dont l'identité et les coordonnées sont détaillées dans l'onglet « cercle de soins » de votre Application.

Ils peuvent aussi être exercés en adressant une demande complète à MEDISSIMO, accompagnée d'un justificatif d'identité aux adresses suivantes :

@
dpo@medissimo.fr

MEDISSIMO SAS
Délégué à la Protection des Données
Technoparc – 8, rue Jeanneret
78300 POISSY

La demande devra contenir les noms, prénoms, adresse e-mail ou adresse postale à laquelle vous souhaitez que la réponse de MEDISSIMO vous parvienne. Sauf circonstances particulières justifiées, cette demande recevra une réponse dans un délai d'un mois suivant la réception de la demande.

Enfin, vous disposez du droit d'introduire une réclamation auprès de la CNIL.

SOUS-ANNEXE – COOKIES

1. Que sont les « cookies » ?

Lors de visites sur les Sites / les Applications, des technologies de traçage sont utilisées et des données sont collectées. Le terme « cookies » désigne l'ensemble des technologies de traçage susceptibles d'être utilisées. Il s'agit notamment de fichiers textes enregistrés sur le terminal de l'utilisateur lors de sa visite sur les Sites / les Applications, contenant des informations sur sa navigation et permettant certaines fonctionnalités.

Il existe plusieurs catégories de cookies, qui poursuivent des finalités différentes :

- Les cookies techniques : ces cookies contribuent à rendre les Sites / les Applications utilisables en activant des fonctions de base comme la navigation de page. Les Sites / les Applications ne peuvent pas fonctionner correctement sans ces cookies.
- Les cookies de mesure d'audience : ces cookies aident, par la collecte et la communication d'informations de manière anonyme, à mesurer le nombre de visiteurs et à comprendre comment leur interaction avec les Sites / les Applications.
- Les cookies de réseaux sociaux : ces cookies dits « sociaux » sont liés aux services fournis par des sites tiers, comme les boutons applicatifs « J'aime », « Partager » ou les lecteurs de contenu multimédia. Ils sont utilisés pour fournir des services aux utilisateurs ou pour mémoriser leurs préférences de partage avec les réseaux sociaux.
Le réseau social fournissant un tel bouton applicatif est susceptible d'identifier l'utilisateur grâce à ce bouton, même sans utilisation par l'utilisateur de ce bouton lors de la consultation des Sites / des Applications. En effet, ce type de bouton applicatif peut permettre au réseau social concerné de comprendre la navigation de l'utilisateur sur les Sites / les Applications, du seul fait l'ouverture de la session de l'utilisateur sur son terminal.
- Les cookies publicitaires : ces cookies sont utilisés pour présenter des publicités qui peuvent correspondre aux centres d'intérêts de l'utilisateur, en personnalisant la publicité et le contenu des Sites / des Applications.

Les cookies peuvent être déposés par MEDISSIMO ou par des tiers. Dans ce dernier cas, l'utilisateur est informé et son consentement est recueilli préalablement à leur dépôt, mais MEDISSIMO n'a pas de contrôle direct sur ces cookies. L'utilisateur est invité à se reporter aux politiques de confidentialité des tiers éditeurs de cookies.

2. Droits concernant les cookies

a) Consentement au dépôt de cookies

Conformément aux dispositions applicables ainsi qu'aux recommandations de la CNIL, aucun cookie n'est déposé si l'utilisateur n'a pas préalablement consenti à ce dépôt. Le consentement exprès est recueilli par un dispositif informant l'utilisateur des cookies utilisés, de leurs éditeurs et de leurs finalités ; ce dispositif lui permettant d'accepter ou de refuser le dépôt des cookies.

La durée de validité du consentement de l'utilisateur concernant les cookies est de 13 mois, à l'expiration de cette durée, le consentement est de nouveau requis.

Certains cookies, considérés comme strictement nécessaires à la fourniture du service, sont exemptés de consentement. Tel est notamment le cas des traceurs suivants :

- Les cookies de « panier d'achat »,
- Les cookies « identifiants de session » pour la durée d'une session, ou les cookies persistants limités à quelques heures dans certains cas,
- Les cookies d'authentification,
- Certaines solutions d'analyse de mesure d'audience (analytics),
- Les cookies persistants de personnalisation de l'interface utilisateur (choix de langue ou de présentation).

En tout état de cause, l'utilisateur peut retirer son consentement à tout moment en s'opposant au dépôt des cookies.

b) Opposition au dépôt des cookies

Lorsque l'utilisateur s'oppose à l'installation ou à l'utilisation d'un cookie, un cookie de refus est installé sur son terminal.

- Le paramétrage du navigateur

L'utilisateur peut configurer son navigateur concernant les cookies, afin de refuser ou d'accepter certaines catégories de cookies :

- Google Chrome : <https://support.google.com/chrome/answer/95647?hl=fr>
- Internet Explorer : <https://support.microsoft.com/fr-fr/help/260971/description-of-cookies>
- Mozilla Firefox : <https://support.mozilla.org/fr/kb/cookies-informations-sites-enregistrent>
- Safari : <https://support.apple.com/fr-fr/guide/safari/sfri11471/mac>
- Safari (mobile) : <https://support.apple.com/fr-fr/HT201265>
- Navigateur Android : <https://support.google.com/chrome/answer/95647?co=GENIE.Platform%3DAndroid&oco=1&hl=fr>
- **Le paramétrage des cookies déposés par des tiers**

L'utilisateur peut s'opposer au dépôt des cookies tiers. Par exemple, pour désactiver le cookie Google Analytics, il est possible de télécharger un module complémentaire à l'adresse <https://tools.google.com/dlpage/gaoptout?hl=fr>

- **Le paramétrage des cookies de publicité personnalisée par la plateforme interprofessionnelle « Youronlinechoices »**

L'utilisateur peut se connecter au site Youronlinechoices, proposé par les professionnels de la publicité digitale regroupés au sein de l'association européenne EDAA (European Digital Advertising Alliance) et géré en France par l'Interactive Advertising Bureau France ; et ainsi connaître les entreprises inscrites à cette plateforme et qui offrent la possibilité de refuser ou d'accepter les cookies utilisés par ces entreprises pour adapter aux informations de navigation les publicités susceptibles d'être affichées sur le terminal des utilisateurs : <http://www.youronlinechoices.com/fr/controler-ses-cookies>

Cette plateforme européenne est partagée par des centaines de professionnels de la publicité sur internet et constitue une interface centralisée permettant à l'utilisateur d'exprimer son refus ou son acceptation des cookies susceptibles d'être utilisés afin d'adapter à la navigation de son terminal les publicités susceptibles d'y être affichées. Cette procédure n'empêchera pas l'affichage de publicités sur les sites internet visités, mais ne bloquera que les technologies qui permettant d'adapter des publicités.

ANNEXE 2 – POLITIQUE DE SECURITE

La présente politique de sécurité (la « **Politique de Sécurité** ») présente et synthétise les mesures de sécurité à mettre en œuvre en matière de sécurité informatique : **(1)** par Medissimo, ainsi que **(2)** par les Professionnels de santé et/ou les Etablissements médico-sociaux, dans le cadre du téléchargement, de l'accès, de l'activation, de la consultation et de l'utilisation des Applications Medissimo.

(1) MESURES DE SECURITE MEDISSIMO

Les mesures de sécurité et les garanties apportées par Medissimo quant à la mise en œuvre de mesures techniques et organisationnelles appropriées destinées à la protection des données personnelles sont les suivantes :

- **Contrôle d'accès des utilisateurs**

L'inscription à l'Application Mobile Medissimo Aidant ou Kimed se fait en ligne, depuis l'application. Lors de l'inscription à l'Application Mobile Medissimo Aidant ou Kimed, l'application vérifie l'adresse mail de l'utilisateur. L'accès aux données d'un patient de la pharmacie depuis l'Application Mobile Medissimo Aidant ou Kimed est accordé par le Pharmacien depuis son Application Web Medissimo Pharmacien.

La connexion aux applications de la plateforme utilise l'identifiant et le mot de passe de l'utilisateur, ainsi qu'un code OTP (« One Time Password ») unique à 6 chiffres et un certificat logiciel qui sont fournis par l'hébergeur OSPI.

- **Gestion des habilitations**

L'accès au dossier partagé d'un patient est réservé aux seuls Professionnels de santé habilités à en connaître. L'habilitation d'un Professionnel tient compte de la notion d'équipe de soins, afin que seuls les professionnels effectivement impliqués dans la prise en charge d'un patient ou dans les soins qui lui sont prodigués puissent avoir accès aux informations couvertes par le secret médical.

Toute demande d'habilitation est validée par un responsable MEDISSIMO et les permissions d'accès des professionnels de santé sont supprimées dès qu'ils ne sont plus habilités à accéder aux données de santé du patient.

- **Mesures de traçabilité**

L'accès aux serveurs est strictement réservé aux personnes habilitées et nécessite un certificat, un VPN et une demande d'ouverture chez notre hébergeur. Chaque demande d'ouverture est tracée dans un journal. Il contient les informations suivantes : date, heure, identifiant du développeur, raison de l'accès. Il est possible de récupérer ces informations pendant 6 mois.

De plus, l'hébergeur possède l'ensemble des identifiants se connectant à la plateforme. De la même manière que l'accès aux serveurs pour les développeurs, les connexions à la plateforme des clients sont journalisées. En cas de problème, Medissimo se réserve le droit de demander un « *extract* » (export) au OSPI afin de vérifier ces informations.

- **Mesures de protection des logiciels**

Les données des Applications Medissimo sont hébergées par le prestataire OSPI, hébergeur de données de santé agréé « Hébergeur de Données de Santé » (article L. 1111-8 du Code de la Santé Publique et décret du 4 janvier 2006 relatif à l'hébergement de données de santé à caractère personnel). Ces données sont intégralement hébergées en France et ne sont pas transférées vers un pays tiers ou à une organisation internationale.

Le OSPI est certifié ISO27001 et HDS et a mis en place les mesures de sécurité nécessaires pour se conformer aux exigences des chapitres de la norme ISO27001 et du référentiel de certification HDS.

Medissimo met tout en œuvre afin que ses serveurs et ses applications possèdent les derniers correctifs applicatifs disponibles, y compris pour les correctifs de sécurité. L'hébergeur OSPI communique avec Medissimo régulièrement sur les différentes migrations et corrections appliquées sur ses serveurs.

- **Sauvegarde des données**

L'hébergeur OSPI lance tous les jours une sauvegarde des bases de données des Applications Medissimo. Ces sauvegardes peuvent être restaurées partiellement ou totalement en cas de problème.

De plus, avant chaque mise en production, Medissimo fait une demande à l'hébergeur afin de sauvegarder l'état de la base de données en amont, afin de pouvoir effectuer une récupération en cas de problème.

- **Chiffrement des données**

L'ensemble de la plateforme Medissimo utilise le protocole de communication HTTPS qui permet de chiffrer les requêtes entre les clients et le serveur. De plus, l'accès aux serveurs est restreint à quelques développeurs et nécessite une procédure (voir le paragraphe « Mesures de traçabilité »).

- **Sous-traitants Medissimo**

- a) **Liste des sous-traitants Medissimo**

La plateforme Medissimo n'utilise qu'un hébergeur pour les données de santé des patients : OSPI (pour les serveurs de production et de préproduction).

- b) **Mesures de contrôle des sous-traitants Medissimo**

Le OSPI possède un système d'alerte qui notifie Medissimo en cas de panne. Cela permet à Medissimo d'informer ses clients si le problème persiste, et si le problème est détecté aux heures d'ouvertures du support Medissimo (du lundi au vendredi, de 9h à 18h).

- **Autres mesures**

Les données techniques de développement sont gérées par les outils Confluence et Jira et stockées chez ATlassian.

(2) MESURES DE SECURITE DES PROFESSIONNELS DE SANTE

Les mesures de sécurité à mettre en œuvre par les Professionnels de Santé et/ou les Responsables de traitement, dans le cadre du téléchargement, de l'accès, de l'activation, de la consultation et de l'utilisation des Applications Medissimo sont les suivantes :

- **Contrôle d'accès des utilisateurs**

Dans l'Application Web Medissimo Pharmacien, le Pharmacien titulaire peut créer un compte utilisateur pour chaque membre du personnel de sa pharmacie autorisé à accéder à l'application (pharmacien ou préparateur en pharmacie). Le Pharmacien titulaire s'engage à ne créer de compte que pour les personnes autorisées, à ne fournir les informations relatives à chaque compte qu'à la personne concernée, et à ne pas divulguer ces informations à des tiers.

Dans l'Application Web Medissimo Etablissement pour les établissements, l'infirmière responsable peut créer un compte utilisateur pour chaque membre du personnel de son établissement autorisé à accéder à l'application (médecin, infirmière ou aide-soignant). L'infirmière responsable s'engage à ne créer de compte que pour les personnes autorisées, à ne fournir les informations relatives à chaque compte qu'à la personne concernée, et à ne pas divulguer ces informations à des tiers.

Dans l'Application Mobile Medissimo Aidant, le proche aidant crée son compte dans l'application avec son adresse mail et son mot de passe. L'accès aux données d'un patient de la pharmacie depuis l'Application Mobile Medissimo Aidant est accordé par le Pharmacien depuis son Application Web Medissimo Pharmacien. Avant d'accorder cet accès, le Pharmacien s'engage à contrôler l'identité du proche aidant avec sa pièce d'identité, et à vérifier la carte Vitale du patient.

Dans l'Application Web Medissimo Infirmière, l'Infirmier crée son compte dans l'application avec son adresse mail, son mot de passe, son numéro RPPS ou ADELI. L'accès aux données d'un patient de la pharmacie depuis l'Application Mobile Medissimo Infirmière est accordé par le Pharmacien depuis son Application Web Medissimo Pharmacien. Avant d'accorder cet accès, le Pharmacien s'engage à contrôler l'identité de l'Infirmier avec sa carte professionnelle.

Dans l'Application Mobile Kimed, le patient crée son compte dans l'application avec son adresse mail et son mot de passe. L'accès aux données d'un patient de la pharmacie depuis l'Application Mobile Kimed est accordé par le Pharmacien depuis son Application Medissimo Pharmacien. Avant d'accorder cet accès, le Pharmacien s'engage à contrôler l'identité du patient avec sa pièce d'identité, et à vérifier la carte Vitale du patient.

Chaque compte permettant d'accéder à une Application Medissimo (Pharmacien, Etablissement, Aidant, Infirmière ou Kimed) est nominatif, personnel et inaccessible. Les utilisateurs s'engagent à ne pas divulguer à des tiers les informations relatives à leur compte, et en particulier leur identifiant et mot de passe, et à prendre toutes les mesures nécessaires pour éviter que des personnes non autorisées puissent accéder à ces informations.

- **Mesures de traçabilité**

La responsabilité de la traçabilité est reportée sur l'hébergement agréé HDS.

- **Sauvegarde des données**

La responsabilité de la sauvegarde est reportée par Medissimo sur l'hébergement agréé HDS.

- **Autres mesures**

Les professionnels de santé s'engagent à ne pas accéder à la plateforme depuis un réseau public et s'engagent à sécuriser leurs réseaux internes.