



POLITIQUE GENERALE DE LA SECURITE ET DE LA PROTECTION DES DONNEES A LA CRAMIF

DOCUMENT PUBLIC

Version 1 du 13 mai 2015



SOMMAIRE

	<u>Page</u>
1	Présentation du document et enjeux..... 3
2	Le contexte applicable 4
2.1	La Loi Informatique, Fichiers et Libertés 4
2.2	La PSSI : Politique de Sécurité du Système d'Information 5
3	L'engagement du Directeur Général de la CRAMIF..... 6
4	Les engagements de la CRAMIF 7
4.1	Garanties sur la confidentialité des données..... 7
4.2	Collecte des données personnelles 7
4.3	Non-communication des données personnelles..... 8
4.4	Droit d'accès aux données à caractère personnel..... 8
4.5	Sécurité et confidentialité 8
4.6	Sécurité des locaux, des biens, et des personnes 9
4.7	Cookies Internet 9
4.8	Liens vers d'autres sites..... 9
5	Glossaire de la sécurité 10

1 Présentation du document et enjeux

L'Assurance Maladie a une mission de service public, elle est l'assureur santé obligatoire des salariés qui relèvent du régime général. A ce titre :

- elle détient un patrimoine informationnel unique et stratégique. Elle a donc des responsabilités particulières, dont certaines sont explicitement mentionnées dans la Loi Informatique et Libertés.
- elle met en œuvre son propre Système d'Information qui intègre l'ensemble des ressources humaines, informatiques, matérielles et immobilières mises en œuvre pour les traitements. Ce système d'information est sécurisé.

Ce document présente la politique de sécurité et de protection des données de la CRAMIF. Notre objectif est que toute personne en relation avec la CRAMIF soit toujours pleinement informée des catégories d'informations que nous recueillons, de la manière dont nous les utilisons, et des circonstances dans lesquelles elles peuvent être communiquées ou corrigées.

2 Le contexte applicable

Le contexte applicable à la sécurité mise en œuvre à la CRAMIF se décline à travers la Loi Informatique Fichiers, et Libertés et la Politique de Sécurité des Systèmes d'Information (PSSI)

2.1 La Loi Informatique, Fichiers et Libertés

Extraits des articles 2 et 5 :

La Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés « *s'applique aux traitements automatisés de données à caractère personnel, ainsi qu'aux traitements non automatisés de données à caractère personnel contenues ou appelées à figurer dans des fichiers.*

Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne.

Constitue un traitement de données à caractère personnel toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction.

Constitue un fichier de données à caractère personnel tout ensemble structuré et stable de données à caractère personnel accessibles selon des critères déterminés.

La personne concernée par un traitement de données à caractère personnel est celle à laquelle se rapportent les données qui font l'objet du traitement » (article 2).

Sont soumis à la présente loi les traitements de données à caractère personnel dont le responsable est établi sur le territoire français. »

2.2 La PSSI : Politique de Sécurité du Système d'Information

La Politique de Sécurité du Système d'Information (PSSI) vise à définir les mesures à mettre en œuvre afin de contenir les risques pesant sur le Système d'Information (matériels, logiciels, information traitée, ressources humaines, organisations, infrastructures - sites, locaux).

Elle s'organise à travers les éléments suivants :

- organisation,
- gestion des biens,
- ressources humaines,
- ressources physiques (matériels),
- exploitation et télécommunications,
- contrôles d'accès,
- applications,
- incidents,
- plan de continuité d'activités,
- conformité.

La SSI prend en compte :

- la sécurité des personnes, des biens et des informations (vol de matériel ou de documents, incendie, coupure de courant, occupation de locaux...)
- la sécurité des données et des applications en garantissant l'intégrité, la disponibilité et la confidentialité à un niveau d'exigence élevé,
- la sécurité du matériel pour assurer la disponibilité et un niveau de contrôle d'accès adapté.

La PSSI de la Cramif est l'application stricte de la PSSI de la Caisse Nationale d'Assurance Maladie (CNAMTS), elle-même relevant de la PSSI de l'état. Elle s'appuie sur la norme ISO 27000.

3 L'engagement du Directeur Général de la CRAMIF

En 2009, le Directeur Général, responsable des traitements mis en œuvre à la CRAMIF, a désigné un Correspondant Informatique et Libertés (CIL) qui assure leur conformité au regard de la loi Informatique, Fichiers et Libertés.

En 2005, le Directeur Général désigne le Manager de la Sécurité du Système d'Informations (MSSI) de la CRAMIF en application de la PSSI nationale. En 2013, il lui confie le pilotage de l'ensemble des actions conduisant à la mise en œuvre de la PSSI. Ces orientations sont confirmées par une lettre de mission en 2014.

Avec ces désignations, le Directeur Général s'engage et soutient la mise en œuvre des actions qui concourent à la sécurité et à la protection des données.

4 Les engagements de la CRAMIF

La CRAMIF souhaite s'engager en matière de conformité sur la protection des données et sur la sécurité mise en place conformément à la PSSI, à travers plusieurs dispositifs complémentaires que nous vous présentons dans ce chapitre.

4.1 Garanties sur la confidentialité des données

L'ensemble des données traitées par la CRAMIF sont notamment celles nécessaires à l'accomplissement des missions qui lui sont confiées par le code de la Sécurité Sociale. La CRAMIF s'engage à respecter la confidentialité des données qui lui sont transmises à ce titre. Dans ce cadre elle applique les législations dont elle relève et la PSSI de l'Assurance Maladie.

4.2 Collecte des données personnelles

Les données utilisées par la CRAMIF proviennent de nos partenaires (organismes de Sécurité Sociale et autres partenaires de la sphère sociale). Elles sont complétées sur la base des éléments que vous nous communiquez. Elles peuvent également nous être directement communiquées par vos soins.

La plupart de nos services ne requièrent aucune forme d'inscription ou d'enregistrement, ce qui vous permet de visiter notre site sans avoir à vous identifier. Cependant, certains services peuvent nécessiter la communication de données personnelles. Dans ces cas, selon la réglementation en vigueur, vos données personnelles nous permettent de vous fournir les services attendus et de communiquer avec vous.

4.3 Non-communication des données personnelles

Vos Données personnelles ne seront jamais vendues, partagées ou communiquées à des tiers, en dehors des cas prévus par la Loi.

Vos données personnelles pourront toutefois être communiquées à des tiers agissant pour notre compte dans le cadre d'un traitement spécifique conformément aux finalités pour lesquelles nous sommes dépositaires. Elles seront traitées suivant la réglementation en vigueur. Ces tiers sont liés par contrat à n'utiliser vos données personnelles qu'aux fins convenues et à ne pas les vendre ou les divulguer à d'autres tiers sauf si la loi le requiert et si nous les y autorisons explicitement.

4.4 Droit d'accès aux données à caractère personnel

Chaque fois que nous traitons des données à caractère personnel, nous prenons toutes les mesures exigées pour nous assurer de l'exactitude et de la pertinence de vos données conformément aux finalités pour lesquelles nous les collectons. Vous disposez d'un droit d'accès à vos données personnelles en contactant notre [CIL](#).

4.5 Sécurité et confidentialité

Pour assurer la sécurité et confidentialité des données que nous traitons, nous utilisons des équipements et réseaux protégés par des dispositifs forts validés par l'Assurance Maladie. Lors du traitement de vos données personnelles, nous prenons toutes les mesures visant à les protéger contre toute perte, utilisation détournée, accès non autorisé, divulgation, altération ou destruction.

4.6 Sécurité des locaux, des biens, et des personnes

Les locaux de la CRAMIF sont disposés en plusieurs points géographiques, tous situés en région Ile de France.

Pour les locaux situés avenue de Flandre et place de l'Argonne, La CRAMIF, établissement recevant du public, s'engage à mettre en œuvre l'ensemble des dispositions légales visant à assurer la sécurité des locaux, des biens, et des personnes. Ces deux sites disposent d'un PC sécurité permettant de prendre en charge les interventions d'urgence.

Pour ses centres externes hébergés dans des locaux de l'Assurance Maladie, la PSSI de l'Assurance Maladie s'applique, avec les mêmes exigences.

4.7 Cookies Internet

Notre site internet utilise Google Analytics. En navigant vous nous autorisez à utiliser des cookies à des fins de mesures d'audience. Les services de mesures d'audience permettent de mesurer le nombre de visites, le nombre de pages vues, ainsi que l'activité des visiteurs sur le site et leur fréquence de retour.

Vous pouvez refuser l'utilisation de Google Analytics directement depuis le site.

4.8 Liens vers d'autres sites

La présente Politique de protection des données s'applique uniquement à notre site, et pas aux sites Web détenus par nos partenaires. Nous donnons parfois des liens vers d'autres sites Web que nous jugeons susceptibles d'intéresser nos visiteurs.

Pour tout accès à votre compte assuré depuis notre site, vous serez redirigé sur le site AMELI de l'Assurance Maladie.

5 Glossaire de la sécurité

Confidentialité : caractère réservé d'une information dont l'accès est limité aux seules personnes admises à la connaître pour les besoins du service.

Disponibilité : aptitude du système à remplir une fonction dans des conditions définies d'horaires, de délais et de performances.

Données à caractère personnel : «Toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne» (Art. 2 loi Informatique, Fichiers et Libertés).

Intégrité : garantit que les informations traitées ne sont modifiées que par une action volontaire et légitime.