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

DOCUMENT PUBLIC

Version 3 du 26 juin 2017

SOMMAIRE

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)

La Loi Informatique, Fichiers et Libertés

Conformément à l'article 2 de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

- Une donnée à caractère personnel se défini comme toute information, quel que soit le support (papier, informatique …), susceptible de permettre l'identification d'une personne physique, directement ou indirectement.
- *Un traitement de données à caractère personnel se défini comme 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.*
- *Un fichier de données à caractère personnel se défini comme 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.* Il peut s'agir dans le cas de la CRAMIF d'un assuré, d'un agent ou toute personne dont nous collectons ou traitons les données.

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

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 Le rôle et les responsabilités de chacun des acteurs concernés par la Protection de Données à caractère personnel :

Le Directeur Général de la CRAMIF est le Responsable de Traitement au sens de la loi Informatique et Libertés :

- il définit (par l'intermédiaire des différents responsables), la ou les finalité(s) pour chaque traitement et les moyens mis en œuvre.

Le MSSI (Manager de la Sécurité des Systèmes d'Information) a la responsabilité de veiller au respect des mesures de sécurité nécessaires à la protection des données :

- il procède à l'analyse de risques concernant la Sécurité du Système d'Informations pour chaque déclaration ou modification de traitement, et fait des préconisations,
- il est informé de tous les incidents, failles de sécurité ou violations de données, suit leur résolution et participe à la revue périodique des incidents de sécurité.

Le Correspondant Informatique et Libertés (CIL), veille de manière indépendante au respect de la loi informatique et libertés :

- il analyse ou fait analyser les traitements,
- il établit, actualise et communique aux personnes en faisant la demande, la liste des traitements (ou registre),
- il accompagne la mise en œuvre des traitements de données à caractère personnel, et à cette occasion formule les conseils et les recommandations nécessaires au respect de la loi informatique et libertés,
- il procède aux formalités Informatique et Libertés, préalables à la mise en œuvre des Traitements,

- il reçoit les demandes et les réclamations adressées par les personnes concernées par les traitements, et selon leur nature les instruit ou les transmet aux services compétents,
- il est tenu informé de toute demande ou réclamation gérée par une autre personne dès le début de la saisine et tout au long du traitement,
- il informe et sensibilise le personnel aux enjeux de la protection des données,
- il alerte le responsable des traitements sur l'existence de manquements à la loi *Informatique et Libertés*,
- il est informé dans les 24h de toute détection de violation de données,
- il rédige et remet au responsable des traitements un bilan annuel des actions menées.

Et en cas de contrôle a posteriori par la CNIL :

- il est associé aux échanges,
- il reçoit la copie du procès-verbal et est informé des suites données,
- il reçoit le cas échéant la copie du rapport à des fins de sanction dans le cadre de poursuites,
- il est consulté pour la rédaction des observations en réponse.

4 L'engagement du Directeur Général de la CRAMIF

En 2009, le Directeur Général a désigné un Correspondant Informatique et Libertés (CIL). En 2017, une lettre de mission est venue préciser les contours de l'action du CIL (cf. point 3).

En 2005, le Directeur Général avait déjà désigné le Manager de la Sécurité du Système d'Informations (MSSI) de la CRAMIF en application de la PSSI nationale. En 2013, il lui a confié le pilotage de l'ensemble des actions conduisant à la mise en œuvre de la PSSI, avec une confirmation en 2014 par lettre de mission.

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.

En 2017, le Directeur Général a souhaité formaliser spécifiquement son engagement quant à la Politique Générale de Sécurité des données (voir ci-après).

Lettre d'engagement du Directeur Général de la CRAMIF

Dans le cadre de la politique de gestion des données à caractère personnel, le Directeur Général engage la CRAMIF sur le respect des dix principes suivants :

Principe 1 – Responsabilité

L'organisme est responsable des traitements de données à caractère personnel qu'il met en œuvre directement ou indirectement en France et à l'étranger. En conséquence, il se conforme aux réglementations applicables, en particulier à la loi informatique et libertés.

Conformément aux exigences légales, il accomplit toutes les formalités nécessaires à la mise en œuvre des traitements de données à caractère personnel.

Principe 2 – Détermination des finalités de la collecte de données à caractère personnel

L'organisme détermine les finalités pour lesquelles il recueille des données à caractère personnel. Ces finalités doivent être légitimes et respectées pendant la durée de vie du traitement.

Principe 3 – Transparence et licéité de la collecte

L'organisme ne collecte pas de données à caractère personnel à l'insu des personnes concernées. De la même manière, l'organisme ne collecte pas des données à caractère personnel lorsque les personnes concernées s'y opposent légitimement.

L'organisme fournit aux personnes concernées, auprès desquelles il recueille leurs données à caractère personnel, les informations sur la finalité du traitement, l'identité du responsable du traitement et sur l'étendue de leurs droits.

Principe 4 – Limitation de la collecte des données à caractère personnel.

L'organisme se limite au recueil des seules données à caractère personnel nécessaires à l'atteinte des finalités énoncées.

Principe 5 – Limitation de la conservation des données à caractère personnel

L'organisme veille à la mise à jour des données à caractère personnel qu'il traite tout en respectant les finalités visées. Les durées de conservation ne doivent pas excéder celles nécessaires à l'atteinte des finalités visées.

Principe 6 – Sécurité physique et logique des données à caractère personnel

L'organisme doit déterminer et mettre en œuvre les moyens nécessaires à la protection des systèmes de traitement de données à caractère personnel pour éviter toute intrusion malveillante et prévenir toute perte, altération ou divulgation de données à des personnes non autorisées.

L'organisme détermine et met en œuvre des mesures de sécurité permettant de garantir la confidentialité des données (art 34 de la loi informatique et libertés).

L'organisme exige de ses sous-traitants qu'ils présentent des garanties suffisantes pour assurer la sécurité et la confidentialité des données à caractère personnel.

Principe 7 – Accès aux données à caractère personnel – information

L'organisme met en œuvre les moyens nécessaires pour informer toute personne qui en fait la demande de l'existence de données à caractère personnel qui la concernent et de l'usage qui en est fait.

Il met en œuvre les moyens nécessaires pour garantir aux usagers l'accès aux données à caractère personnel qui les concernent lorsqu'ils en font la demande. Il prend toute mesure pour rectifier ou supprimer les informations erronées.

Principe 8 – Communication et mise en œuvre de la politique de gestion des données à caractère personnel.

L'organisme doit mettre à disposition de ses usagers une information précise sur la politique de gestion des données à caractère personnel et les principes qui la composent.

L'organisme détermine et met en œuvre l'ensemble des mesures opérationnelles utiles et nécessaires pour permettre à ses services d'appliquer les principes de la politique de gestion des données à caractère personnel.

Principe 9 – Respect des principes énoncés.

L'organisme est pourvu d'un Correspondant Informatique et Libertés (CIL) qui veille au respect des règles en matière de collecte et de traitement de données à caractère personnel énoncées dans le présent document.
Toute personne doit pouvoir saisir la Correspondant Informatique et Libertés (CIL) sur les principes énoncés ci-dessus.

Principe 10 – Pérennité de la politique de gestion des données à caractère personnel

Pour les besoins de la pérennité de sa politique de gestion des données à caractère personnel, l'organisme s'assure régulièrement de l'adéquation des principes qui la composent aux évolutions des technologies, du droit et des besoins des usagers et des tiers.

Paris, le 10 MAI 2017

Le Directeur Général

David CLAIR

5 Les engagements de la CRAMIF

Au-delà de l'engagement aux 10 grands principes énoncé précédemment, 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.

5.1 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.

5.2 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.

5.3 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.

5.4 Liens vers d'autres sites

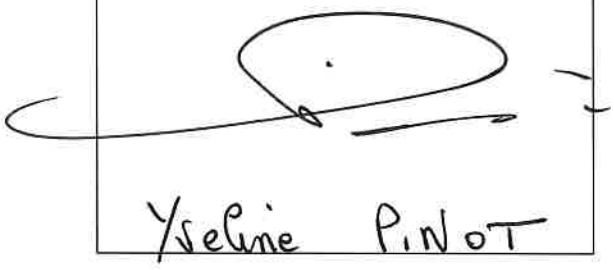
La présente Politique de protection des données s'applique uniquement à notre site, et pas aux sites Web détenus par nos partenaires. Nous donnons parfois des liens vers d'autres sites Web que nous jugeons susceptibles d'intéresser nos visiteurs.

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

Cette politique est diffusée en interne auprès des salariés via l'intranet et en externe via le site internet Cramif.fr.

Validation du CIL :

le 26 Juin 2017



Yseline PINOT

6 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.