l'Assurance Maladie
Agir ensemble, protéger chacun
Caisse nationale

Charte du contrôle T2A

Protection des données personnelles dans le cadre d'un contrôle sur pièces

Table des matières

Contexte 1

I. La base légale de la communication des pièces nécessaires aux personnes chargées du contrôle dans le cadre de leurs missions 2

II. Les catégories de données collectées par les personnes chargées du contrôle 3

III. La confidentialité et la sécurité des données dans le cadre de la transmission des données 4

IV. Les personnes habilitées à accéder aux documents 4

V. Les droits et obligations de l'établissement contrôlé 4

VI. La durée de conservation 5

VII. Les droits des personnes concernées 5

1. L'information des personnes concernées 5

2. Les réponses aux exercices des droits des personnes concernées 5

VIII. La notification et communication des violations de données à caractère personnel ...6~~5~~

Annexe : Description de l'outil Bluefiles ..... 7~~6~~

1. Présentation de l'outil Bluefiles ..... 7~~6~~

2. Le mode opératoire pour le dépôt de fichier ..... 7~~6~~

Contexte

Le contrôle T2A est un contrôle externe mixte, Etat / Assurance Maladie.

La tarification à l'activité (T2A), introduite dans les établissements MCO publics en 2004 et privés en 2005, avec un objectif de répartir de manière efficiente les financements entre les établissements de santé, repose sur un système déclaratif et implique, en contrepartie, un contrôle du respect des règles de codage et des règles de législation de Sécurité Sociale, impactant cette facturation.

Les organismes de Sécurité Sociale contrôlent la bonne application des règles de facturation et de codage fixées par les dispositions de l'article L.162-22-3 du Code de la sécurité sociale (CSS).

Le contrôle de la T2A, au titre de L.162-23-13 du CSS est par conséquent un contrôle de régularité et de sincérité de la facturation, qui peut être réalisé sur pièces et sur place auprès de l'établissement contrôlé soumis à ce mode de tarification.

Ce contrôle nécessite la transmission de tous documents administratifs ou d'ordre médical d'ordre individuel ou général en lien avec les séjours à contrôler. Tout document complémentaire nécessaire au contrôle pourra également être transmis, dans les suites des échanges entre le médecin responsable du contrôle et le médecin DIM. Ce transfert d'information est prévu aux articles R.162-35-2 et R. 166-1 du Code de la sécurité sociale (CSS).

De plus, afin de moderniser, sécuriser et s'inscrire dans la démarche de développement durable, la Caisse nationale d'Assurance Maladie (Cnam) a mis en place une transmission des fichiers de contrôle et des documents administratifs et d'ordre médical nécessaires au contrôle par voie dématérialisée via l'outil sécurisé Bluefiles dans le respect du secret médical.

Ainsi, l'Assurance Maladie met en œuvre des traitements de données dans le cadre de son activité de contrôle prévue par la règlementation en vigueur.

En sa qualité de responsable des traitements de données, l'Assurance Maladie s'engage à assurer la protection, la confidentialité et la sécurité de l'ensemble des données personnelles qu'elle collecte dans le respect de la vie privée des personnes concernées.

Afin d'assurer le bon déroulement de ces missions et de réaffirmer les obligations qu'elle s'impose en qualité de responsable des traitements mis en œuvre sur la base des données collectées auprès des établissements mentionnés, l'Assurance Maladie a décidé de diffuser une charte des contrôles dits T2A.

Cette charte vient compléter le document « Organisation des contrôles T2A, actualisation 2024 » qui décrit tous les points de détail du contrôle. Le Guide du contrôle externe (Contrôle T2A MCO) de 2018 sera prochainement mis à jour pour tenir compte de cette actualisation.

I. La base légale de la communication des pièces nécessaires aux personnes chargées du contrôle dans le cadre de leurs missions

Ce traitement de données à caractère personnel a pour finalité les contrôles des prestations dans le cadre de la lutte contre les abus, fautes, fraudes des professionnels et établissements de santé[1]. Conformément à l'article 6 du Règlement général sur la protection des données (RGPD), la base légale de ce traitement pour les organismes d'Assurance Maladie est fondée sur une obligation légale en vertu des articles L.114-9 et suivants du Code de la sécurité sociale, l'article L.224-14 du Code de la sécurité sociale et l'article L.161-29 du Code de la sécurité sociale.

Dans le cadre de ce traitement, les praticiens-conseils des organismes peuvent procéder à un contrôle sur place et/ou sur pièces[2] auprès des établissements de santé pour constater d'éventuels manquements aux règles de facturation[3], d'erreur de codage ou d'absence de réalisation d'une prestation facturée.

Les organismes d'Assurance Maladie et les établissements sont responsables de traitements distincts dans le cadre de ces contrôles. En effet, les organismes d'Assurance Maladie sont responsables de la réalisation des contrôles auprès des établissements de santé, et les établissements sont responsables des traitements mis en œuvre pour la prise en charge des patients.

Pour permettre aux personnes chargées du contrôle de mener à bien leur mission et nécessaires à la procédure, l'établissement est tenu de leur fournir l'ensemble des documents qu'elles demandent en lien avec le séjour facturé[4], conformément à l'obligation légale confiée

[2] Conformément à l'article L.162-23-13 du Code de la sécurité sociale (CSS)
[3] Conformément aux articles L.162-22-3 et L.162-23-1 du Code de la sécurité sociale
[4] Conformément à l'article R. 162-35-2 du Code de la sécurité sociale

aux organismes d'Assurance Maladie dans le cadre de ses missions de lutte contre la fraude. En ce sens, il n'y a aucune obligation de réaliser une convention dans le cadre du transfert de données des établissements à l'Assurance Maladie.

II. Les catégories de données collectées par les personnes chargées du contrôle

- Documents à transmettre par l'établissement contrôlé en début de contrôle :
  - le fichier informatique des RSS des séjours contrôlés (*SecRssCtl.zip) ;*
  - les éléments du dossier médical relatif au séjour contrôlé, tel que décrit à l'article R 1112-2 du CSP ;
  - les éléments de facturation ;
  - la fiche de liaison adressée par le médecin Conseil responsable du contrôle (MCRC) au médecin du DIM avant le début de contrôle et complétée par l'établissement.

Seuls sont sollicités les documents relatifs aux séjours contrôlés et facturés dans le respect du principe de limitation et de minimisation des données transmises[5].

- Catégorie de données personnelles collectées par les personnes chargées des contrôles :
  - données d'identification du patient (Nom, Prénom, NIR, Date de naissance)[6]
  - données relatives au séjour :
    - diagnostic principal (DP) avec diagnostic relié (DR) si justifié
    - diagnostics associés (DAS) et comorbidités (CMA)
    - acte(s) CCAM
    - supplément(s) le cas échéant
    - données administratives et d'ordre médical du séjour contrôlé précisés dans le format de fichier[7] des RSS de l'année contrôlée :
      - n° administratif de séjour
      - id RUM
      - date de naissance
      - sexe
      - n° UM
      - autorisation lit dédié
      - date entrée et de sortie UM
      - provenance
      - passage structure des urgences
      - poids entrée
      - âge gestationnel
      - date des dernières règles
      - IGS2
      - type de machine RxT
      - type de dosimétrie
      - n° innovation
      - prise en charge RAAC
      - contexte patient
      - surveillance particulière
      - administration de produit de la RH
      - rescrit

[5] Conformément à l'article 5-1 c) du RGPD
[6] Cf Fiche de liaison
[7] Format des RSS précisé annuellement par l'ATIH

- données relatives à la facturation :
  - GHS
  - bordereau S3404
  - suppléments

III. La confidentialité et la sécurité des données dans le cadre de la transmission des données

Les organismes de l'Assurance Maladie s'engagent à prendre toutes les mesures requises en vertu de l'article 32 du RGPD relatif à la sécurité du traitement et adéquation avec la sensibilité des données sous-traitées et à mettre en œuvre les exigences de la Politique de sécurité des systèmes d'information pour les ministères chargés des affaires sociales (PSSI-MCAS) applicables pour les systèmes d'information de l'Assurance Maladie.

Un outil à l'état de l'art des exigences de l'article précité sera utilisé pour l'ensemble des transmissions de données des établissements auprès des organismes de l'Assurance Maladie. De ce fait, pour la réalisation du contrôle sur pièces et afin de sécuriser les échanges, l'établissement transmettra les pièces nécessaires au contrôle via **l'outil sécurisé Bluefiles**, tel que décrit en Annexe de la présente charte.

Les organismes de l'Assurance Maladie s'engagent également à ne divulguer aucune donnée à caractère personnel à un tiers sans l'accord écrit préalable des établissements, et à ne pas utiliser les documents transmis à d'autres fins que celles prévues dans le cadre de cette charte.

IV. Les personnes habilitées à accéder aux documents

Conformément à la charte informatique annexée au règlement intérieur de la Cnam et la PSSI-MCAS, les données et documents collectés lors d'un contrôle et leur conservation ultérieure font l'objet de procédures garantissant leur authenticité, leur intégrité et leur confidentialité, quel qu'en soit le support.

Seuls les agents de l'Assurance Maladie habilités à participer au contrôle T2A de l'établissement contrôlé peuvent accéder aux dossiers de contrôle dans la limite de leur besoin d'en connaître et dans le respect du secret médical.

Conformément à l'article L.161-29 du Code de la sécurité sociale, sont habilités à réaliser un contrôle T2A, les praticiens-conseils (médecin, chirurgien-dentiste et pharmacien) des régimes d'Assurance Maladie, les médecins de l'ARS et les médecins inspecteurs de santé publique. Le praticien responsable du contrôle est un médecin-conseil. Les personnels travaillant sous leur responsabilité sont des techniciens de l'information médicale (TIM), des infirmiers ou du personnel administratif, nommément présentés par le médecin Conseil responsable du contrôle en début de contrôle. Lors du contrôle, les personnels en charge du contrôle, nommément désignés à cette fin, ont accès aux données collectées, sous la responsabilité du médecin Conseil responsable du contrôle.

Les agents de l'Assurance Maladie sont astreints au secret professionnel pour les faits, actes ou renseignements dont ils ont pu avoir connaissance en raison de leurs fonctions, sous peine de poursuites pénales.

V. Les droits et obligations de l'établissement contrôlé

L'établissement de santé a connaissance en amont du contrôle par le DG ARS de la durée du contrôle, soit via le courrier de notification du contrôle de l'ARS, soit lors de l'entretien entre le médecin responsable du contrôle et le médecin DIM.

L'établissement contrôlé peut s'assurer du nom et la qualité du médecin responsable du contrôle, communiqué par le DG ARS lorsque le contrôle a été arrêté.

Il a également connaissance en amont du contrôle par le DG ARS :

- des activités, prestations ou ensemble de séjours sur lesquels porte le contrôle ;
- du caractère sanctionnable ou non d'un champ ;
- de la période concernée par le contrôle.

L'opposition d'un établissement à la préparation ou à la réalisation d'un contrôle, pourrait constituer un obstacle à la réalisation du contrôle[8].

De même, conformément aux dispositions du Code de la sécurité sociale[9], le secret professionnel ainsi que le secret médical ne peuvent être opposés aux personnes chargées du contrôles.

VI. La durée de conservation

Les données et documents collectés lors d'un contrôle et leur conservation ultérieure font l'objet de procédures garantissant leur authenticité, leur intégrité et leur confidentialité, quel qu'en soit le support.

Ces données et documents sont stockés de manière sécurisée, sur un serveur sécurisé accessible uniquement par les personnes habilitées en charge du contrôle.

L'ensemble des pièces transmises par l'établissement contrôlé permettant de justifier la facturation des séjours ciblés sont conservés jusqu'à l'intervention d'une décision définitive en cas de contentieux, conformément au décret n°2015-390 du 3 avril 2015. En l'absence de contentieux, les données et pièces collectées sont détruites dans l'année suivant la clôture du dossier (contrôle sans suite ou indu non contesté et recouvré).

VII. Les droits des personnes concernées

1. L'information des personnes concernées

Comme pour tous les traitements qu'elle met en œuvre, l'Assurance Maladie veille au respect de l'information des personnes concernées, que la collecte soit directe ou indirecte. Une information relative aux contrôles T2A sera renforcée en ce sens sur la politique générale et spéciale de l'Assurance Maladie disponible sur ameli.fr.

Les établissements de santé procèderont également, à l'information des patients sur les traitements de leurs données au sein des livrets d'accueil qui seront complétés afin de les informer de la possibilité que l'Assurance Maladie peut être destinataire de leurs données issues du PMSI, dans le cadre des contrôles T2A.

2. Les réponses aux exercices des droits des personnes concernées

En cas d'exercice de droits réalisé par un assuré (personne couverte par un régime de Sécurité sociale bénéficiant d'une prise en charge de ses frais de santé et exerçant ses droits auprès de sa caisse primaire d'Assurance Maladie de rattachement), au titre du contrôle effectué, il appartient aux organismes de l'Assurance Maladie d'assurer la gestion et l'effectivité des droits

[8] Conformément à l'article R. 162-35-6 du CSS.
[9] Conformément aux articles R. 166-1 du CSS et L. 161-29 du CSS.

des personnes concernées, conformément à l'article 12 du RGPD, et pour les droits énumérés aux articles 15 à 23 du RGPD.

En cas d'exercice de droits réalisé par un patient (personne recevant des soins médicaux et exerçant ses droits auprès de son établissement de santé) au sein de son établissement, il appartient à l'établissement concerné d'assurer la gestion et l'effectivité des droits des personnes concernées, conformément à l'article 12 du RGPD, et pour les droits énumérés aux articles 15 à 23 du RGPD.

VIII. La notification et communication des violations de données à caractère personnel

Si une violation de données sur des données collectées au sein des établissements devait avoir lieu, l'organisme d'Assurance Maladie victime s'engage à prévenir l'établissement et les personnes concernées.

Annexe : Description de l'outil Bluefiles

1. Présentation de l'outil Bluefiles

Bluefiles permet le transfert de mails et/ou de pièces et assure un chiffrement de bout en bout depuis l'émetteur jusqu'à son destinataire, garantissant ainsi la sécurité de l'envoi des pièces nécessaires au contrôle.

La gestion de la sécurité est transparente pour l'utilisateur qui se connecte à son compte via Login / mot de passe, rédige son mail et/ou sélectionne la pièce jointe à transmettre.

Le destinataire hérite de la licence Bluefiles de l'émetteur pour répondre de façon sécurisée avec un mail ou un fichier.

2. Le mode opératoire pour le dépôt de fichier

Le dépôt des documents, sollicités dans le cadre d'un contrôle, dans l'outil Bluefiles est le moyen le plus sécurisé pour collecter des données à caractère personnel et en particulier des données sensibles telles que des données de santé contenues dans les pièces transmises par le médecin DIM de l'établissement de santé concerné.

En effet, l'outil Bluefiles permet de créer et gérer une page de dépôt pour permettre à un tiers de venir y déposer des contenus.

Ainsi, dans le cadre du contrôle T2A, le MCRC crée une page de dépôt via l'interface, et le paramètre en lui donnant un titre [référence du contrôle].

La page de dépôt est ensuite activée, et l'URL de la page est partagée par mail sécurisé avec le médecin du DIM de l'établissement contrôlé.

Ce dernier accède ensuite à l'URL et doit renseigner son e-mail afin de recevoir un lien sécurisé pour transmettre les pièces du contrôle. Cette étape de vérification sécurisée permet de se protéger des robots qui déposent des fichiers de façon malveillante et automatique.

Une fois que le médecin DIM accède à l'URL, il saisit une description de son envoi en rappelant les références du contrôle, un message d'accompagnement facultatif et ajoute les pièces à adresser pour la réalisation du contrôle, puis clique sur "Envoyer".

Point d'attention, le message d'accompagnement des pièces n'étant pas chiffré, il est recommandé de ne pas y inscrire des données à caractère personnel ou des données sensibles telles que des données de santé.

Le MCRC qui a créé la page de dépôt est alors notifié par mail de l'ajout des pièces. Ce dernier y accède via son compte Bluefiles dans "Éléments reçus".

Pour la bonne réalisation du contrôle, une fois le lien URL reçu par le médecin du DIM de l'établissement, il est attendu que les pièces soient **envoyées** dans un délai raisonnable qui concilie les contraintes de l'établissement et la nécessité de ne pas ralentir le déroulement de la mission de contrôle de l'Assurance Maladie.