RÉSEAU DES
RÉFÉRENTS RÉGIONAUX
D'IDENTITOVIGILANCE

Fiche pratique

Gestion des copies de pièces d'identité dans le système d'information

Version 1 du 09/12/2020

LISTE DES CONTRIBUTEURS

- Mme Céline DESCAMPS, CRIV Nouvelle-Aquitaine
- Dr Moufid HAJJAR, Délégué à la protection des données au CHU Bordeaux
- Dr Manuela OLIVER, GRADeS ieSS PACA ieSS
- Mme Emilie PASSEMARD, juriste à la Délégation du numérique en santé
- Dr Bernard TABUTEAU, CRIV Nouvelle-Aquitaine
- M. Bertrand PINEAU GRADeS SESAN Ile de France

SOMMAIRE

1 CONTEXTE

La fiabilisation de l'identification des usagers et des documents les concernant est un enjeu majeur de la sécurité des soins. Le Référentiel national d'identitovigilance (RNIV)[1] stipule qu'elle repose notamment sur le contrôle de cohérence entre les traits d'identité d'un dispositif d'identification à haut niveau de confiance présenté par l'usager et ceux enregistrés dans son identité numérique.

L'objet de cette fiche pratique est de préciser les modalités de recueil, d'utilisation, de conservation et d'information de l'usager concernant la copie d'une pièce d'identité[2].

2 ASPECTS JURIDIQUES

Un document officiel d'identité présente un caractère relativement sensible, en raison notamment des risques de réutilisation frauduleuse des données qu'il contient.

Le droit relatif à la protection des données à caractère personnel suppose des mesures techniques et organisationnelles visant à réduire le traitement des données à caractère personnel conformément aux principes de proportionnalité et à pouvoir être en mesure d'en rendre compte (traçabilité). En particulier, seules les personnes ayant besoin des informations personnelles peuvent être habilitées à y avoir accès.

L'article 5 du RGPD, expose les principes relatifs au traitement des données à caractère personnel et précise notamment que les données doivent être[3] :

- c*) adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données)* ;
- d*) exactes et, si nécessaire, tenues à jour; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder (exactitude)* ;
- *e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées.*

3 MODALITÉS DE GESTION DU DOCUMENT D'IDENTITÉ

3.1 Règles générales

Après consultation de la Commission nationale informatique et libertés (CNIL), il est autorisé de conserver une copie de la pièce d'identité de l'usager dans les mêmes conditions que le dossier patient pour **une durée maximale de 5 ans à compter de la dernière venue de l'usager** dans la structure sous réserve :

- du chiffrement des pièces d'identité numérisées ;
- d'une limitation des accès à cette copie à des professionnels spécifiquement habilités.

Seule la conservation d'une copie de la pièce d'identité sous forme numérique et dans un espace dédié permet de respecter ces conditions pour :

- la gestion de la durée de conservation ;
- la coordination entre acteurs concernés qui disposent d'une seule et unique copie d'une pièce d'identité.

Si le système d'information ne le permet pas, le recours à la photocopie est acceptable, sous couvert

---

1 https://solidarites-sante.gouv.fr/soins-et-maladies/qualite-des-soins-et-pratiques/securite/securite-des-soins-securite-des-patients/article/identitovigilance

2 En dehors du cas où un dispositif électronique d'authentification autorisé a été utilisé pour valider l'identité

3 https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre2#Article5

du respect des principes évoqués hormis le chiffrement, mais nécessite la formalisation d'une procédure rigoureuse pour la gestion de l'accès à l'information aux acteurs habilités.

3.2 Éléments pouvant faire l'objet d'un enregistrement

Tous les éléments présents sur la pièce d'identité peuvent être saisis dans le dossier de l'usager à l'exception du numéro de la pièce d'identité.

3.3 Modalités de conservation en cas de photocopie du document

Dans le cas où seule une conservation sur support papier du document d'identité est envisagée, la photocopie de la pièce d'identité de l'usager doit être conservée dans la partie administrative du dossier patient. Une seule copie doit être conservée par dossier.

Le dossier physique de l'usager est réglementairement conservé dans un local sécurisé et fermé à clef. L'accès au dossier patient est limité à des catégories de professionnels dûment identifiés dans une procédure *ad hoc* (cf. 4).

3.4 Modalités de conservation en cas de numérisation du document

La pièce d'identité numérisée est à conserver, après chiffrement, dans l'outil de gestion administrative de l'usager, dans un espace dédié bénéficiant de droits d'accès spécifiques.

Un document doit décrire les professionnels habilités à consulter ce document (cf. 4) ainsi que les modalités de traçabilité (historisation de la date et de l'identification du professionnel ayant accédé à cette information).

3.5 Destruction du document au-delà de 5 ans

Une procédure formalisée doit préciser l'organisation mise en œuvre dans chaque structure de santé pour garantir la destruction des pièces d'identité lorsque le délai maximal de conservation est dépassé.

Elle peut reposer, par exemple :
- sur le service des archives médicales qui est chargé de détruire le document papier 5 ans après le dernier passage enregistré ;
- sur un mécanisme de suppression automatique ou manuel du document numérisé, notamment après une opération conforme de validation de l'identité INS dans le délai réglementaire de 3 à 5 ans.

4 PROFESSIONNELS HABILITÉS À ACCÉDER AU DOCUMENT D'IDENTITÉ

Seules certaines catégories de professionnels sont habilitées à accéder aux documents d'identification conservés. La liste doit en être précisée dans un document *ad hoc* formalisé par la structure.

En pratique, il s'agira des professionnels qui en ont potentiellement besoin pour la création, le contrôle ou de la modification *a posteriori* de l'identité numérique.

Dans les structures de santé, ces usages sont liés :
- à la validation et/ou à la qualification de l'identité numérique d'un usager quand celle-ci est réalisée de façon secondaire (organisation de la structure qui prévoit la réalisation du contrôle de cohérence en *back office* par une équipe dédiée, en l'absence de l'usager) ;
- au contrôle de cohérence avec l'identité INS, notamment lorsqu'une opération de vérification via le téléservice INSi, prévue par le référentiel INS tous les 3 à 5 ans, révèle des anomalies ;
- au traitement d'une suspicion d'utilisation frauduleuse d'identité ;

- à la sécurisation d'une opération de fusion de dossiers en doublon ;
- à une opération de mise en cohérence des traits d'identité dans le cadre d'un rapprochement des identités inter-structures ;
- à une demande d'expertise quant à la demande d'interprétation des traits, reçue par l'instance opérationnelle d'identitovigilance (locale ou régionale) ;
- au signalement d'une erreur d'identification ou à la demande d'une rectification des traits à la suite d'une erreur de saisie.

À titre indicatif, cette habilitation est susceptible de concerner :
- les professionnels administratifs ou médico-administratifs habilités à créer ou modifier une identité numérique, dans le cadre de leur activité normale ;
- les personnels soignants faisant partie du cercle de confiance des professionnels participant à la prise en charge technique de l'usager, dans le cadre des procédures d'identification secondaire ;
- des membres de l'instance opérationnelle d'identitovigilance locale, dans le cadre de la gestion des risques liés à l'identification des usagers ;
- le médecin responsable du département d'information médicale (DIM), dans les établissements de santé ;
- les professionnels dédiés au traitement des demandes de rectification adressées par les usagers…

5 PRÉCISIONS RELATIVES À LA MISE EN ŒUVRE PRATIQUE DE LA MESURE

5.1 Information des usagers

Les usagers doivent être informés[4] :
- de l'identité et des coordonnées du responsable du traitement, du représentant du responsable du traitement et du délégué à la protection des données ;
- des finalités du traitement auquel sont destinées les données à caractère personnel ainsi que la base juridique du traitement[5] ;
- de la durée de conservation de la copie de leur pièce d'identité ;
- des destinataires de cette donnée ;
- de leur droit d'accès aux informations ainsi conservées ;
- de leur droit de s'opposer à cet archivage.

L'information de l'usager est réalisée via :
- des affiches d'information, disposées dans les points d'accueil, qui évoquent les enjeux de la bonne identification des usagers et les modalités mises en œuvre dans la structure pour la sécuriser ;
- le livret d'accueil de l'usager ;
- d'autres supports si besoin.

5.2 Modalités d'échanges de documents d'identité

Les instances d'identitovigilance locales, territoriales (groupements hospitaliers de territoire) ou régionales peuvent exceptionnellement avoir besoin d'échanger une copie de la pièce d'identité pour statuer sur les bons traits d'identification d'un usager à saisir en cas de discordances constatées ou d'une enquête relative à un événement indésirable.

Dans ce cas, l'échange de la copie de la pièce d'identité ne peut se faire que par messagerie sécurisée

---

[4] Article 13 Règlement Général de Protection des Données. Informations à fournir lorsque des données à caractère personnel sont collectées auprès de la personne concernée

[5] Article 9 Règlement Général de Protection des données. Traitement portant sur des catégories particulières de données à caractère personnel

de santé ou par un dispositif sécurisé et uniquement sur demande dûment justifiée. Après enquête, cette pièce est détruite ou remplace l'ancien document conservé.

La cellule d'identitovigilance à l'origine de la demande doit tracer cette dernière et en justifier la raison.

5.3 Perspectives à moyen terme

Des dispositifs d'identification/authentification de niveau au moins *substantiel* au sens du règlement européen eIADS sont appelés à se développer. Ils pourront être utilisés comme dispositifs d'identification à haut niveau de confiance, tel que prévu par le référentiel national d'identitovigilance (RNIV 1). Il sera nécessaire, lors de leur déploiement, de préciser les modalités de conservation des données qu'ils comportent pour répondre aux besoins de contrôles *a posteriori*.

Pour exemple, il est prévu de disposer d'une carte Vitale dématérialisée (application carte Vitale ou ApCV) de niveau *substantiel* qui devrait permettre, à l'horizon 2023, de disposer d'un dispositif apportant toutes les informations nécessaires pour valider l'identité de l'usager et permettre de qualifier l'identité numérique. La conservation d'une copie de pièce d'identité ne resterait alors nécessaire que pour les usagers non-détenteurs de ce type de dispositif.

6 RÉFÉRENCES

- Référentiel national d'Identitovigilance (https://solidarites-sante.gouv.fr/soins-et-maladies/qualite-des-soins-et-pratiques/securite/securite-des-soins-securite-des-patients/article/identitovigilance)
- Arrêté du 24 décembre 2019 portant approbation du référentiel « Identifiant National de Santé »
- Règlement (UE) 2016/679 du Parlement européen et du Conseil 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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).
- Règlement (UE) N° 910/2014 du parlement Européen et du conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE.