Phase 3 : Mise en perspective des droits et obligations en matière de confidentialité et de communication des données médicales

Partie 1. Cadre juridique de la communication des données médicales en France à la suite de l'entrée en vigueur du règlement européen sur la protection des données personnelles (RGPD)

Le règlement européen sur la protection des données personnelles (RGPD) est entré en application le 25 mai 2018. Il procède à une définition plus large des données de santé qu'auparavant (1). Le droit français s'y est conformé en adoptant les compléments nécessaires.

Par conséquent, un régime juridique particulier est applicable au traitement des données médicales (2) ; les établissements de santé étant soumis à quelques règles supplémentaires par rapport aux praticiens libéraux (3), des sanctions s'appliquent en cas de non-respect (4).

1. La définition des données de santé soumises aux nouvelles règles de confidentialité

Le RGPD définit les données personnelles comme « toute information se rapportant à une personne physique identifiée ou identifiable » c'est-à-dire une personne physique qui peut être identifiée, directement ou indirectement.

En pratique, il peut s'agir de données d'identification comme les nom, prénom, adresse, ou numéro de téléphone, d'informations sur la vie personnelle du patient (ex : nombre d'enfants), sa couverture sociale (ex : assurance maladie obligatoire, assurance maladie complémentaire, etc.) et surtout d'informations relatives à sa santé (pathologie, diagnostic, prescriptions, soins, etc.), les éventuels professionnels qui interviennent dans sa prise en charge, mais également le numéro de sécurité sociale des patients (Numéro d'Inscription au Répertoire des Personnes Physiques - NIR) pour facturer les actes réalisés.

Les données à caractère personnel concernant la santé sont les **données relatives à la santé physique ou mentale, passée, présente ou future, d'une personne physique** (y compris la prestation de services de soins de santé) **qui révèlent des informations sur l'état de santé de cette personne**.

Cette définition comprend donc, parmi d'autres :

1. les informations relatives à une personne physique collectées lors de son inscription en vue de bénéficier de services de soins de santé ou lors de la prestation de ces services : un numéro, un symbole ou un élément spécifique attribué à une personne physique pour l'identifier de manière unique à des fins de santé ;
2. les informations obtenues lors du test ou de l'examen d'une partie du corps ou d'une substance corporelle, y compris à partir des données génétiques et d'échantillons biologiques ;
3. les informations concernant une maladie, un handicap, un risque de maladie, les antécédents médicaux, un traitement clinique ou l'état physiologique ou biomédical de la personne concernée (indépendamment de sa source, qu'elle provienne par exemple d'un médecin ou d'un autre professionnel de santé, d'un hôpital, d'un dispositif médical ou d'un test de diagnostic in vitro).

De plus, cette définition permet d'englober certaines données de mesure à partir desquelles il est possible de déduire une information sur l'état de santé de la personne.

La notion de données de santé est désormais large. Elle est à apprécier, au cas par cas, compte tenu de la nature des données recueillies.

Entrent dans cette notion trois catégories de données :

- celles qui sont des ***données de santé par nature*** : antécédents médicaux, maladies, prestations de soins réalisés, résultats d'examens, traitements, handicap, etc.

- celles, qui du fait de leur ***croisement avec d'autres données, deviennent des données de santé en ce qu'elles permettent de tirer une conclusion sur l'état de santé*** ou le risque pour la santé d'une personne : croisement d'une mesure de poids avec d'autres données (nombre de pas, mesure des apports caloriques…), croisement de la tension avec la mesure de l'effort, etc.

- celles qui deviennent des ***données de santé en raison de leur destination, c'est-à-dire de l'utilisation qui en est faite au plan médical***.

A noter : la loi ne s'applique pas aux traitements qui comporteraient des données de santé à l'usage exclusif de la personne. A titre d'exemple, la loi ne s'applique pas aux applications mobiles en santé qui proposent dans leurs fonctionnalités, la collecte, l'enregistrement ou la conservation de données à condition que ces opérations s'effectuent localement sur un ordinateur ou une tablette, sans connexion extérieure et à des fins exclusivement personnelles.

N'entrent pas dans la notion de données de santé celles à partir desquelles aucune conséquence ne peut être tirée au regard de l'état de santé de la personne concernée (ex : une application collectant un nombre de pas au cours d'une promenade sans croisement de ces données avec d'autres).

Cette notion recouvre non seulement l'ensemble des données collectées et produites dans le cadre du parcours de soins mais aussi celles qui, détenues par d'autres acteurs (développeurs d'application par exemple), constituent une information sur l'état de santé de la personne.

2. Régime juridique des données de santé

Une fois la qualification de données de santé retenue, un régime juridique particulier justifié par la sensibilité des données s'applique.

Différentes législations sont susceptibles de s'appliquer, aux côtés des exigences du règlement RGPD, en fonction des hypothèses concernées (cette liste n'est pas exhaustive) :

- loi Informatique et Libertés n°78-17 du 6 janvier 1978 (art. 8 et chapitre IX) ;
- dispositions sur le secret médical (art. L1110-4 du CSP) ;
- dispositions relatives aux référentiels de sécurité et d'interopérabilité des données de santé (art. L1110-4-1 du CSP) ;
- dispositions sur l'hébergement des données de santé (art. L1111-8 et R1111-8-8 et s. du CSP) ;
- dispositions sur la mise à disposition des données de santé (art. L1460-1 et s. du CSP) ;
- interdiction de procéder à une cession ou à une exploitation commerciale des données de santé (art. L1111-8 du CSP, art. L4113-7 du CSP)…

L'usage des dossiers « patients » doit respecter **les principes fondamentaux de la protection des données personnelles** : article 5 RGPD et article 6 (Chapitre II : « Conditions de licéité des traitements de données à caractère personnel ») de la loi Informatique et Libertés.

2.1. Les dossiers papiers ou logiciel médico-administratif doivent répondre à des finalités déterminées, explicites et légitimes.

Les informations collectées dans les dossiers « patients » sont utilisées pour exercer l'activité de prévention, de diagnostic et de soins. Elles répondent aux besoins de la prise en charge des patients. Il s'agit notamment de permettre :

• la gestion des rendez-vous ;

• la gestion des dossiers médicaux ;

• l'édition des ordonnances ;

• l'envoi de courriers aux confrères ;

• l'établissement et la télétransmission des feuilles de soins.

Toute autre utilisation des informations collectée à l'occasion de la prise en charge doit être réalisée avec précaution. En particulier, toute utilisation personnelle ou commerciale des dossiers des patients est naturellement prohibée.

2.2. Les données collectées et reportées dans les dossiers des patients, doivent être adéquates, pertinentes et limitées à ce qui est nécessaire à la prise en charge du patient au titre des activités de prévention, de diagnostic et de soins.

Toutes les informations que le patient a pu révéler, dans le cadre des échanges avec le praticien médical, ne doivent pas nécessairement intégrer son dossier. Seules celles qui sont utiles au suivi du patient peuvent être enregistrées et conservées.

Dans ce cadre, la CNIL estime légitime de collecter certaines catégories de données personnelles, notamment :

• les données d'identification : nom, prénom, date de naissance, adresse, numéro de téléphone ;

• le numéro de sécurité sociale : uniquement pour l'édition des feuilles de soins et la télétransmission aux caisses d'assurance maladie ;

• selon les contextes, la situation familiale : situation matrimoniale, nombre d'enfants ;

• selon les contextes, la vie professionnelle : profession, conditions de travail ;

• la santé : historique médical, historique des soins, diagnostics médicaux, traitements prescrits, nature des actes effectués, résultats d'examens de biologie médicale et tout élément de nature à caractériser la santé du patient et considéré comme pertinent par le médecin ;

• informations relatives aux habitudes de vie : si collectées avec l'accord du patient et dans la stricte mesure où elles sont nécessaires au diagnostic et aux soins.

• autres informations : si nécessaires au diagnostic médical (ex : origine ethnique ayant une influence particulière sur une pathologie déterminée ou un traitement médical, habitudes alimentaires, etc.).

En revanche, toute information qui serait sans lien avec l'objet de la consultation du patient ou qui ne serait pas indispensable au diagnostic ou à la délivrance des soins doit être exclue. Par exemple, des informations sur la vie privée du patient qui ne sont pas médicalement nécessaires (ex : religion du patient, orientation sexuelle, etc.).

2.3. Les données collectées sur les patients doivent être conservées pour une durée qui n'excède pas la durée nécessaire à l'utilisation qui en est faite.

Il est important de prendre en compte les délais de prescription des éventuelles actions en responsabilité et toutes autres dispositions particulières.

C'est l'article R1112-7 du code de la santé publique qui prévoit les délais de conservation des dossiers médicaux au sein des établissements de santé[1] :

• 20 ans à compter de la date de la dernière consultation du patient ;

• si le patient est mineur et que ce délai de 20 ans expire avant son 28ème anniversaire, la conservation des informations le concernant doit être prolongée jusqu'à cette date ;

• dans tous les cas, si le patient décède moins de 10 ans après sa dernière consultation, les informations le concernant doivent être conservées pendant 10 ans à compter de la date du décès ;

• en cas d'action tendant à mettre en cause la responsabilité du médecin, ces délais de conservation sont suspendus.

Les doubles des feuilles de soins doivent être conservés 3 mois.

2.4. Information nécessaire des patients de l'existence des dossiers médicaux et de leurs droits à cet égard[2].

Cette information peut se faire par voie d'affichage, dans la salle d'attente, ou par la remise d'un document spécifique (ex : dépliant remis au patient ou mis à disposition dans la salle d'attente).

L'information doit comporter impérativement les éléments suivants :

• le nom et les coordonnées du médecin traitant ;

• les finalités et la base juridique du traitement, y compris les finalités ultérieures ;

• les destinataires des données ;

• la durée de conservation ;

• les droits de la personne : accès, rectification, à certaines conditions effacement, limitation, opposition, introduction d'une réclamation auprès de la CNIL ;

• caractère obligatoire des données fournies et des conséquences éventuelles d'un défaut de réponse ;

• le cas échéant, utilisation ultérieure des données pour une finalité autre que celle pour laquelle les données ont été collectées (ex : si un médecin souhaite utiliser ultérieurement les données à des fins de recherche).

Les patients disposent de droits. Ils peuvent[3] :

• accéder aux données les concernant ;

• rectifier ces données en cas d'erreur ;

• s'opposer au traitement pour des raisons tenant à leur situation particulière ;

• effacer les données, dans certaines situations particulières (par exemple, dossier patient conservé trop longtemps, données non adéquates, etc.).

[1] En l'absence de dispositions spécifiques portant sur la durée de conservation des dossiers des professionnels exerçant en libéral, le Conseil national de l'Ordre des médecins préconise de s'aligner sur ces délais
[2] Article 13 RGPD
[3] Art. 15 à 23 RGPD et art. 38 à 43 ter loi Informatique et libertés

Chaque demande portant sur ces droits doit être examinée dans un délai raisonnable. Dans le cas d'une demande d'accès au dossier « patient », le délai est obligatoirement de 8 jours, porté à 2 mois lorsque les informations datent de plus de 5 ans[4].

Pour tout savoir sur l'exercice des droits des patients, il existe une fiche thématique « Les droits pour maîtriser vos données personnels »[5].

2.5. Prendre toutes les précautions utiles pour empêcher que des tiers non autorisés aient accès aux données de santé.

Seules certaines personnes sont autorisées, au regard de leurs missions et en vertu de dispositions législatives les y habilitant, à accéder aux données de santé des patients (ex : équipe de soins d'un établissement de santé intervenant dans la prise en charge sanitaire du patient, etc.).

En pratique, il sera important de veiller au respect des règles relatives à l'échange et au partage de données entre professionnels (sur ce point, voir la fiche pratique du CNOM « Echange et partage d'informations », déc. 2016[6]).

Ainsi, tout professionnel de santé intervenant dans la prise en charge du patient peut avoir un accès spécifique aux seules informations nécessaires à cette prise en charge, ou si cela n'est pas possible, le médecin peut envoyer les informations nécessaires directement à ces professionnels.

Quant au personnel administratif, il ne peut avoir un accès global aux dossiers des patients. Certaines données (nom, prénom, code acte, NIR, date de la consultation) sont adressées aux organismes d'assurance maladie via la télétransmission ou les feuilles de soins.

En cas de recours à un prestataire de service pour assurer la maintenance du logiciel gérant les dossiers des patients, celui-ci n'est pas censé accéder aux données de santé à caractère personnel. Il a un rôle purement technique. En principe, les données doivent être chiffrées afin de permettre au technicien d'assurer ses missions sans pouvoir lire ces données.

Si le stockage des dossiers « patients » est confié à un prestataire chargé d'en assurer la conservation, dans des serveurs à distance, celui-ci doit être hébergeur agréé ou certifié pour l'hébergement, le stockage, la conservation de données de santé conformément aux dispositions de l'article L. 1111-8 du code de la santé publique.

En toute hypothèse, dès que les services d'un prestataire (société de maintenance, hébergeur de données de santé agréé ou certifié) sont sollicités, celui-ci agit pour le compte de l'hôpital/ médecin. Il faut donc formaliser la relation en passant un contrat de sous-traitance qui mentionne que, le prestataire, en tant que sous-traitant[7] :

• ne traite les données à caractère personnel que sur l'instruction de l'hôpital/ médecin ;

• veille à la signature d'engagements de confidentialité par le personnel ;

• prend toutes les mesures de sécurité requises ;

• ne recrute pas de sous-traitant sans l'autorisation écrite préalable de son commanditaire ;

• coopère avec son commanditaire pour le respect de ses obligations en tant que responsable de traitement notamment lorsque des patients ont des demandes concernant leurs données ;

• supprime ou renvoie à l'hôpital/ médecin l'ensemble des données à caractère personnel à l'issue des prestations ;

• collabore dans le cadre d'audits.

[4] Art. L.1111-7 du Code de la santé publique
[5] https://www.cnil.fr/fr/les-droits-pour-maitriser-vos-donnees-personnelles
[6] https://www.conseilnational.medecin.fr/sites/default/files/cnomechangepartageinfos_0.pdf
[7] Art. 28 RGPD

2.6. Prendre toutes les mesures nécessaires pour sécuriser et protéger les données personnelles traitées[8].

Respecter les mesures prévues par les référentiels de sécurité et d'interopérabilité des données de santé : art. L1110-4-1 du code de la santé publique.

Pour une information détaillée, vous pouvez consulter le guide de la sécurité des données personnelles publié par la CNIL[9] et le mémento relatif à la sécurité informatique pour les professionnels de santé en exercice libéral publié par l'Agence des systèmes d'information partagés de santé (ASIP Santé)[10].

En ce qui concerne la sécurisation du système informatique, tout professionnel qui manie des données personnelles des patients doit respecter les grands principes suivants :

• utilisation d'un mot de passe conforme aux recommandations de la CNIL, 12 caractères (chiffres, lettres majuscules et minuscules, caractères spéciaux), renouvelé régulièrement ;

• verrouillage de la session informatique automatiquement après maximum 30 minutes d'inactivité ;

• antivirus à jour, pare-feu, application systématique des correctifs de sécurité du système informatique et des logiciels ;

• sauvegardes régulières des données (sauvegarde au minimum hebdomadaire, avec conservation des sauvegardes mensuelles sur 12 mois glissants) et leur conservation dans un lieu différent que le cabinet médical ;

• chiffrement des données avec un logiciel adapté ;

• absence ou minimisation des connexions d'appareils non professionnels sur le réseau ;

• authentification via la Carte de professionnel de santé (CPS) ou tout moyen alternatif d'authentification forte.

La CPS doit rester strictement personnelle. En aucun cas, les codes secrets ne doivent pas être communiqués au personnel (ex : secrétaire médicale). Il est possible de mettre en place une authentification forte pour le personnel au moyen d'un mot de passe à usage unique par exemple (identifiant, mot de passe et envoi d'un code à chaque connexion) ou au moyen d'une Carte de personnel d'établissement (CPE) à demander à votre Caisse primaire d'assurance maladie[11].

Si le logiciel gérant les dossiers « patients » est accessible à distance et est hébergé par un prestataire (un éditeur de logiciel en général), le praticien doit s'assurer que ce tiers ou son sous-traitant est agréé ou certifié pour l'hébergement des données de santé conformément à l'article L1111-8 du code de la santé publique.

Si les dossiers sont conservés sous format papier, il faut également s'assurer de leur sécurité (locaux sécurisés, armoire contenant les dossiers fermée à clé, etc.).

3. Obligations supplémentaires de l'établissement de santé

3.1. Tenir un registre des activités de traitement

Chaque établissement doit tenir un registre des activités de traitement recensant tous les traitements mis en œuvre dans le cadre de l'activité, notamment : un registre pour le suivi des patients (les dossiers « patients »), un registre résultant de l'utilisation de la messagerie électronique sécurisée[12] ou d'un dispositif de télémédecine, etc. Il permet de disposer d'une vue d'ensemble de ce que l'établissement fait avec les données personnelles.

[8] Art. 32 RGPD et art. 34 loi Informatique et libertés
[9] https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle.pdf)
[10] http://esante.gouv.fr/sites/default/files/Memento_Securite.pdf
[11] http://esante.gouv.fr/services/espace-cps/cartes-professionnelles-de-sante
[12] La CNIL travaille actuellement à la mise à jour du référentiel consacré à la messagerie électronique sécurisée.

Le registre est prévu par l'article 30 du RGPD. Il participe à la documentation de la conformité.

Document de recensement et d'analyse, il doit refléter la réalité des traitements de données personnelles et permet d'identifier précisément :

- les parties prenantes (représentant, sous-traitants, co-responsables, etc.) qui interviennent dans le traitement des données,
- les catégories de données traitées,
- à quoi servent ces données, qui accède aux données et à qui elles sont communiquées,
- combien de temps elles sont conservées,
- comment elles sont sécurisées.

Au-delà de la réponse à l'obligation prévue par l'article 30 du RGPD, le registre est un outil de pilotage et de démonstration de la conformité au RGPD. Il permet de documenter les traitements de données et de se poser les bonnes questions : a-t-on vraiment besoin de cette donnée dans le cadre du traitement médical ? Est-il pertinent de conserver toutes les données aussi longtemps ? Les données sont-elles suffisamment protégées ? Etc.

Sa création et sa mise à jour sont ainsi l'occasion d'identifier et de hiérarchiser les risques au regard du RGPD. Cette étape essentielle permettra d'en déduire un plan d'action de mise en conformité des traitements aux règles de protection des données.

L'article 30 du RGPD prévoit des obligations spécifiques pour le registre du responsable de traitement de données personnelles et pour le registre du sous-traitant.

Le registre du responsable de traitement doit recenser l'ensemble des traitements mis en œuvre par l'établissement de santé.

En pratique, une fiche de registre doit donc être établie pour chacune de ces activités.

Ce registre doit comporter le nom et les coordonnées de l'établissement ainsi que, le cas échéant, de son représentant, si l'établissement n'est pas établi dans l'Union européenne, et du délégué à la protection des données lorsqu'il existe.

En outre, pour chaque activité de traitement, la fiche de registre doit comporter au moins les éléments suivants :

1. le cas échéant, le nom et les coordonnées du responsable conjoint du traitement mis en œuvre ;
2. les finalités du traitement, l'objectif en vue duquel ces données sont collectées ;
3. les catégories de personnes concernées (client, prospect, employé, etc.) ;
4. les catégories de données personnelles (exemples : identité, situation familiale, économique ou financière, données bancaires, données de connexion, donnés de localisation, etc.) ;
5. les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, y compris les sous-traitants éventuels ;
6. les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale et, dans certains cas très particuliers, les garanties prévues pour ces transferts ;
7. les délais prévus pour l'effacement des différentes catégories de données, c'est-à-dire la durée de conservation, ou à défaut, les critères permettant de la déterminer ;
8. dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles mises en œuvre.

Le RGPD impose que le registre se présente sous une forme écrite. Le format du registre est libre et peut être constitué au format papier ou électronique.

La CNIL propose un modèle de base répondant aux conditions posées par le RGPD.

3.2. Désignation d'un délégué à la protection des données (DPO)

Les hôpitaux et organismes qui traitent des données de santé à grande échelle (ex : exercice au sein d'un réseau de professionnels, dossiers partagés entre plusieurs professionnels de santé, etc.), doivent soit désigner un délégué à la protection des données (DPO) en interne, soit solliciter les services d'un DPO externe (consultants, cabinets d'avocats, etc.). Une expertise juridique et technique et une bonne connaissance de la structure qui le sollicite sont requises.

Le RGPD déclare que le délégué doit être « *associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel* ». Il est l'interlocuteur privilégié des personnes souhaitant poser des questions relatives au traitement de leurs données à caractère personnel et à l'exercice des droits que leur confère le RGPD.
Sa tâche est « *d'informer et de conseiller le responsable du traitement ou le sous-traitant ainsi que les employés qui procèdent au traitement sur [leurs] obligations* », de « *contrôler le respect* » du RGPD et de tous les autres textes liés à la protection des données (que ce le droit de l'Union ou celui des États membres), de coopérer avec la Cnil et de dispenser des conseils, sur demande.

La désignation d'un délégué est obligatoire dans trois cas de figure :

- si le traitement est réalisé par une entité publique ;
- si la structure a une activité l'amenant « à réaliser un suivi régulier et systématique des personnes à grande échelle » (P.ex. au sein d'un hôpital) ;
- si la structure effectue un traitement impliquant des données sensibles ou liées à des condamnations pénales et infractions.

4. Sanctions en cas de non-respect des règles

Les professionnels de santé qui ne respectent pas ces obligations, peuvent faire l'objet d'une sanction administrative de la CNIL, voire d'une sanction pénale.

La CNIL peut prononcer, en fonction de la gravité du non-respect de la réglementation, des amendes administratives allant jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires annuel. Quant aux peines pénales maximales, elles sont, pour une personne physique, de 5 ans d'emprisonnement et de 300.000 d'euros d'amende et, pour une personne morale, de 1,5 millions d'euros d'amende.

Il est donc impératif de se mettre en conformité avec la réglementation et de documenter cette conformité (registre des activités de traitement, traçabilité des violations de données, engagements de confidentialité du personnel, etc.). Si la CNIL constate un défaut de conformité, elle peut mettre en demeure de s'y conformer ; ce qui laisse une chance aux professionnels d'adopter les mesures nécessaires pour éviter une sanction.

La CNIL a indiqué que les contrôles de conformité qu'elle pourrait réaliser seront, dans les premiers mois d'application du RGPD, à visée pédagogique. L'essentiel est de pouvoir démontrer que vous êtes engagé dans une démarche de mise en conformité.

Partie 2. Cadre juridique de la communication des données médicales en Italie à la suite de l'entrée en vigueur du règlement européen sur la protection des données personnelles (RGPD)

1. Introduction

La protection des données à caractère personnel a une place très importante pour la protection de la santé humaine, surtout si on se concentre sur les dynamiques transfrontalières. Ce troisième livrable cherche à fournir un état des lieux de la protection des données à caractère personnel en ce qui concerne surtout la mobilité sanitaire transfrontalière des patients entre la *Regione Piemonte* et l'Hôpital de Briançon côté français. Le livrable vise aussi à expliciter comment l'Italie a adapté sa législation afin de protéger les données des patients, notamment à la suite du règlement européen RGPD.

Tout d'abord il faut préciser le champ de la recherche. A la différence de l'analyse territoriale – qui a notamment examiné les spécificités du territoire sur lequel l'ASL TO 3 opère du côté italien et l'hôpital de Briançon sur le versant français – et de l'analyse du cadre juridique des transports sanitaires qui s'est référée au même périmètre géographique, la protection des données à caractère personnel s'étend, comme on le verra, sur tout le territoire de l'Union européenne et, pour certains aspects, aussi sur celui de pays tiers. Donc, c'est la protection des données dans sa généralité qui constitue le point de départ de notre analyse.

Cadre juridique de références :

Il faudra attacher notre attention au droit de l'Union européenne et non pas au strict droit italien. L'adoption du règlement 2016/679[13] (ci d'après : règlement RGPD) a, en premier lieu, abrogé la vieille directive 95/46[14] qui avait permis en Italie l'adoption du *decreto legislativo*[15] établissant le *codice della privacy*. A la suite de l'entrée en vigueur du règlement RGPD le 25 mai 2018 (article 99 du règlement RGPD), l'Italie a dû amender le *codice della privacy* ; cela a été fait par le *decreto legislativo* 101/2018[16]. Donc, aujourd'hui, **toute la législation sur la protection des données à caractère personnel en Italie est contenue dans le *codice della privacy,* issue de la nouvelle formulation de septembre 2018 et du règlement RGPD.**

Cela étant, la protection offerte par le règlement RGPD doit être, en tout cas, coordonnée avec les exigences de circulation de donnée génétiques, biométriques et concernant la santé aussi bien que la circulation des patients. Ces exigences relèvent surtout du domaine de **la mobilité transfrontalière des patients selon la directive 2011/24**[17].

[13] 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) JO L 119 du 4.5.2016, p. 1–88.

[14] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données JO L 281 du 23.11.1995, p. 31–50.

[15] Decreto legislativo 30 giugno 2003, n.196 recante il "Codice in materia di protezione dei dati personali" (in S.O n. 123 alla G.U. 29 luglio 2003, n. 174.

[16] Decreto legislativo 10 agosto 2018, n. 101 Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonche' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). (18G00129) (GU Serie Generale n.205 del 04-09-2018).

[17] Directive 2011/24/UE du Parlement européen et du Conseil du 9 mars 2011 relative à l'application des droits des patients en matière de soins de santé transfrontaliers JO L 88 du 4.4.2011, p. 45–65.

A l'égard du droit applicable, il faut rappeler que selon l'article 288 du Traité sur le fonctionnement de l'Union européenne (TFEU) « *Le règlement a une portée générale. Il est obligatoire dans tous ses éléments et il est directement applicable dans tout État membre* ». La Cour de justice de l'Union européenne a, à plusieurs occasions, remarqué qu'un règlement ne nécessite pas d'être transposé dans les ordres juridiques nationaux. Cette précision est très importante pour notre objet d'étude et pour le présent troisième livrable, car elle permet de se référer directement au règlement RGDP sans considérer – sauf cas exceptionnels, comme on le verra – le *codice della privacy*.

De plus, la protection des droits à caractère personnelles est l'un des droits fondamentaux reconnus par la Charte des droits fondamentaux de l'Union européenne. Et la Charte se pose comme un socle contraignant tant pour l'adoption des nouveaux instruments législatifs par les institutions de l'Union que dans la phase éventuelle de transpositions de ceux-ci par les États membres.

Compte tenu de ces observations, la protection des données à caractère personnel, génétiques, biométriques et concernant la santé et leur circulation liée à la mobilité des patients qui franchissent la frontière franco-italienne pour se rendre à Briançon (ou ailleurs en France) doit être évalué en se référant au règlement RGPD et à la Charte des droits fondamentaux de l'Union européenne.

Le droit italien a presque disparu, sauf pour le rôle de *garante per la protezione dei dati personali* (ci d'après : *garante privacy*). Un avis a récemment été rendu, contenant des lignes directrices en ce qui concerne la protection de la santé en Italie. De plus, l'absence d'un code de la santé ne permet pas d'avoir de règles spécifique en la matière mais implique qu'on doit se référer directement au règlement RGPD. Pour cette raison, en Italie, le règlement RGPD est la seule source normative de référence. Aucun pouvoir discrétionnaire n'est laissé aux Régions, ni aux *aziende sanitarie locali (ASL*). En effet, pour eux, il s'agit simplement de mettre à jour leurs pratiques, leur formulaires, leurs fiches selon les indications du règlement RGPD.

2. Le règlement RGPD et les droits fondamentaux dans le domaine sanitaire

Comme on vient de le voir, les normes régissant le traitement des données sanitaires et médicales sont contenues dans le seul règlement RGPD. En Italie, il n'y pas d'autres instruments internes à prendre en considération.

Le règlement RGPD est un acte législatif très long : 88 pages pour 99 articles ; il est donc impossible de l'analyser en quelques pages. Le mot santé est répété à de nombreuses reprises (63 fois) pour signaler son importance dans le cadre général de la protection des données personnelles. En fait, les règles relatives traitement des données à caractère personnel sont inspirées par le fait que la Charte des droits fondamentaux de l'Union européenne affirme explicitement le droit au respect de la vie privée et familiale et des communications (article 7) aussi bien que la protection des données à caractère personnel (article 8). Le paragraphe 2 de l'article 8 de la Charte ajoute que « *Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi* ». Cela est prévu aussi par l'article 16 du Traité sur le fonctionnement de l'Union européenne (TFUE) qui constitue la base juridique du règlement RGPD. Il s'agit là des grands axes du droit à la protection des données à caractère personnel.

Par ailleurs, le 35ème considérant du règlement RGPD affirme que « *Les données à caractère personnel concernant la santé devraient comprendre l'ensemble des données se rapportant à l'état de santé d'une personne concernée qui révèlent des informations sur l'état de santé physique ou mentale passé, présent ou futur de la personne concernée* ». L'article 1er du RGDP affirme aussi le principe de la liberté de circulation des données ; il s'agit là d'un aspect très important pour la mobilité transfrontalière des patients. Et puisque la mobilité des patients entre l'Italie et la France relève du droit de l'Union européenne, le règlement RGPD est la dernière référence en date applicable à leurs données (articles 2-3).

Le premier concept est le consentement, « de la personne concernée, toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement » (article 4, paragraphe 11).

L'article 4, paragraphe 13, indique que les « *« données génétiques »* [sont] *les données à caractère personnel relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique qui donnent des informations uniques sur la physiologie ou l'état de santé de cette personne physique et qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne physique en question* ». L'article 4, paragraphe 15, indique que les « *« données concernant la santé »* [sont] *les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne* ».

Dans le cas de la mobilité entre l'ASL TO 3 et l'hôpital de Briançon, elle relève aussi de la notion de l'article 4, paragraphe 23, de « *« traitement transfrontalier »*, [à savoir] *a) un traitement de données à caractère personnel qui a lieu dans l'Union dans le cadre des activités d'établissements dans plusieurs États membres d'un responsable du traitement ou d'un sous-traitant lorsque le responsable du traitement ou le sous-traitant est établi dans plusieurs États membres* ».

L'article 9 introduit des limitations au traitement « *des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits », sauf si « le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique, dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement* ».

De plus, la lettre h du même article affirme que d'autres exceptions sont admissibles si « *le traitement est nécessaire aux fins de la médecine préventive ou de la médecine du travail, de l'appréciation de la capacité de travail du travailleur, de diagnostics médicaux, de la prise en charge sanitaire ou sociale, ou de la gestion des systèmes et des services de soins de santé ou de protection sociale sur la base du droit de l'Union, du droit d'un État membre ou en vertu d'un contrat conclu avec un professionnel de la santé et soumis aux conditions et garanties visées au paragraphe 3* ».

Ensuite, la lettre i de l'article 9 prévoit que *« le traitement est nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique, tels que la protection contre les menaces transfrontalières graves pesant sur la santé, ou aux fins de garantir des normes élevées de qualité et de sécurité des soins de santé et des médicaments ou des dispositifs médicaux, sur la base du droit de l'Union ou du droit de l'État membre qui prévoit des mesures appropriées et spécifiques pour la sauvegarde des droits et libertés de la personne concernée, notamment le secret professionnel* ».

Encore, selon le paragraphe 3 « *Les données à caractère personnel visées au paragraphe 1 peuvent faire l'objet d'un traitement aux fins prévues au paragraphe 2, point h), si ces données sont traitées par un professionnel de la santé soumis à une obligation de secret professionnel conformément au droit de l'Union, au droit d'un État membre ou aux règles arrêtées par les organismes nationaux compétents, ou sous sa responsabilité, ou par une autre personne également soumise à une obligation de secret conformément au droit de l'Union ou au droit d'un État membre ou aux règles arrêtées par les organismes nationaux compétents* ».

En conclusion, le paragraphe 4 de l'article 9 stipule que « *Les États membres peuvent maintenir ou introduire des conditions supplémentaires, y compris des limitations, en ce qui concerne le traitement des données génétiques, des données biométriques ou des données concernant la santé* ». Apparemment, l'Italie n'a pas établi de telles règles spécifiques supplémentaires.

En résumé, le régime de la protection des données personnelles est complexe et très détaillé :

Les données à caractère personnel, qui inclut aussi la catégorie spéciale des données de santé, constituent un droit fondamental de l'homme et doivent être protégées en tant que telles ;

Le traitement rencontre des limités liées à la nature des données, surtout en ce qui concerne leur circulation ;

Le règlement RGPD ne laisse aucune marge de manœuvre aux États membres de l'Union européenne.

En conclusion, le règlement RGDP a occupé tout le champ de la protection des données d'un particulier, en imposant aussi des obligations aux établissements publics et privés qui les gèrent. Il fournit les principes généraux régissant la protection des données de la santé, qui doivent être coordonnés (voir paragraphe 4 de ce livrable) avec la directive sur la mobilité transfrontalière des patients 2011/24.

3. Le règlement RGPD en Italie

Les règles découlant du *decreto legislativo* 101/2018 sont le miroir du règlement RGPD car toutes les normes italiennes sont issues de celui-ci. Il n'y a pas de dispositions spécifiquement applicables au domaine sanitaire car, comme on l'a déjà vu, il relève du règlement RGPD.

Néanmoins, il est important de présenter un avis rendu par le *Garante della privacy*[18] concernant la protection des données médicales :

-*En première lieu*, il y a des dérogations à l'interdiction générale de traiter les données de santé mais cette interdiction doit être conciliée avec la présence des exigences liées à la santé publique, c'est-à-dire la protection des graves menaces ayant un caractère transfrontalière ou le maintien de paramètres de niveau élevé pour garantir le respect du droit à la santé dans les États membres.

-*En deuxième lieu*, il est possible d'identifier d'autres exceptions dans le domaine de la médecine préventive, l'assistance sanitaire ou le bon déroulement d'une thérapie. Si le bon déroulement d'une thérapie l'exige, un professionnel de santé, soumis au secret professionnel, n'a pas d'obligation de requérir (et obtenir) le consentement éclairé d'un patient et cela qu'il travaille dans un hôpital ou comme professionnel privé. Les traitements sanitaires non obligatoires, d'autre part, requièrent toujours le consentement du patient.

Par exemple, le *Garante della privacy* a identifié des obligations complémentaires en ce qui concerne l'utilisation des applications téléphoniques médicales, la fidélisation des patients de la part des pharmacies, les traitements opérés par des personnes morales aussi bien ceux qui concernent le dossier sanitaire électronique[19].

Le *Garante* affirme aussi que les normes du consentement dans le cas du dossier sanitaire électronique doivent être mises à jour selon les dispositions, probablement plus protectrices et uniformes par rapport à celles du *codice della privacy*, du règlement RGPD.

En ce qui concerne les informations à transmettre aux patients, le *Garante* souligne qu'il faudra simplement mettre à jour les formulaires car les lignes directrices, surtout pour la clarté et la transparence, sont encore valides. Le *Garante* suggère aussi aux *ASL* d'utiliser un principe de progressivité pour informer, précisément d'une manière progressive, les patients en fonction les traitements nécessaires. De plus, il faudra fournir aussi des indications sur la durée de la conservation des données.

Ensuite, chaque hôpital ou chaque *ASL* doit créer la fonction de responsable du traitement. Il est en tout cas permis d'identifier une seule personne compétente (*ASL* et hôpitaux de son ressort). En revanche, le professionnel de santé qui opère en régime privé n'a pas cette obligation.

En conclusion, en Italie le régime de protection des données personnelles a été complètement harmonisé et parachevé : il n'y a aucun espace pour des interventions complémentaires, ni au niveau

[18] Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario – 7 marzo 2019, registro dei provvedimenti n. 55 del 7 marzo 2019.

[19] Testo del decreto-legge 18 ottobre 2012, n. 179 (pubblicato nel supplemento ordinario n. 194/L alla Gazzetta Ufficiale 19 ottobre 2012, n. 245), coordinato con la legge di conversione 17 dicembre 2012, n. 221 (in questo stesso supplemento ordinario alla pag. 1), recante: «Ulteriori misure urgenti per la crescita del Paese.». (12A13277) (GU Serie Generale n.294 del 18-12-2012 - Suppl. Ordinario n. 208).

central ni au niveau régional. Aux *ASL* il ne reste plus qu'à mettre à jour leurs pratiques conformément au règlement RGPD et de les mettre en œuvre là où elles manquaient.

C'est exactement pour cette raison que l'ASL TO 3 a dû publier une note pour expliquer ses stratégies de protection des données et elle est encore plus explicative que la base normative, c'est-à-dire le règlement RGPD. Dans les 4 pages de *l'informazione sul trattamento dei dati personali,* l'ASL TO 3 explique à ses patients tous ce qu'il faut savoir en la matière. Encore, l'ASL TO 3 a lancé un avis de marché pour identifier un délégué à la protection des données qui a été embauché d'une entreprise tierce[20]. En effectuant ces démarches, l'ASL TO 3 a accompli ses obligations découlant du règlement RGPD.

Pour toutes ces raisons il est encore plus important d'insister sur le fait qu'en Italie le domaine de la protection de donnés découle entièrement du règlement RGPD. Le *codice della privacy* n'est que sa copie conforme ; cela étant, en pratique son rôle a été substitué par le règlement RGPD lui-même. En effet, le *codice della pricacy* avait quelque utilité pour la transposition de la directive 95/46 mais, eu égard au règlement, il est désormais 'répétitif'.

La dernière partie à examiner concerne les relations entre le règlement RGPD et la mobilité transfrontalière des patients, un aspect très spécifique et surtout essentiel dans les territoires objets de notre étude qui relève aussi du champ d'application de la directive sur la mobilité transfrontalière des patients 2011/24.

4. La libre circulation des données médicales

La directive 2011/24 codifie la jurisprudence de la Cour de justice en matière de mobilité des patients dans les États membres de l'Union européenne. On l'avait déjà mentionné à propos de l'analyse concernant le transport pour affirmer qu'elle n'a pas un rôle direct dans ce domaine.

Le considérant 25 de la directive 2011/24 affirme que la notion de données doit être tirée de la directive 95/46, ce qui se traduit aujourd'hui dans le régime introduit par le règlement RGPD. Ensuite, il est répété que la protection des données constitue un droit fondamental de l'homme et que les données doivent circuler librement sur le territoire de l'Union. Plus précisément, selon l'article 3, lettre m, de la directive 2011/24, il s'agit des données « figurant dans leurs dossiers médicaux contenant des informations telles que des diagnostics, des résultats d'examens, des avis de médecins traitants et tout traitement ou intervention entrepris ». Par conséquent, les patients qui ont bénéficié d'un traitement médical transfrontalier, selon le principe de la continuité des soins, ont le droit d'avoir accès à leur dossier médical. Ensuite, parmi les obligations de l'Etat membre d'affiliation – c'est à dire l'Etat où un patient est affilié à un régime de sécurité sociale et/ ou d'assurance maladie – il y a celle de mettre à disposition du patient son dossier.

Enfin, l'article 14 de la directive sur la mobilité transfrontalière des patients 2011/24 est consacré à la santé en ligne, établissant qu'il faut mettre en commun, partager les dossiers qui contiennent les données des patients entre l'État d'affiliation et celui de soin aussi bien que de mettre en œuvre des systèmes numériques pour en permettre l'utilisation, l'identification, l'authentification et la transférabilité.

Ces notions sont importantes pour comprendre des aspects spécifiques de la mobilité des patients, surtout dans des zones comme celles que l'analyse territoriale a décrites, où il y a des entraves géographiques, sociales et économiques qui peuvent empêcher la mobilité des personnes. Il en découle que la mise à jour et la mise en œuvre des systèmes informatiques pour garantir la continuité des soins sont cruciales pour garantir à la fois le droit à la santé, et la protection des données personnelles.

Le *fascicolo sanitario elettronico* créé par l'article 12 du *decreto legge* 179/2012 est le dossier électronique qui recueille les données et les documents dérivants de l'événement clinique d'un patient. Il est géré et généré par les régions italiennes et doit respecter la législation en matière de protection des données. Il sert aussi à évaluer la qualité des soins fournis.

[20] Determinazione n. 95 del 23 luglio 2018.

Selon l'article 3 bis du *decreto legge* 179/2012, le patient a le droit de décider des données à ne pas y inclure.

Ensuite, les médecines ont l'obligation de maintenir le secret professionnel aussi bien que d'informer les patients sur les modalités de traitement de leurs données.

L'article 13 du *decreto legge* 179/2012 prévoit la création de la *cartella clinica digitale* pour remplacer les prescriptions médicales papier par des formats électroniques, en prévoyant l'obligation pour les médecines de l'utiliser pour toutes les prescriptions. Ces dispositions législatives s'insèrent dans l'idée de la dématérialisation des données de santé dans la mesure où il sera plus facile de les transmettre et partager entre les institutions concernées, surtout lorsqu'il s'agit d'un traitement transfrontalier.

Le système repose entièrement sur deux socles, le règlement RGPD et le consentement du patient. En effet, il faut rappeler que le règlement RGPD a pour but la protection des données mais aussi leur libre circulation. Par conséquent, la législation italienne semble avoir correctement mis en œuvre l'acquis de l'Union européenne pour faciliter la libre circulation des données comme une partie très importante de la mobilité sanitaire transfrontalière qui renforce également le droit à la santé.

Conclusion : un régime uniforme issu du règlement RGPD n'excluant pas les divergences liées aux cadres et règles complémentaires

Le règlement RGPD, en tant qu'acte législatif de l'Union européenne directement applicable dans les systèmes juridiques des États membres, a occupé tout le champ matériel, personnel et territorial de la protection des données en France et en Italie dont la législation en la matière n'est que le reflet fidèle du règlement RGPD.

Néanmoins, une première source de divergences pourraient constituer les règles internes qui viennent compléter le champ du RGPD.

En Italie, seules quelques recommandations de la *Garante della privacy* viennent simplement expliciter le dispositif. En revanche, les très nombreuses règles françaises préexistantes et complémentaires au RGPD en fonction des hypothèses concrètes qui se présentent (par exemple, les dispositions sur la communication des données à travers la loi Informatique et Libertés, les dispositions sur le secret médical, etc.) pourraient faire défaut en Italie, voire entrer en contradiction avec l'ordre juridique interne italien.

Une autre source de différences potentielles entre la France et l'Italie pourrait constituer le fait qu'en France la législation sanitaire est regroupée dans un corpus de règles nationales applicables sur tout le territoire. Tandis que, comme pour les transports sanitaires (cf. livrable 2), en Italie ce sont les régions qui détiennent les pouvoirs règlementaires en la matière.

Cela étant, même si la compétence régionale italienne peut créer des problèmes de coordination et une certaine inégalité sur certains aspects spécifiques secondaires comme le coût du transport et du ticket de remboursement, cela n'est pas permis lorsqu'un droit fondamental comme le droit à la protection des données à caractère personnel est en jeu.

Ces conclusions sont renforcées par la constatation que la mobilité des patients entre le territoire de l'ASL TO 3 et l'hôpital de Briançon relèvent, en général, de la libre prestation de services de l'article 56

TFEU et ne peut pas être entravée sans justifications. Il en découle que la protection des données à caractère médical et, si jamais, les différences législatives entre la France et l'Italie ne peuvent pas constituer une entrave à la mobilité des patients entre les deux territoires en question.

Le système de protection des données est donc uniforme, des différences substantielles ne sont pas admises. Bien sûr, cela n'empêche pas qu'elles ne peuvent exister. Le cas échéant, c'est le règlement RGDP qui devra trouver à s'appliquer. De plus, en cas de litige, ça sera au règlement RGDP à prévaloir sur les normes nationales divergentes et s'il y a des doutes d'interprétation, le juge nationale – français ou italien, en fonction de la juridiction compètent – soulèvera une question préjudicielle auprès de la Cour de justice de l'Union européenne. La Cour, à la fois, interprètera le règlement RGPD et par ricochet, éventuellement, la législation nationale. Mais cela pourrait arriver éventuellement en France ; il est difficile imaginer cette hypothèse en Italie puisque le *decreto legislativo* 101/2018 a essentiellement copié le règlement RGPD.

En conclusion, l'uniformité de la protection des données à caractère personnel a été atteinte à travers le règlement RGPD. Toutes les administrations sont obligées à le respecter et à l'appliquer, soit en présence de question interne soit en présence de questions de mobilité transfrontalière. Enfin, les particuliers peuvent l'invoquer, vis-à-vis les administrations publiques et/ ou devant les juges nationaux.

Glossaire

RGPD : 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).

Decreto legislativo 101/2018 : acte italien qui met à jour le *codice della privacy* en incorporant le RGPD.

Codice della privacy : code qui recueille les normes en matière de protection de données.

Données à caractère personnel : toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée « personne concernée ») ; est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

Données génétiques : les données à caractère personnel relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique qui donnent des informations uniques sur la physiologie ou l'état de santé de cette personne physique et qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne physique en question.

Données biométriques : les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques.

Données de santé : les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne.

Délégué à la protection des données (DPO) : l'interlocuteur privilégié des personnes souhaitant poser des questions relatives au traitement de leurs données à caractère personnel et à l'exercice des droits que leur confère le RGPD au sein des hôpitaux et organismes qui traitent des données de santé à grande échelle.

Consentement de la personne concernée : toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement.

Etat membre d'affiliation : l'Etat où un patient est affilié à un régime de sécurité sociale et/ ou d'assurance maladie.

État membre de soin : l'Etat où le patient reçoit un soin médical.

Fascicolo sanitario elettronico : ensemble des données et documents sanitaires découlant des évènements cliniques d'un patient en Italie.

Cartella clinica digitale : document créé par la structure sanitaire italienne qui soigne un patient pour lui garantir la continuité de l'assistance.

Garante della privacy : autorité administrative indépendante italienne qui surveille la protection des données à caractère personnel.

CNIL (Commission nationale de l'informatique et des libertés) : l'autorité administrative indépendante française en charge de veiller à la protection des données personnelles. A ce titre, elle dispose notamment d'un pouvoir de contrôle et de sanction.

Informazione sul trattamento dei dati personali : acte que l'ASL doit publier pour informer les patients des règles concernant la protection de leurs données.