



Requête en constatation d'un traitement de données illicite

Recommandation du 19 juillet 2023

I. Le Préposé cantonal à la protection des données et à la transparence constate:

1. Dans un courrier recommandé daté du 1^{er} mai 2023 adressé à A., directeur de la direction des affaires juridiques et responsable LIPAD des Hôpitaux universitaires de Genève (HUG), X., représentant Y., fait état de ce qui suit. Ce dernier a été réengagé par les HUG depuis le 1^{er} octobre 2022. Dans le cadre de son engagement, il a informé le service de « médecine du travail », chargé de l'évaluation de l'aptitude du personnel médical, de ses antécédents psychiatriques. Le 8 février 2023, il a été hospitalisé aux urgences des HUG. Dans ce cadre, des personnes (collègues employés des HUG) auraient accédé de manière indue (par pure curiosité) à son dossier médical, notamment à son dossier psychiatrique relatif à un passage aux urgences psychiatriques le 5 février 2023. Dans des courriels du 31 mars et 19 avril 2023 (non communiqués au Préposé cantonal), les HUG auraient indiqué que l'interniste visée par l'accès indu n'aurait pas reçu de sanctions selon l'art. 64 LIPAD, faute de compétence en la matière. X. estime choquant le fait que l'ensemble du personnel hospitalier des HUG ait accès aux données médicales de tous les employés de l'établissement hospitalisés pendant toute la durée de conservation. En définitive, elle réclame l'octroi d'un patronyme fictif pour Y. dans son dossier patient intégré (DPI), afin de faire cesser l'atteinte illicite qu'il continuerait de subir.
2. Par courrier adressé le 25 mai 2023 à A., la précitée s'est enquis des mesures que les HUG entendent prendre pour mettre fin à l'atteinte dont elle dit victime Y.
3. Dans sa réponse du 14 juin 2023, A. indique que le DPI est conçu à la fois pour protéger la confidentialité des données patients et pour assurer la plus grande qualité de soins possible; les accès sont de la sorte restreints au maximum, mais dans la limite de ce qui est nécessaire pour permettre une prise en charge optimale du patient. Le responsable LIPAD précise que tous les collaborateurs des HUG n'ont pas les mêmes droits d'accès au DPI. Par ailleurs, « *Pour des raisons de qualité de prise en charge et de sécurité des patients, l'accès aux dossiers médicaux ne doit pas faire l'objet d'obstacles, notamment de nature technique. En effet, dans le contexte d'une prise en charge globale ou postérieure par exemple, il est absolument nécessaire pour les médecins et le personnel soignant de pouvoir accéder aux informations du patient concerné, même si celui-ci a été pris en charge ultérieurement dans un service différent. Admettre le contraire pourrait grandement mettre en péril la qualité des soins et la sécurité des patients. Afin de garantir la confidentialité des données patients, les règles institutionnelles imposent certains devoirs aux collaborateurs des HUG qui accèdent au DPI. Ainsi, ces collaborateurs ne sont en principe autorisés à accéder au dossier d'un patient que dans le cadre d'une relation thérapeutique durant une période limitée ou au moyen d'une justification valable. Afin de surveiller le respect de ces règles, chaque connexion hors prise en charge doit être justifiée, chaque navigation est enregistrée et chaque patient peut accéder à la liste des accès à son dossier et éventuellement dénoncer un accès suspect, qui fera, le cas échéant, l'objet d'investigations* ». Enfin, la Directive « Confidentialité liée aux patients » ne trouve pas application dans le cas d'espèce, si bien que la demande d'octroi d'un patronyme fictif ne peut être accordée.

4. Le 15 juin 2023, X. a saisi la Commission de surveillance des professions de la santé et des droits des patients (CSPSDP) d'une plainte contre les HUG et certains membres de son personnel pour manquements sévères aux dispositions légales relatives à la protection des données et à la personnalité et déni de justice. Elle relève notamment le manque de protection des données médicales des patients au sein des HUG. Elle requiert que soient constatés le déni de justice formel des HUG et les manquements de ces derniers dans la mise en place et la gestion du système d'accès et de traitement des données médicales des patients.
5. Le 15 juin 2023, la susnommée a fait parvenir au Préposé cantonal le courrier mentionné plus haut (sans ses annexes). Elle sollicite que l'accès au dossier psychiatrique de son mandant, plus généralement des patients des HUG, soit à l'avenir strictement bloqué pour tous les membres du personnel travaillant en dehors du service psychiatrique.
6. Par courrier du 23 juin 2023 adressé au Préposé cantonal, X. estime que la Directive « Confidentialité liée aux patients » trouve application et permet donc d'octroyer au lésé la protection requise.
7. Conformément à l'art. 49 al. 5 LIPAD, « *le Préposé cantonal instruit la requête de manière informelle, puis il formule, à l'adresse de l'institution concernée et du requérant, une recommandation écrite sur la suite à donner à la requête* ».

II. Le Préposé cantonal à la protection des données et à la transparence observe en droit:

8. Entrée en vigueur le 1^{er} mars 2002, la LIPAD pose le principe de la transparence des institutions publiques. Son but est de favoriser la libre formation de l'opinion et la participation à la vie publique des citoyennes et des citoyens. A ce titre, la loi leur donne des droits en matière d'accès aux documents en lien avec les activités des institutions publiques.
9. En 2008, la loi a fait l'objet d'une révision importante: la protection des données personnelles a été ajoutée au volet transparence. De la sorte, un autre objectif figure désormais dans le texte: protéger les droits fondamentaux des personnes physiques ou morales de droit privé quant aux données personnelles les concernant.
10. La LIPAD est applicable aux institutions publiques genevoises, en particulier aux « *institutions, établissements et corporations de droit public cantonaux et communaux, ainsi que leurs administrations et les commissions qui en dépendent* » (art. 3 al. 1 litt. c LIPAD). Les Hôpitaux universitaires de Genève (HUG) constituent un établissement public médical du canton de Genève (art. 1 al. 1 de la loi sur les établissements publics médicaux du 19 septembre 1980; LEPM; RSGe K 2 05). De la sorte, la LIPAD leur est applicable.
11. Par données personnelles, il faut comprendre « *toutes les informations se rapportant à une personne physique ou morale de droit privé, identifiée ou identifiable* » (art. 4 litt. a LIPAD). Tant que les données n'ont pas été rendues anonymes, l'on se trouve face à des questions relatives à la protection de données personnelles.
12. Les données personnelles sensibles comprennent les données personnelles sur les opinions ou activités religieuses, philosophiques, politiques, syndicales ou culturelles; la santé, la sphère intime ou l'appartenance ethnique; des mesures d'aide sociale; des poursuites ou sanctions pénales ou administratives (art. 4 litt. b LIPAD).

13. La loi énonce un certain nombre de principes généraux régissant la protection des données personnelles (art. 35 à 40 LIPAD), soit en particulier:

– **Base légale** (art. 35 al. 1 et 2 LIPAD)

Le traitement de données personnelles ne peut se faire que si l'accomplissement des tâches légales de l'institution publique le rend nécessaire. En outre, la loi stipule que des données personnelles sensibles ou des profils de la personnalité ne peuvent être traités que si une loi définit clairement la tâche considérée et si le traitement en question est absolument indispensable à l'accomplissement de cette tâche ou s'il est nécessaire et intervient avec le consentement explicite, libre et éclairé de la personne concernée.

– **Bonne foi** (art. 38 LIPAD)

Il n'est pas permis de collecter des données personnelles sans que la personne concernée en ait connaissance, ni contre son gré. Quiconque trompe la personne concernée lors de la collecte des données – par exemple en collectant les données sous une fausse identité ou en donnant de fausses indications sur le but du traitement – viole le principe de la bonne foi. Il agit également contrairement à ce principe s'il collecte des données personnelles de manière cachée.

– **Proportionnalité** (art. 36 LIPAD)

En vertu du principe de la proportionnalité, seules les données qui sont nécessaires et qui sont aptes à atteindre l'objectif fixé peuvent être traitées. Il convient donc toujours de peser les intérêts en jeu entre le but du traitement et l'atteinte à la vie privée de la personne concernée en se demandant s'il n'existe pas un moyen moins invasif permettant d'atteindre l'objectif poursuivi.

– **Finalité** (art. 35 al. 1 LIPAD)

Conformément au principe de finalité, les données collectées ne peuvent être traitées que pour atteindre un but légitime qui a été communiqué lors de leur collecte, qui découle des circonstances ou qui est prévu par la loi. Les données collectées n'ont ensuite pas à être utilisées à d'autres fins, par exemple commerciales.

– **Reconnaissabilité de la collecte** (art. 38 LIPAD)

La collecte de données personnelles, et en particulier les finalités du traitement, doivent être reconnaissables pour la personne concernée. Cette exigence de reconnaissabilité constitue une concrétisation du principe de la bonne foi et augmente la transparence d'un traitement de données. Cette disposition implique que, selon le cours ordinaire des choses, la personne concernée doit pouvoir percevoir que des données la concernant sont ou vont éventuellement être collectées (principe de prévisibilité). Elle doit pouvoir connaître ou identifier la ou les finalités du traitement, soit que celles-ci lui sont indiquées à la collecte ou qu'elles découlent des circonstances.

– **Exactitude** (art. 36 LIPAD)

Quiconque traite des données personnelles doit s'assurer de l'exactitude de ces dernières. Ce terme signifie également que les données doivent être complètes et aussi actuelles que les circonstances le permettent. La personne concernée peut demander la rectification de données inexactes.

– **Sécurité des données** (art. 37 LIPAD)

Le principe de sécurité exige non seulement que les données personnelles soient protégées contre tout traitement illicite et tenues confidentielles, mais également que l'institution en charge de leur traitement s'assure que les données personnelles ne soient pas perdues ou détruites par erreur.

– **Destruction des données** (art. 40 LIPAD)

Les institutions publiques détruisent ou rendent anonymes les données personnelles dont elles n'ont plus besoin pour accomplir leurs tâches légales, dans la mesure où ces données ne doivent pas être conservées en vertu d'une autre loi.

14. L'art. 47 LIPAD détermine les prétentions que toute personne physique ou morale de droit privé peut exiger des institutions publiques à propos des données la concernant, soit qu'elles s'abstiennent de procéder à un traitement illicite, le cas échéant qu'elles mettent fin à un tel traitement et en suppriment les effets, ou qu'elles constatent le caractère illicite de ce traitement, qu'elles détruisent celles qui ne sont pas pertinentes ou nécessaires (sauf disposition légale contraire), rectifient, complètent ou mettent à jour celles qui sont respectivement inexactes, incomplètes ou dépassées, ou fassent figurer, en regard de celles dont ni l'exactitude ni l'inexactitude ne peuvent être prouvées, une mention appropriée, à transmettre également lors de leur communication éventuelle.
15. Selon l'art. 49 LIPAD, une institution publique qui n'entend pas donner suite à une prétention fondée sur les art. 44, 47 ou 48 LIPAD doit transmettre la requête au Préposé cantonal avec ses observations, afin qu'il rende une recommandation écrite à son attention et à celle du requérant.

III. Le Préposé cantonal à la protection des données et à la transparence considère:

16. En préambule, les Préposés relèvent que les données personnelles dont il est présentement question sont des données sensibles au sens de l'art. 4 litt. b LIPAD, dès lors qu'elles sont relatives à la santé.
17. La requérante réclame tout d'abord l'octroi d'un patronyme fictif pour Y. dans son dossier patient intégré (DPI). Elle sollicite ensuite que l'accès au dossier psychiatrique de son mandant, plus généralement des patients des HUG, soit à l'avenir strictement bloqué pour tous les membres du personnel travaillant en dehors du service psychiatrique.
18. S'agissant en premier lieu de **l'octroi d'un patronyme fictif**, les Préposés constatent que la Directive « Confidentialité liée aux patients », approuvée par le Comité de direction des HUG dans sa séance du 2 février 2015, a pour but de renforcer, en cas d'impérative nécessité, la confidentialité d'un patient dans les HUG (point 1). Elle rappelle le secret professionnel, qui couvre l'identité du patient hospitalisé (ou soigné en ambulatoire) et donc sa présence même à l'hôpital (point 2). La Directive envisage deux mesures à mettre en œuvre: la discrétion totale (point 3) et le changement d'identité (point 4). La première est une mention faite au dossier pour assurer qu'aucune information sur la présence du patient à l'hôpital n'est fournie à l'externe (acheminement du courrier, de fleurs, d'appel ou de visites). Le personnel de l'accueil ne dispose plus des noms sur la liste des patients actifs, mais conserve l'accès à cette information en passant par le dossier patient administratif (DPA). La Directive envisage ensuite le changement d'identité, soit une mesure exceptionnelle (qui n'est pas destinée aux collaborateurs des HUG) soumise à l'approbation du délégué à la sécurité des HUG, nécessitant une information à la Direction générale et à la Direction générale adjointe dans le but d'assurer la sécurité d'une personnalité publique ou à risque durant son hospitalisation. A la fin du séjour, l'opération inverse est réalisée selon la même voie pour réconcilier les données sous l'identité officielle, permettre la facturation et assurer la qualité des soins en cas d'hospitalisation future.
19. Dans le cas d'espèce, Y. est à la fois un employé et un patient des HUG. La requérante réclame pour ce dernier l'octroi d'un patronyme fictif, soit un changement d'identité.

Cette mesure doit d'emblée être écartée, car la Directive prévoit expressément que cette mesure exceptionnelle n'est pas destinée aux collaborateurs des HUG. Quand bien même la discrétion totale n'est pas sollicitée, elle ne répondrait pas non plus au but visé par la plaignante, puisqu'elle vise une discrétion pour l'extérieur et que si le personnel de l'accueil ne dispose plus des noms sur la liste des patients actifs, il conserve néanmoins l'accès à l'information en passant par le DPA. Au surplus, la Directive vise uniquement le renforcement de la confidentialité d'un patient dans les HUG, en cas « d'impérative nécessité », ce qui n'a pas été démontré par la requérante. Dès lors, pour les Préposés, l'octroi d'un patronyme fictif ne peut être accordé, d'autant plus qu'il ne s'agit pas d'une prétention prévue par l'art. 47 LIPAD.

20. La précitée demande ensuite que **l'accès au dossier psychiatrique de son mandant**, plus généralement des patients des HUG, **soit à l'avenir strictement bloqué** pour tous les membres du personnel travaillant en dehors du service psychiatrique. Il s'agit donc d'une requête en constatation du caractère illicite de l'atteinte, puisque des employés des HUG auraient accédé de manière indue (par pure curiosité) au dossier médical de Y., notamment à son dossier psychiatrique.
21. Les Préposés remarquent que le principe de sécurité (art. 37 LIPAD) exige notamment que les données personnelles soient protégées contre tout traitement illicite et tenues confidentielles. L'art. 13 al. 1 RIPAD précise que les institutions publiques prennent les mesures organisationnelles et techniques propres à assurer la sécurité des données personnelles. Selon l'art. 13 al. 2 litt. c RIPAD, ces mesures sont notamment définies par l'article 23A al. 5 du règlement d'application de la loi générale relative au personnel de l'administration cantonale, du pouvoir judiciaire et des établissements publics médicaux du 24 février 1999 (RPAC; RSGe B 5 05.01). Selon cette norme, « *Lorsque les intérêts prépondérants de l'Etat de Genève, tels que la sécurité informatique ou le bon fonctionnement du service, l'exigent, des contrôles individualisés, et le cas échéant un accès à la liste des appels et à leur durée, au poste de travail informatique ou au compte de messagerie, peuvent être ordonnés par le chef du département ou son secrétaire général. Ces mesures respectent, dans toute la mesure du possible, la sphère privée des membres du personnel concernés* ». En outre, selon l'art. 13 al. 3 RIPAD, les institutions publiques tiennent à jour un répertoire des personnes ayant accès aux systèmes d'information contenant des données personnelles. Enfin, l'art. 54 de la loi sur la santé du 7 avril 2006 (LS; RSGe K 1 03) prévoit que le dossier du patient peut être tenu sous forme informatisée, pour autant que toute adjonction, suppression ou autre modification reste décelable et que l'on puisse identifier son auteur et sa date.
22. Les Préposés comprennent que tous les collaborateurs des HUG n'ont pas les mêmes droits d'accès au DPI et qu'afin de garantir la confidentialité des données patients, les règles institutionnelles leur imposent certains devoirs: ils ne sont en principe autorisés à accéder au dossier d'un patient que dans le cadre d'une relation thérapeutique durant une période limitée ou au moyen d'une justification valable.
23. Les Préposés prennent également note du fait que les HUG jugent nécessaire pour les médecins et le personnel soignant de pouvoir accéder aux informations du patient concerné, même si celui-ci a été pris en charge ultérieurement dans un service différent, afin de garantir la qualité des soins et la sécurité des patients.
24. La requérante reconnaît que le système mis en place par les HUG conserve les empreintes digitales ou logs (données relatives aux dates des connexions, personnes connectées, temps passé à consulter un document, etc.) des personnes qui se sont connectées aux dossiers médicaux, ce qui instaure ainsi une traçabilité certaine. Les HUG avancent à cet égard que « *chaque connexion hors prise en charge doit être justifiée, chaque navigation est enregistrée et chaque patient peut accéder à la liste des*

accès à son dossier et éventuellement dénoncer un accès suspect, qui fera, le cas échéant, l'objet d'investigations ».

25. Au vu de ce qui précède, il apparaît que les HUG ont mis en place des mesures techniques et organisationnelles pour protéger les données d'une consultation indue. Cependant, à titre incident, ils considèrent que certaines réserves pourraient être avancées, au regard du principe de proportionnalité. En effet, les accès mis en place sont très larges. L'on pourrait imaginer par exemple que les HUG donnent un accès complet au DPI au service des urgences, mais restreignent ledit accès aux autres services, afin que ces derniers ne traitent que des données personnelles nécessaires à leur activité, et si besoin, sur demande, puissent accéder à l'ensemble du dossier. Les Préposés suggèrent qu'une réflexion soit entamée sur cette question des accès.
26. Il convient encore d'évoquer l'art. 64 al. 1 LIPAD, selon lequel « *Celui qui, au sein d'une institution soumise à la présente loi, traite des données personnelles à des fins étrangères à l'accomplissement des tâches légales qui lui sont confiées est passible de l'amende, sans préjudice des peines plus fortes prévues par le droit fédéral* ».
27. L'amende est prononcée, pour le contrevenant relevant d'un établissement public autonome, par l'instance directrice supérieure de l'établissement (art. 64 al. 3 litt. e LIPAD). La Direction des HUG peut donc tout à fait prononcer une amende sur cette base.
28. S'il appert qu'une personne a indûment consulté des dossiers, se pose alors la question de la sanction à infliger à l'auteur de ce traitement illicite (selon l'art. 64 LIPAD ou selon les règles disciplinaires idoines). L'absence de sanction équivaut à tolérer un traitement illicite. Si l'entité publique n'entend pas infliger de sanction, des accès plus restreints aux données personnelles doivent être prévus.
29. En conséquence, sous la réserve précédente, les Préposés recommandent aux HUG de rejeter la requête en constatation du caractère illicite de l'atteinte.

Recommandation

Se fondant sur les considérations qui précèdent, le Préposé cantonal recommande au Hôpitaux universitaires de Genève (HUG) de rejeter la requête en constatation du caractère illicite de l'atteinte.

Dans les 10 jours à compter de la réception de la présente recommandation, les Hôpitaux universitaires de Genève (HUG) doivent rendre une décision sur les prétentions des requérants (art. 49 al. 6 LIPAD).

La présente recommandation est notifiée par pli recommandé à:

- X.....
- A., responsable LIPAD, HUG, Direction des affaires juridiques, boulevard de la Cluse 77, 1211 Genève 4

Stéphane Werly
Préposé cantonal

Joséphine Boillat
Préposée adjointe

Pour rappel, conformément à l'art. 49 al. 6 LIPAD, l'institution publique notifie une copie de sa décision au Préposé cantonal à la protection des données et à la transparence.
--