S.E.L.A.R.L. OPALEBIO LABORATOIRES DE BIOLOGIE MEDICALE
20 RUE DE VERDUN BP 71 62630 ETAPLES

CHARTRE

PROTECTION DES DONNEES

Table des matières

1 Préambule

1. La présente charte de protection des données à caractère personnel a pour objet de formaliser les règles de déontologie et de sécurité que s'engagent à respecter tous les utilisateurs du système d'informations du laboratoire de biologie médicale OPALEBIO pour assurer la conformité des traitements de données à caractère personnel avec la réglementation sur la protection des données.

2. Ainsi, la présente charte de protection des données à caractère personnel illustre le comportement responsable et loyal que chacun doit observer à l'occasion de la réalisation et de l'exploitation des traitements de données à caractère personnel.

2 Enjeux

3. Le LBM entend considérer la protection des données à caractère personnel comme une nécessité visant à sauvegarder:

- d'une part, l'absence d'atteinte à la vie privée et aux libertés de ses patients ;
- d'autre part, la réputation et la responsabilité des responsables du LBM.

4. Le LBM a la volonté d'inscrire ses activités dans le respect des obligations en matière de protection des données qui lui incombent et de mettre en œuvre les moyens nécessaires à cet effet.

5. Cette volonté s'est traduite par la mise en place de moyens techniques et humains, et de mesures organisationnelles adaptées issus du code de conduite des LBM qui s'inscrivent dans une approche qualité de l'application du règlement général sur la protection des données[1] de la loi Informatique et libertés[2] et de ses principes directeurs au sein du LBM.

6. Cette charte a pour objectif de :

- diffuser une culture concernant la protection des données au sein du LBM ;
- favoriser le maintien d'une adéquation permanente entre, d'une part, les exigences de la réglementation et les recommandations de la Cnil, et d'autre part, les réalités quotidiennes du LBM.

7. Par ailleurs, dans cette optique de protection des données, ont été définies :

- des politiques et procédures internes ;
- des actions de sensibilisation, d'information et de formation du personnel.

[1] 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

[2] Loi n°78-17 du 6 janvier 1978 relative à l'Informatique, aux fichiers et aux libertés

8. C'est au cœur de cette démarche responsable et proactive du LBM que s'inscrit la présente charte.

3 Définitions

9. Les termes ci-dessous définis, au singulier ou au pluriel, ont la signification suivante :

- « Cnil » : Commission Nationale de l'Informatique et des Libertés ;

- « données à caractère personnel » : toutes informations 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 à caractère personnel sensibles » : données à caractère personnel se rapportant de façon directe ou indirecte aux origines raciales, ethniques, politiques, philosophiques, religieuses ou à l'appartenance syndicale des personnes, à la santé ou la vie sexuelle. Dans la présente charte, il s'agira avant tout des données se rapport à la santé ;

- « données de santé » : données à caractère personnel relatives à la santé physique, y compris la prestation et services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne ;

- « flux transfrontières » : transmission par tout moyen de données à caractère personnel à un destinataire localisé dans un pays situé hors de l'Union européenne ;

- « personne concernée » : personne à laquelle se rapportent les données qui font l'objet d'un traitement. En l'espèce, il s'agit le plus souvent des patients du LBM ;

- « sécurité des données » : la notion de sécurité des données à caractère personnel comprend des impératifs d'intégrité et de confidentialité des données à caractère personnel. Tout responsable d'un traitement de données à caractère personnel doit prendre toutes les précautions utiles qui, au regard de la nature des données et des risques présentés par un traitement, s'imposent pour préserver l'intégrité et la confidentialité des données et ainsi empêcher que ces dernières ne soient déformées, endommagées ou que des tiers non autorisés en prennent connaissance et y aient accès ;

- « sous-traitant » : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement ;

- « système d'informations » : le système d'informations et de communication, les ordinateurs (fixes ou portables), les périphériques, les assistants personnels, les réseaux informatiques, les photocopieurs, les téléphones, les logiciels, les bases de

données, les systèmes de messagerie, intranet, extranet, les services interactifs et les sessions des postes de travail ;

- « utilisateurs » : les personnes salariées ou non, tous statuts juridiques confondus, permanents ou temporaires, autorisées à utiliser les systèmes d'information ;

- « zones de commentaires libres » : zones de saisie libre des applications informatiques des systèmes d'information, par exemple les zones « observations ».

4 Périmètre

10. La présente charte a vocation à s'appliquer dès lors qu'un traitement de données à caractère personnel est mis en œuvre ou exploité par un utilisateur pour le compte du LBM.

5 Principes de traitement des données à caractère personnel

5.1 Finalité déterminée

11. Les utilisateurs s'engagent à ce que les données collectées le soient pour des finalités déterminées, explicites et légitimes et à ce que les données ne soient pas traitées ultérieurement de manière incompatible avec les finalités initiales du traitement[3].

12. En tout état de cause, il est interdit aux utilisateurs de commercialiser auprès de tiers les données à caractère personnel collectées par le LBM.

5.2 Principe de loyauté et de licéité

13. Chaque utilisateur s'engage à ne réaliser un traitement de données à caractère personnel qu'à partir de données collectées de manière licite, loyale et transparente au regard du patient[4].

14. En particulier, chaque utilisateur s'engage à ne collecter que les données à caractère personnel nécessaires à la réalisation du traitement dans le respect du droit à l'information des personnes concernées ou, le cas échéant, après avoir recueilli son consentement.

15. A ce titre, l'utilisateur s'engage à respecter la procédure d'information et la note d'informations mises à disposition par le LBM (ex. apposition d'une affichette dans la salle d'attente, délivrance d'un livret d'accueil, etc.).

5.2.1 Principal fondement du traitement de données de santé

16. En principe, l'utilisateur ne peut procéder à un traitement de données de santé pour le compte du LBM que si celui-ci est nécessaire aux fins de la prise en charge sanitaire du patient et repose sur l'article 9.2.h) du RGPD[5].

[3] RGPD, art. 5.1,b)
[4] RGPD, art. 5.1.a)

17. Dans cette hypothèse, l'utilisateur n'est pas tenu de recueillir le consentement du patient mais doit informer ce dernier conformément au principe de transparence susvisé. Ainsi, avant de mettre en œuvre un traitement, l'utilisateur en charge de celui-ci doit vérifier que les patients concernés ont été informés :

- des traitements portant sur les données à caractère personnel les concernant ;
- de leurs droits.

18. A ce titre, un modèle d'information ainsi qu'une procédure d'information des patients est mis à disposition de l'utilisateur par le LBM (ex. apposition d'une affichette dans la salle d'attente, délivrance d'un livret d'accueil, etc.).

5.2.2 Traitements nécessitant le consentement du patient

19. En revanche, lorsque les traitements de données de santé ne sont pas nécessaires aux fins de diagnostics médicaux, de prise en charge sanitaire du patient ou à la gestion des systèmes et services de soins de santé, l'utilisateur doit informer le patient et recueillir son consentement au traitement[6].

5.2.3 Spécificité concernant l'utilisation des fonds de tube

20. L'utilisation des fonds des prélèvements à des fins médicales ou scientifiques autres que celle pour laquelle le prélèvement a été effectué (ex. fond de tube) suppose une information spécifique et préalable du patient aux fins pour celui-ci de pouvoir, le cas échéant, exercer son droit d'opposition[7].

21. A ce titre, le modèle de note d'information mis à disposition par le LBM comprend ces mentions.

5.3 Principes de minimisation et d'exactitude des données

5.3.1 Règles générales

22. Seules peuvent être collectées les données à caractère personnel adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles le traitement est réalisé, c'est-à-dire au regard de la prise en charge du patient[8].

23. L'utilisateur doit s'assurer que les données des patients sont exactes et, lorsque cela est nécessaire, tenues à jour. L'utilisateur s'engage à mettre à jour régulièrement les données à caractère personnel traitées et à prendre des mesures afin de permettre que les données inexactes soient effacées ou rectifiées.

5.3.2 Traitement portant sur le numéro de sécurité sociale (NIR)

24. A l'intérieur du LBM, un identifiant local doit être utilisé, propre à chaque patient, lequel doit être distinct du numéro d'assuré social (NIR)[9] Chaque échantillon biologique est notamment identifié par cet identifiant.

---

[5] RGPD, art. 9
[6] RGPD, art. 9
[7] CSP, art. L. 1211-2
[8] RGPD, art. 5.1.c) et d)
[9] CSP, art. D. 6211-2

25. Sur la base du principe de minimisation susvisé, le NIR doit être utilisé uniquement lorsque ce dernier est strictement nécessaire, à savoir, pour les opérations de facturation et, le cas échéant, lors de l'échange ou du partage de données médicales.

26. Outre le respect des prérequis applicables à tout traitement de données à caractère personnel, l'utilisateur concerné doit, avant la mise en œuvre d'un traitement portant sur le numéro de sécurité sociale, vérifier que l'utilisation souhaitée de ce numéro correspond à l'une des hypothèses autorisées par la loi.

27. En tout état de cause, toute utilisation du numéro de sécurité sociale doit faire l'objet d'une analyse préalable afin d'en déterminer sa licéité.

28. A défaut, la collecte du numéro de sécurité sociale est interdite.

5.3.3 Spécificités des zones commentaires

29. Lorsque des zones commentaires ou zones libres sont présentes dans le système d'information du LBM, celles-ci ne doivent contenir que des données objectives respectant la dignité des personnes concernées. Les données d'identification raciales, ethniques, religieuses ou cultuelles, les informations injurieuses, diffamatoires, blessantes, péjoratives ou désobligeantes sont interdites.

5.4 Limitation de la durée de conservation des données

30. Chaque utilisateur s'engage à ne conserver les données faisant l'objet des traitements réalisés que pour la durée nécessaire à la finalité du traitement réalisé[10].

31. A ce titre, l'utilisateur doit respecter la politique de durée de conservation des données du LBM et le système de purge automatique ou manuel décrit dans la politique de suppression des données mise à disposition par le LBM.

6 La sécurité des données

6.1 Principes directeurs

32. Tout utilisateur en charge d'un traitement de données à caractère personnel doit prendre toutes les précautions utiles au regard du risque encouru afin de préserver la sécurité, la confidentialité et l'intégrité des données, et d'empêcher toute communication à des tiers non autorisés[11].

33. A ce titre, outre les sanctions administratives prévues par le RGPD et la loi informatique et libertés[12], le non-respect des obligations de sécurité est pénalement sanctionné.

34. L'utilisateur s'engage à respecter les principes relatifs à la protection des données dès la conception du traitement et à la protection des données par défaut[13] :

[10] RGPD, art. 5.1.e)
[11] RGPD, art. 32
[12] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
[13] RGPD, art. 25

- la protection dès la conception consiste à mettre en œuvre, en amont et lors de la détermination des moyens du traitement, des mesures techniques et organisationnelles destinées au respect des principes relatifs à la protection des données du patient en fonction du risque généré par le traitement.
    - par exemple, tout développement informatique ou test afférent doit être effectué dans un environnement distinct de celui de la production et avec des données fictives ou anonymisées.

- la protection par défaut consiste à garantir que, par défaut, seules les données nécessaires à la finalité sont traitées, notamment au regard de la quantité des données, l'étendue des traitements, la durée de conservation et leur accessibilité.

6.2 Sécurité du système d'information pour la mise en œuvre d'un traitement

35. Les utilisateurs s'engagent à respecter l'ensemble des règles permettant d'assurer la sécurité des données à caractère personnel faisant l'objet de l'un de leurs traitements, notamment les règles définies dans la charte d'utilisation du système d'information du laboratoire et en particulier les règles d'identification et d'authentification qui lui sont imposées dans ce cadre.

36. Ils vérifient et assurent la sécurité de l'accès aux applications qu'ils utilisent et qui contiennent des données à caractère personnel.

37. Afin d'assurer la confidentialité des données à caractère personnel qu'ils traitent, les utilisateurs s'interdisent de les rendre accessibles à des services non habilités à en prendre connaissance.

38. De la même façon, il est interdit de communiquer par quelque moyen que ce soit à des tiers non autorisés des données à caractère personnel.

39. En tout état de cause, il est nécessaire d'informer le responsable du LBM de tout risque concernant la sécurité des données à caractère personnel, par les outils mis en œuvre et dans les meilleurs délais.

6.3 Sécurité des échanges de données à caractère personnel avec les tiers

40. Il convient que chaque utilisateur veille à la sécurisation des transmissions de données à caractère personnel préalablement à leur mise en œuvre.

41. Les données à caractère personnel ne peuvent être transmises qu'aux personnes habilitées à en connaître.

42. Avant transmission de données à caractère personnel, l'utilisateur s'engage à vérifier :

- l'identité et les coordonnées du destinataire ainsi que sa légitimité à en connaître (habilitation). Il peut également solliciter l'avis de sa direction préalablement à la transmission ;

- que les moyens de communications utilisés sont de nature à assurer la sécurité et la confidentialité des données. Cela implique que les flux soient chiffrés (VPN SSL ; Https, FTPS, Web service sécurisés, MSS, etc.). Tout risque

de défaillance de sécurité dont un utilisateur aurait connaissance doit conduire à suspendre la transmission jusqu'à résolution du problème rencontré.

43. Tout utilisateur mettant en œuvre un traitement de données à caractère personnel ou amené à réceptionner des données à caractère personnel s'interdit de prendre connaissance des données à caractère personnel qui ne lui sont pas destinées ou dont il n'est pas habilité à prendre connaissance.

6.4 Mesures de sécurité contractuelles avec les sous-traitants

44. Chaque utilisateur qui sous-traite une partie ou la totalité d'un traitement de données à caractère personnel, s'engage à imposer contractuellement à son sous-traitant des garanties de confidentialité des données à caractère personnel par le biais de mesures techniques et humaines de protection de ces données.

45. L'utilisateur doit veiller à ce que l'engagement entre le LBM et le sous-traitant soit formalisé par un contrat reprenant les modèles de clauses types mis à disposition par le LBM[14].

6.5 Incidents de sécurité et violation de données

46. L'utilisateur doit signaler tout incident de sécurité au responsable du LBM dans le respect de la procédure de notification des incidents de sécurité mise à disposition par le LBM[15]. Cette procédure précise les éléments liés à :

- la détection des violations et, le cas échéant, l'information du délégué à la protection des données à caractère personnel ;
- la détermination de la nature de la violation ;
- la formulation des recommandations et la transmission au responsable du LBM ;
- la formulation d'un plan d'actions appropriées et sa validation ;
- la réalisation des actions correctives ;
- la révision de l'étude des risques.

47. Il est précisé à l'utilisateur que les délais suivants de notification de toute violation de données sont imposés au LBM :

- la notification à la Cnil doit être réalisée dans les meilleurs délais et si possible 72 heures au plus tard après en avoir pris connaissance ; et
- lorsqu'elle est nécessaire, la communication aux patients doit être effectuée dans les meilleurs délais.

48. A défaut, le LBM et son responsable sont exposés à des sanctions administratives et pénales.

[14] RGPD, art. 28

[15] RGPD, art. 33 et 34

7 Délégué à la protection des données

Ces informations de contact permettent à toute personne de joindre le délégué facilement. La CNIL les tient à disposition du public dans des formats ouverts.

Adresse postale publique 20 RUE DE VERDUN
62630 ETAPLES
FRANCE
Ligne téléphonique dédiée 0321946335
Adresse électronique dédiée DPO.OPALEBIO@ORANGE.FR

Les exigences relatives à la désignation d'un délégué à la protection des données (statut, fonction, missions, qualités professionnelles) sont définies aux articles 37 à 39 du règlement européen relatif à la protection des données personnelles (RGPD). Le non-respect de ces dispositions est passible de sanctions.
En savoir plus : https://www.cnil.fr/le-dpo
Les données personnelles nécessaires à l'accomplissement des missions de la CNIL sont conservées et traitées dans des fichiers destinés à son usage exclusif. Les personnes concernées peuvent exercer leurs droits Informatique et Libertés en s'adressant au délégué à la protection des données de la CNIL via un formulaire en ligne ou par courrier postal.
Pour en savoir plus : https://www.cnil.fr/donnees-personnelles.

49. Le délégué à la protection des données du LBM a pour missions de:

- informer et conseiller sur les obligations qui incombent en vertu des règles relatives à la protection des données ;

- contrôler le respect de ces règles, y compris concernant la répartition des responsabilités au sein du LBM, la sensibilisation et la formation des utilisateurs ainsi que les audits s'y rapportant ;

- dispenser des conseils concernant l'analyse d'impact des nouveaux traitements ;

- coopérer avec la Cnil ou toute autre autorité compétente et faire office de point de contact avec celle-ci.

50. En cas de difficultés, l'utilisateur doit prendre contact avec sa hiérarchie à qui il appartient de communiquer toute problématique liée à la protection des données au délégué à la protection des données du LBM. Celui-ci sera alors chargé d'élaborer des pistes de solutions à soumettre dans les délais utiles au responsable du LBM.

8 Les droits des personnes concernées

51. Les principaux droits des patients à respecter sont notamment :

- le droit à la transparence ;
- le droit d'accès ;
- le droit à la rectification ;
- le droit à « l'oubli » ;
- le droit à la limitation du traitement ;
- le droit à la portabilité ;
- le droit d'opposition.

52. Chaque utilisateur responsable d'un traitement de données à caractère personnel s'engage à mettre en place, en interne, l'ensemble des moyens humains et techniques permettant d'assurer de façon effective le respect des droits des patients.

8.1 Droit d'accès du patient

53. Dans ce cadre, chaque utilisateur, responsable d'un traitement de données à caractère personnel, s'engage à mettre en place ou à vérifier la présence, en interne, d'une cellule ou d'un service composé d'une ou plusieurs personnes membres du personnel qui auront en charge de répondre aux demandes d'accès des patients.

54. Ce service de gestion des droits d'accès assure la communication des données à caractère personnel à la personne concernée ayant fait une telle demande dans le respect de la procédure de gestion des droits d'accès mise en œuvre par le LBM concernant :

- la vérification de l'identité du demandeur ;
- la personne du LBM en charge de répondre aux demandes ;
- les délais de réponse, étant précisé que l'accès aux données de santé du patient datant de moins de cinq ans doit être mise en œuvre au plus tard dans les huit jours suivant la demande et au plus tôt après qu'un délai de réflexion de quarante-huit heures aura été observé[16] ;
- la liste des documents et des informations susceptibles d'être communiqués ;
- les modalités d'accès (consultation sur place ou envoi du dossier, selon la décision du patient).

8.2 Droit de rectification et droit à l'effacement

55. L'utilisateur s'engage à prendre en compte les demandes émanant de patients concernant la rectification ou la complétude de leurs données lorsque celles-ci sont inexactes ou incomplètes[17].

56. L'utilisateur doit également tenir compte des demandes de patients concernant l'effacement de leurs données, lorsque celles-ci ne sont plus nécessaires au regard des finalités pour lesquelles le LBM les a collectées ou traitées (ex. données présentes dans un serveur de résultat BIOSERVEUR)[18]. A ce titre, ces données peuvent devoir être conservées sur un support distinct conformément aux obligations de conservation du LBM.

57. Un service de gestion de ces droits assure le traitement des demandes de rectification et d'effacement dans le respect de la procédure de suppression des données mise à disposition par le LBM.

8.3 Droit à la limitation et d'opposition au traitement

58. L'utilisateur s'engage à prendre en compte les demandes de patients à la limitation du traitement. Cette demande peut être réalisée dans les cas suivants :

[16] CSP, art. L. 1111-7
[17] RGPD, art. 16
[18] RGPD, art. 17

- le patient conteste l'exactitude des données à caractère personnel traitées par le LBM ;

- le traitement mis en œuvre par le LBM est illicite ;

- la conservation des données n'est plus nécessaires mais ces données sont nécessaires au patient pour la constatation, l'exercice ou la défense de droits en justice ;

- le patient s'est opposé au traitement pendant la vérification de la balance des intérêts entre le responsable du traitement et ceux du patient, en particulier, lorsque le traitement est fondé sur les intérêts légitimes du LBM[19].

59. De plus, le patient peut s'opposer, pour des motifs légitimes, aux traitements mis en œuvre par le LBM lorsqu'ils sont fondés sur l'intérêt légitime du LBM ou nécessaires à l'exécution d'une mission d'intérêt public.

60. Un service de gestion de ces droits assure le traitement des demandes de limitation et d'opposition au traitement dans le respect de la procédure de gestion des droits mise à disposition par le LBM.

8.4 Droit à la portabilité des données

61. L'utilisateur s'engage à prendre compte les demandes de portabilité des données des patients dans l'hypothèse où le LBM met en œuvre un traitement :

- fondé sur une des bases légales suivantes :
  - le recueil du consentement du patient (recherche) ;
  - l'exécution d'un contrat auquel le patient est partie.

- effectué à l'aide de procédés automatisés.

62. Un service de gestion de ces droits assure le traitement des demandes de portabilité des données dans le respect de la procédure de gestion des droits mise à disposition par le LBM.

8.5 Droit de définir des directives sur le sort des données

63. L'utilisateur s'engage à prendre en compte toute demande de patients concernant des directives sur le sort de leurs données après le décès.

64. Un service de gestion de ce droit assure le traitement de ces demandes dans le respect de la procédure mise à disposition par le LBM.

9 Flux transfrontières

65. Les flux transfrontières vers l'Union européenne ou hors de l'Union européenne doivent être communiqués au responsable du LBM en respectant un préavis minimum de six mois[20] avant toute mise en œuvre.

[19] RGPD, art. 6.1.f)

[20] A confirmer

10 Traitement en tant que sous-traitant

66. Lorsque le LBM procède au traitement de données à caractère personnel en tant que sous-traitant (ex. réalisation d'examens de biologie médicale pour le compte d'un autre laboratoire), les règles issues de la présente charte s'appliquent.

11 Evolution

67. La présente charte pourra évoluer en fonction du contexte légal et réglementaire et de la doctrine de la Cnil.

68. Les éventuelles modifications seront portées à la connaissance des utilisateurs et entreront en vigueur un mois à compter de leur mise à disposition par voie d'affichage.

12 Contrôle et audit

69.Le respect des stipulations de la présente charte pourra faire l'objet d'opérations de contrôle et d'audit par le LBM auprès des utilisateurs.

70.L'utilisateur s'engage à collaborer dans le cadre des opérations de contrôle et d'audit qui pourraient être menées par le LBM afin de vérifier le respect des stipulations de la présente charte.

13 Portée et opposabilité

71. La présente charte constitue des lignes directrices pour les utilisateurs. Elle rappelle aux utilisateurs les grands principes et les principales obligations en matière de protection des données.

72. Les utilisateurs sont supposés en avoir pris connaissance avant toute mise en œuvre d'un traitement de données à caractère personnel.

14 Entrée en vigueur

73. La charte entrera en vigueur le 1er FEVRIER 2019.