

Comité de sécurité de l'information Chambre sécurité sociale et santé

CSI/CSSS/22/480

DÉLIBÉRATION N° 22/268 DU 12 SEPTEMBRE 2022 RELATIVE À LA MÉTHODE GÉNÉRIQUE D'ÉCHANGE DE DONNÉES À CARACTÈRE PERSONNEL RELATIVES À LA SANTÉ DANS LE CADRE DE BE-HERA

Le Comité de sécurité de l'information, chambre sécurité sociale et santé (dénommé ci-après le « comité »),

Vu la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale*, en particulier l'article 15, § 1^{er} ;

Vu le 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 relatif à la protection des données ou RGPD);

Vu la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel* ;

Vu la loi du 3 décembre 2017 *relative à la création de l'Autorité de protection des données*, en particulier l'article 114, modifié par la loi du 25 mai 2018 ;

Vu la loi du 5 septembre 2018 *instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en œuvre du 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* ;

Vu la loi du 13 décembre 2006 portant dispositions diverses en matière de santé, notamment l'article 42, §2, 3°;

Vu la loi du 21 août 2008 *relative à l'institution et à l'organisation de la plate-forme eHealth*, notamment l'article 11;

Vu la demande de Sciensano visant à obtenir une autorisation;

Vu le rapport d'auditorat de la Plate-forme eHealth ;

Vu le rapport de monsieur Bart Viaene.

Émet, après délibération, la décision suivante, le 12 septembre 2022 :

A. OBJET DE LA DEMANDE

1. Sciensano est une institution scientifique de l'Etat fédéral belge, qui a été créée par la loi du 25 février 2018 portant création de Sciensano (I). Elle a pour principale mission de réaliser des études scientifiques en vue de soutenir la politique de la santé. Sciensano fournit également une expertise et des services d'intérêt public dans le domaine de la santé publique.
2. En réaction à la pandémie de SARS-CoV-2, la Commission européenne a créé l'Autorité européenne de préparation et de réaction en cas d'urgence sanitaire (EU-HERA). Son objectif est de renforcer l'Union européenne de la santé, en améliorant notamment la préparation et la réaction aux futures épidémies (pandémies) nationales et internationales de maladies infectieuses. Le projet HERA-Incubator a été lancé par HERA en 2021, et le volet belge de ce projet permet de développer une infrastructure nationale pour la collecte de données de séquençage haut-débit (HTS), en particulier des données de séquençage du génome entier (WGS), ainsi qu'une infrastructure durable dans laquelle les données génomiques peuvent être traitées de manière harmonisée et couplées à des données cliniques et épidémiologiques.

La collecte centralisée de données génomiques ainsi que le couplage à des données cliniques et épidémiologiques permettent de détecter en temps utile et avec précision les variantes et/ou les épidémies. Par ailleurs, le projet répond aussi au traitement transactionnel de gros volumes de données en cas de grande épidémie ou pandémie. L'infrastructure envisagée, dénommée Be-HERA, pourra donc être utilisée plus largement pour anticiper les épidémies de maladies infectieuses et gérer les risques qui y sont liés.

Déjà dans le contexte de l'épidémie de coronavirus SARS-CoV-2, il existe une infrastructure de collecte de données auprès de Sciensano pour limiter la propagation et renforcer le contrôle du SARS-CoV-2¹. L'utilisation des composants actuels de cette infrastructure SARS-CoV-2 et leur extension à la collecte de données génomiques, cliniques et épidémiologiques de maladies infectieuses, de manière standardisée, permet de renforcer le paysage belge de la santé en ligne, conformément aux objectifs des programmes HERA et HERA-Incubator de l'UE. À cet effet, le but est a) d'honorer les accords fixés dans les plans d'action eSanté interfédéraux précédents (notamment au niveau des standards terminologiques et techniques et de la collecte des données dans les systèmes sources des prestataires de soins), b) d'éviter la fragmentation et la duplication des (flux de) données par différents systèmes et c) de limiter la charge d'enregistrement pour les prestataires de soins.

Sciensano soumet maintenant à l'approbation du Comité de sécurité de l'information la demande de mise en œuvre de la méthode générique décrite ci-après en vue de la collecte, de la gestion et de la communication de données à caractère personnel relatives à la santé dans

¹ Voir la délibération n° 20/132 du 3 mai 2020, modifiée le 13 mai 2020, le 2 juin 2020, le 7 juillet 2020, le 31 juillet 2020, le 3 novembre 2020 et le 30 mars 2021, relative à la communication de données à caractère personnel par divers prestataires de soins ou organisations actives dans le domaine de la santé ou des soins à Sciensano et à leur communication ultérieure dans le cadre de la lutte contre la propagation du coronavirus SARS-CoV-2.

le cadre de Be-HERA. En ce qui concerne les projets qui souhaitent avoir recours à cette méthodique (ou à des composants de celle-ci), des demandes d'autorisation de la communication de données à caractère personnel spécifiques au projet devront être introduites auprès du Comité de sécurité de l'information.

3. Les objectifs de l'architecture Be-HERA sont les suivants:
 - Collecte et traitement centraux standards de données épidémiologiques, cliniques et génomiques en rapport avec des maladies infectieuses
 - Couplage de données épidémiologiques, cliniques et génomiques en rapport avec des maladies infectieuses
 - Pérennisation de l'infrastructure du SARS-CoV-2 pour faire face à d'autres maladies infectieuses
 - Préparation générale et amélioration de la réaction en cas d'épidémies ou de pandémies de maladies infectieuses.

4. Différents acteurs sont impliqués dans le projet Be-HERA en tant que fournisseur de données, destinataire de données ou de prestataire de service technique. Il s'agit à cet égard des acteurs suivants:
 - Le patient ou le citoyen qui, par le biais des plateformes telles HD4PAT (HealthData for Patient) ou des applications sur www.masante.be, après authentification par le Federal Authentication Service (FAS) du SPF BOSA, est en mesure de partager des données nominatives (p.ex. *résultats d'autotests, contacts à haut risque*) avec les autorités sanitaires qui possèdent un mandat juridique pour gérer les crises sanitaires. L'usage effectif de ces plateformes de patients dépendra des besoins pendant une pandémie et sera, si nécessaire, régulé au moyen d'instruments juridiques appropriés.
 - Les laboratoires de biologie clinique: exécution d'examens de routine et/ou spécialisés pour la biologie clinique, à savoir des tests de laboratoire sur des échantillons cliniques afin d'obtenir des informations relatives à la santé d'un patient et pour appuyer le diagnostic, le traitement et la prévention de maladies infectieuses. En ce qui concerne la survenance de maladies infectieuses, un suivi a lieu depuis 1983 par un réseau de laboratoires (EPILABO²). Dans le cadre du suivi EPILABO, coordonné par Sciensano, les laboratoires vigies partagent volontairement des données, dans le but de surveiller la situation épidémiologique de maladies infectieuses à l'appui de différentes autorités sanitaires régionales, nationales et internationales. Dans le cadre de l'épidémie de coronavirus SARS-CoV-2³, un transfert de données obligatoire au départ de ces laboratoires a lieu vis-à-vis de Sciensano, afin de limiter la propagation et de renforcer la lutte contre le SARS-CoV-

² Voir aussi: Délibération n° 17/ 010 du 21 février 2017, modifiée le 18 juillet 2017, portant sur la collecte et la mise à la disposition de données à caractère personnel codées relatives à la santé via la plateforme Healthdata dans le cadre du suivi de maladies infectieuses par un réseau de laboratoires (EPILABO)

³ Art. 6 de l'accord de coopération du 25 août 2020 conclu entre l'Etat fédéral, la Communauté flamande, la Région wallonne, la Communauté germanophone et la Commission communautaire commune concernant le traitement conjoint de données par Sciensano et les centres de contact désignés par les autorités régionales compétentes ou par les agences compétentes, par les inspections sanitaires et par les équipes mobiles dans le cadre d'un suivi des contacts auprès des personnes (présumées) infectées par le coronavirus SARS-CoV-2 sur la base d'une base de données auprès de Sciensano

2. Le but est que l'architecture Be-HERA puisse être utilisée par des laboratoires de biologie clinique en tant que fournisseurs de données pour la collecte de données EPILABO volontaire actuelle ainsi que pour les collectes de données obligatoires dans le cadre de maladies à déclaration obligatoire ou de pandémies.

- Les centres nationaux de référence en microbiologie humaine (CNR⁴): un réseau belge de 41 CNR se porte garant pour l'expertise, le diagnostic et la surveillance d'un ensemble d'agents pathogènes importants pour la santé publique. Tout CNR se compose d'un ou de plusieurs laboratoires de biologie clinique et est désigné comme tel pour un seul agent pathogène ou un groupe d'agents pathogènes. Les CNR existent tant au sein qu'en dehors de Sciensano. La coordination de ce réseau appartient au service Epidémiologie des maladies infectieuses de Sciensano. Les données traitées par les CNR contribuent à la confirmation et/ou au diagnostic des agents pathogènes dans les échantillons cliniques envoyés par les laboratoires cliniques périphériques et/ou des prestataires de soins ambulatoires et servent à caractériser les souches (p.ex. génotypage, examen des antigènes, étude de la résistance aux antibiotiques). Les données provenant des tests microbiologiques et génomiques réalisés constituent un complément important aux données cliniques/épidémiologiques dans le cadre d'une surveillance accrue des (nouvelles) souches émergentes et/ou circulantes. Dans les objectifs de Be-HERA, ces centres fournissent des données nominatives qui peuvent être utilisées par d'autres laboratoires et administrations sanitaires. Après pseudonymisation par une Tierce partie de confiance (TTP), ces données pourront aussi être partagées avec le service Epidémiologie des maladies infectieuses.
- Les prestataires de soins ambulatoires (p.ex. médecins généralistes): exercice des soins de santé. Dans le cadre de l'épidémie de coronavirus SARS-CoV-2, un transfert obligatoire de données par certains prestataires de soins ambulatoires (notamment les médecins généralistes et les pharmaciens) à Sciensano a lieu afin de limiter la propagation et de renforcer la lutte contre le SARS-CoV-2 (cf. accord de coopération du 25 août 2020 mentionné en note de bas de page 3). En ce qui concerne les maladies infectieuses, des données nominatives, par exemple liées à des prescriptions pour des tests ou le diagnostic, peuvent aussi être fournies par les prestataires de soins ambulatoires si le cadre réglementaire le prévoit.
- Les autorités sanitaires des Etats fédérés (Agentschap Zorg & Gezondheid (AZG), Agence Wallonne pour une Vie de Qualité (AViQ), Commission communautaire commune (GGC), Ministère de la Communauté germanophone): organisations publiques responsables du traçage des contacts, de la détection de clusters au sein des collectivités ou d'autres initiatives visant à lutter contre la propagation des infections. À cet effet, ils ont besoin de recevoir des données nominatives relatives à la propagation des maladies infectieuses. L'infrastructure Be-HERA entend harmoniser, dans un souci d'efficacité, le transfert de ces données aux administrations sanitaires des entités fédérées.
- Service healthdata.be (HD) de Sciensano: fournisseur de services techniques permettant de faciliter les collectes de données sécurisées, de structurer les données, de conserver les données, de transférer et de rapporter des données liées à des projets

⁴ Pour plus d'informations concernant les CNR et le rôle de Sciensano: voir l'arrêté royal du 9 février 2011 fixant les conditions de financement des centres de référence en microbiologie humaine

scientifiques et/ou d'appui à la politique en matière de (soins de) santé. Healthdata.be fournira au sein de l'infrastructure Be-HERA, des instruments pour une collecte de données sécurisée auprès de fournisseurs de données (*p.ex. laboratoires cliniques, CNR, prestataires de soins ambulatoires, gestionnaires de sources authentiques*) et une mise à la disposition de ces données, sous forme nominative ou pseudonymisée, en fonction du mandat du destinataire des données.

- Service Epidémiologie des maladies infectieuses de Sciensano: décrit et suit les tendances épidémiologiques des maladies infectieuses sur la base de données pseudonymisées collectées auprès de différentes sources, notamment des réseaux de médecins généralistes, de laboratoires cliniques, de CNR, d'hôpitaux et de microbiologistes. L'interprétation de ces données permet de déterminer l'impact de ces maladies sur la santé publique, par exemple en termes d'incidence et de mortalité. Grâce aux connaissances relatives aux maladies infectieuses dont dispose le service Epidémiologie des maladies infectieuses et qui sont fournies par lui, les autorités sanitaires peuvent prendre des décisions fondées sur le plan scientifique, à titre de prévention ainsi que pendant des problèmes ou crises sanitaires urgentes. Cet appui est offert tant au niveau local qu'au niveau régional, national et international suite à un contact avec différentes autorités sanitaires. Le service publie également, sur les portails publics, des données agrégées relatives aux tendances des maladies infectieuses. Conformément aux objectifs, à la finalité et à la proportionnalité, le service Epidémiologie des maladies infectieuses (Sciensano) reçoit des données pseudonymisées de Be-HERA.
- Le service Activités transversales en génomique appliquée de Sciensano : développe et implémente des applications de la biologie moléculaire et des bio-informatiques pour les différents services de Sciensano. Dans le domaine des maladies infectieuses, il s'agit de la détection moléculaire et de l'identification d'agents pathogènes par le recours aux techniques de laboratoire les plus adéquats et avancés, à la biotechnologie, plus précisément le recours au séquençage à haut débit et à la méthodologie bio-informatique pour les analyses de données génomiques. Ces activités ont lieu, à titre de routine, pour les laboratoires cliniques et/ou les CNR au sein de Sciensano, mais aussi à un niveau scientifique au sein de différents projets de recherche nationaux et internationaux. Le service Activités transversales en génomique appliquée (Sciensano) est, au sein de l'architecture de Be-HERA, un destinataire de données non nominatives, génomiques et génomiques-techniques. Il partagera les résultats des analyses génomiques avec les CNR et le service Epidémiologie des maladies infectieuses.
- La Plate-forme eHealth: fournisseur de certains services techniques de base pour Be-HERA tels une eHealthbox qui facilite les transferts de données chiffrés, la Trusted Third Party (TTP) pour la pseudonymisation de données à caractère personnel et l'intégration dans des sources authentiques, notamment le registre national et CoBRHA. La Plate-forme eHealth reçoit comme TTP des données nominatives de certains composants et fournit des données pseudonymisées à d'autres composants au sein de Be-HERA.
- Les gestionnaires de certaines sources authentiques ou de banques de données externes: si légitimé et requis pour la gestion de crise d'une pandémie déterminée, les gestionnaires de certaines sources authentiques (*p.ex. le Registre national, CoBRHA*) ou les banques de données externes (*p.ex. Vaccinnet, banque de données Résumés*)

Hospitaliers Minimums, banques de données de l'AIM) peuvent être invités à fournir des données pour des finalités telles le traçage efficace des contacts, l'évaluation des mesures politiques, des statistiques précises, la surveillance épidémiologique, l'étude scientifique, etc.

- Les autorités sanitaires internationales (OMS, CEPCM, etc.): en vue du soutien des autorités sanitaires européennes et internationales, des données pseudonymisées ou anonymes sont échangées avec par exemple le Centre européen de Prévention et de Contrôle des Maladies (CEPCM) et l'Organisation mondiale de la santé (OMS) dans le cadre du monitoring international des maladies infectieuses.
- D'autres destinataires autorisés: en fonction du projet et/ou de la situation (p.ex. pandémie), sur la base des collections de données au sein de l'architecture Be-HERA, moyennant le cadre juridique adéquat, des données à caractère personnel peuvent être échangées avec les acteurs mandatés qui assument un rôle au niveau de la gestion des soins de santé et/ou de la gestion de crise (par exemple, l'INAMI, le SPF Santé publique, l'AFMPS, le Collège intermutualiste national, ...). Le mandat juridique du destinataire final déterminera s'il s'agit de données nominatives, pseudonymisées, individuelles ou agrégées.
- Le public général/la société: afin de fournir des informations relatives aux tendances des maladies infectieuses, un ensemble limité de données agrégées sera rendu disponible sur les portails publics.

5. Be-HERA comprend différents traitements de données à caractère personnel pour lesquels, en fonction de la finalité et du sous-traitant, soit des données à caractère personnel nominatives, soit des données à caractère personnel pseudonymisées sont traitées. Les données ont, d'une part, trait à des personnes ayant un diagnostic supposé ou confirmé lié à un agent pathogène, éventuellement à leur médecin traitant. Outre des données individuelles de tests positifs détectant l'agent pathogène, des données individuelles de tests négatifs peuvent, si cela s'avère pertinent et proportionnel, aussi être partagées moyennant autorisation par un cadre réglementaire. D'autre part, des données à caractère personnel nominatives ou pseudonymisées de médecins traitants des patients concernés peuvent aussi être collectées. Les droits d'accès à certaines données sont différenciés sur la base des besoins par acteur avec une attention particulière pour la proportionnalité et le principe du Trusted Third Party. Ce principe implique que le type de données suivant ne peut jamais être présent dans le même environnement et être disponible pour les mêmes acteurs:

- l'ID d'une personne concernée, à savoir une personne avec un diagnostic supposé ou confirmé lié à l'agent pathogène X
- les données business liées à la personne concernée, à savoir les données démographiques et les données relatives à la santé
- le pseudoID de la personne concernée

Par exemple :

- ID (p.ex. un numéro NISS) et les données business sont disponibles pour les prestataires de soins ou l'établissement de soins, le pseudoID ne peut pas être disponible pour eux
- l'ID & le PseudoID peuvent être disponibles pour la Trusted Third Party (eHealth), mais non les données business

- Le pseudoID & les données business, mais non l'ID, peuvent être disponibles pour le chercheur.

Par conséquent, plusieurs environnements techniques séparés ayant chacun une gestion des utilisateurs adéquate sur la base de rôles et de séparations de fonction sont cruciaux.

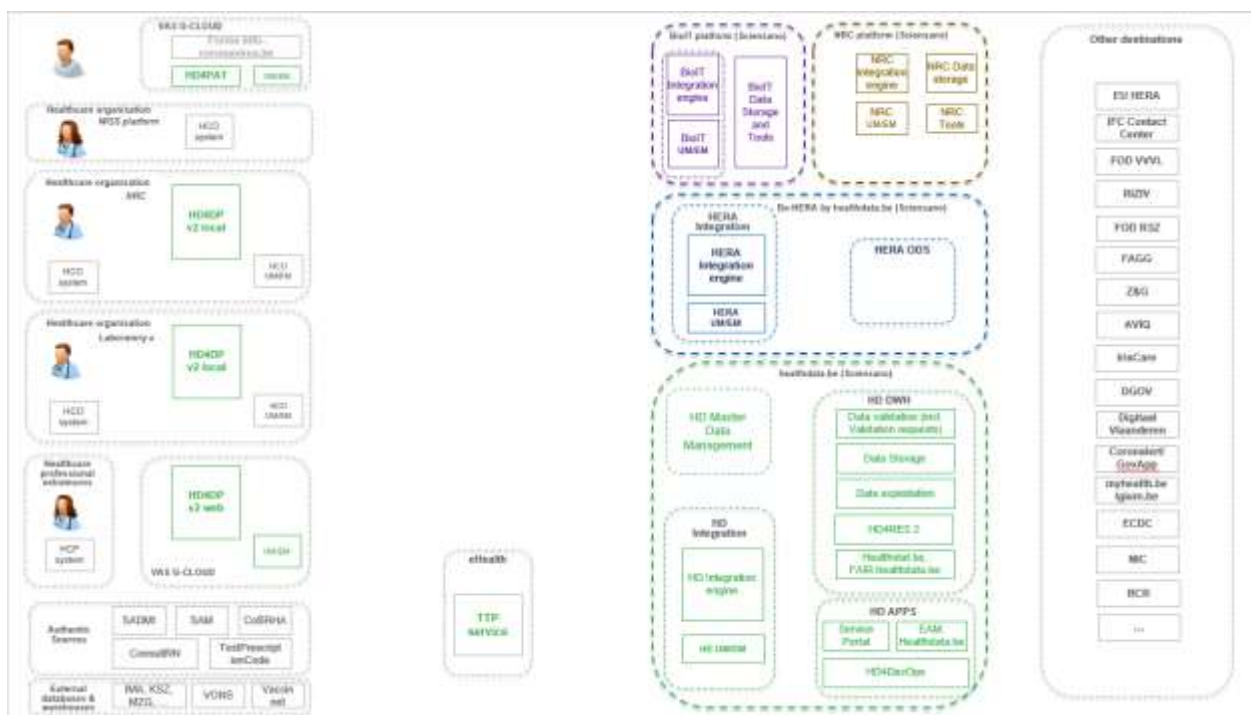
6. Au sein de l'architecture Be-HERA qui comprend plusieurs composants, le type de traitement et le type de données déterminent l'infrastructure IT et les applications IT. Par exemple :
 - Volume (la quantité de données générées et enregistrées): pour certaines finalités qui font appel à la collecte des données via Be-HERA, il sera fait appel à des fichiers de données génomiques bruts. Il s'agit de fichiers qui constituent le résultat du séquençage haut-débit du matériel génétique, i.e. génome, d'un agent pathogène et/ou de leur traitement bio-informatique. Le séquençage parallèle de masse permet de lire la séquence brute du génome en parties, ce qui permet d'obtenir une séquence consensus globale du génome après traitement bio-informatique. Ces fichiers de données génomiques sont très grands et nécessitent d'autres matériels et logiciels informatiques pour traiter ce type de données volumineuses, en comparaison avec les données qui sont extraites du *laboratory management information system* (LIMS) et/ou des systèmes Electronic Health Record. Les fichiers de données génomiques bruts conviennent moins à un enregistrement et à un traitement dans des banques de données classiques dans des centres de données traditionnels. Pour cette raison, certains composants de l'architecture Be-HERA nécessitent des solutions basées sur le cloud. Cela permet également de concevoir des solutions évolutives, de sorte qu'en cas d'épidémie, elles puissent être étendues rapidement si nécessaire.
 - Velocity (vitesse à laquelle les données sont générées et traitées afin de satisfaire à la demande en matière d'usage de données). La vitesse de systèmes transactionnels, c'est-à-dire de systèmes qui transfèrent principalement des données entre le point a et le(s) point(s) b-z, est sensiblement supérieure à celle des plateformes analytiques (telles les *data warehouses*, les *data lakes*, etc.). Ils ont tous leurs propres besoins, standards et approches en matière de matériels et de logiciels informatiques.
7. L'objectif de l'architecture Be-HERA est d'éviter la duplication de la conservation des données et des activités business. Chaque plateforme au sein de l'architecture Be-HERA a ses propres gestionnaires, utilisateurs, finalités et fonctionnalités. Ce sont les finalités et les fonctionnalités qui déterminent si les données ne sont pas conservées, sont conservées pendant une brève période ou une longue période. La figure à l'annexe 1 de la présente délibération illustre les plateformes et les principes en matière de Trusted Third Party, de types de données différenciés, et pour éviter les duplications et les structures de gestion propres par plateforme.
8. La demande a trait au projet d'architecture pour Be-HERA. Cette architecture se compose des éléments suivants :
 - a) élément laboratoires biologique clinique
 - b) élément CNR
 - c) Plateforme WGS
 - d) Plateforme technique Be-HERA
 - e) Plateforme BioIT

- f) plateforme CNR
- g) plate-forme eHealth
- h) healthdata.be intégration
- i) healthdata.be datawarehouse
- j) outils pour des transferts sécurisés à d'autres destinataires

Seront ensuite décrits, par composant, le propriétaire, le type de données, l'infrastructure et les activités. Pour la description des composants et des flux de données, l'accent est mis sur les composants et les flux qui sont déjà utilisés en période non pandémique et qui nécessitent une autorisation pour les phases de développement et de tests de l'architecture Be-HERA.

D'autres composants tels le composant pour l'input des patients, le composant pour les acteurs de soins ambulatoires et le composant banques de données externes ne sont, pour l'instant, pas pris en considération. Cependant, moyennant les autorisations requises au niveau du projet et/ou sur la base des besoins pendant une pandémie, il peut y être fait appel. En ce qui concerne les sources authentiques, Be-HERA souhaite, d'emblée, pouvoir faire appel au registre national (via le service ConsultRN de eHealth) et à CoBRHA car ces sources joueront un rôle important dans l'ensemble des projets dans le cadre du traitement de données à caractère personnel exactes relatives aux personnes concernées mentionnées au point 5. Pour l'utilisation du Registre national, une autorisation sera demandée au Ministre de l'Intérieur. Puisque Be-HERA sera également confrontée à des personnes qui ne sont pas inscrites au registre national ou dont toutes les données à caractère personnel nécessaires ne sont pas systématiquement mises à jour dans le registre national, elle demande, pour la même finalité, un accès aux mêmes données à caractère personnel dans les registres Banque Carrefour, visés à l'article 4 de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale, pour autant que ces données soient disponibles. D'autres sources authentiques seront considérées comme spécifiques au projet et soumises à l'approbation du Comité de sécurité de l'information, chambre sécurité sociale et santé, dans le cadre de demandes d'autorisation spécifiques au projet.

9. Aperçu high level des composants du paysage Be-HERA:



- a) Composant laboratoires de biologie clinique (propriétaire = HealthCare Organisation (HCO): Laboratoires de biologie clinique): des tests de laboratoire sont exécutés sur des échantillons cliniques pour obtenir des informations relatives à la santé d'un patient et soutenir le diagnostic, le traitement et la prévention de maladies infectieuses. Ce composant contient les éléments suivants:
- i. système HCO: Laboratory Management Information System (LMIS)
 - ii. HD4DP v2 (HealthData for Data Provider version 2) Local: Une application locale fournie par healthdata.be (Sciensano) afin de faciliter la détermination (automatique ou manuelle) et le transfert de données
 - iii. HCO UM/EM⁵: une application de messagerie pour un transfert sécurisé (chiffré) de données de HCO vers d'autres parties (telles que healthdata.be) à l'aide de la eHealthBox et du service eHealth Trusted Third Party (pseudonymisation d'ID)
- b) Composant laboratoires nationaux de référence (propriétaire = HCO: Centre national de référence en microbiologie humaine (CNR)): des tests de laboratoire sont exécutés sur des échantillons cliniques pour obtenir des informations relatives à la santé d'un patient et soutenir le diagnostic, le traitement et la prévention de maladies. Plus précisément: les analyses primaires de biologie clinique de laboratoires sont validés. D'autres actions sont notamment: analyses sur l'agent pathogène concerné, sous-typages d'agents pathogènes, tests de résistance et autres. Ce composant contient les éléments suivants:
- i. système HCO: Laboratory Management Information System (LMIS)

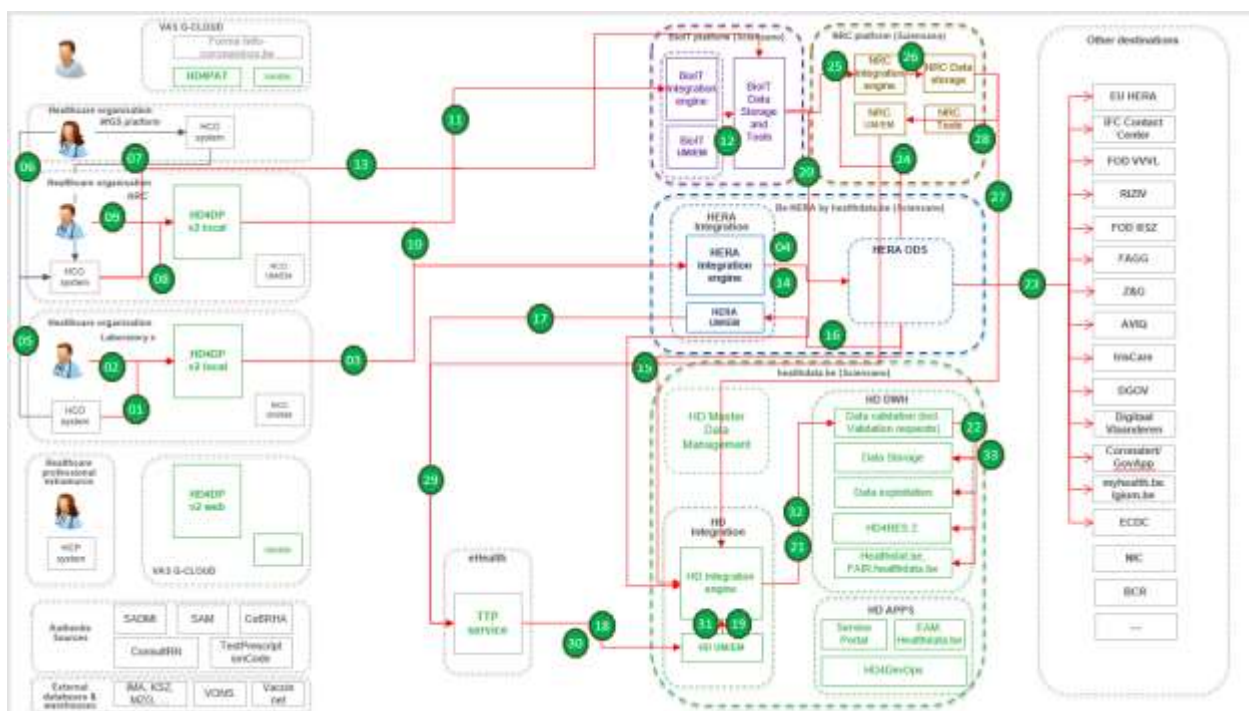
⁵ Dans la figure et la description du flux de données, UM est l'abréviation de Unified Messaging et EM de Encryption Module.

- ii. HD4DP v2 (HealthData for Data Provider version 2) Local: Une application locale fournie par healthdata.be (Sciensano) afin de faciliter la détermination (automatique ou manuelle) et le transfert de données
 - iii. HCO UM/EM: une application de messagerie pour un transfert sécurisé (chiffré) de données de HCO vers d'autres parties (telles que healthdata.be) à l'aide de la eHealthBox et du service eHealth Trusted Third Party (pseudonymisation d'ID)
- c) Plateforme WGS (Whole Genome Sequencing) (propriétaire= HCO: Plateforme WGS) : plateforme pour la réalisation d'un séquençage haut-débit d'échantillons cliniques. Les résultats du séquençage parallèle massif comprennent la lecture du matériel génétique, c'est-à-dire le génome, d'un agent pathogène sous la forme de plusieurs morceaux bruts de séquence et, éventuellement, à titre complémentaire, par traitement bio-informatique, sous la forme d'une séquence consensus globale ou de résultats d'interprétation génomique spécifiques basés sur la ou les séquences, c'est-à-dire les indicateurs génomiques. Une plateforme WGS fournit des données génomiques (brutes) de séquençage à des laboratoires de biologie clinique ou des CNR. Cette plateforme peut se situer dans le laboratoire même mais cela n'est pas indispensable (il est possible de faire appel à un sous-traitant). Ce composant contient l'élément suivant:
- i. système HCO: système local dans lequel sont conservées des données relatives aux échantillons et des données génomiques (brutes)
- d) Plateforme technique Be-HERA (propriétaire = organe interfédéral à déterminer): transmission de données nominatives aux personnes concernées. Ce composant contient les éléments suivants:
- i. moteur d'intégration HERA: moteur d'interface indépendant de la plate-forme permettant la gestion des informations par la transmission bidirectionnelle de nombreux types de messages
 - ii. HERA Operational Data Store (ODS): plateforme pour la collecte de données issues de plusieurs sources, organisées pour la distribution, le partage et les sous-ensembles et le partage
 - iii. HCO UM/EM: une application de messagerie pour un transfert sécurisé (chiffré) de données de HCO vers d'autres parties (telles que healthdata.be) à l'aide de la eHealthBox et du service eHealth Trusted Third Party (pseudonymisation d'ID)
- e) Plateforme BioIT (propriétaire = service Activités transversales en génomique appliquée (Sciensano)): plateforme pour l'analyse de données de séquençage (WGS). Ce composant contient les éléments suivants:
- i. moteur d'intégration BioIT : moteur d'interface indépendant de la plate-forme permettant la gestion des informations par la transmission bidirectionnelle de nombreux types de messages
 - ii. BioIT UM/EM: une application de messagerie pour un transfert sécurisé (chiffré) de données de HCO vers d'autres parties (telles que healthdata.be) à l'aide de la eHealthBox et du service eHealth Trusted Third Party (pseudonymisation d'ID)
 - iii. BioIT Data Storage et Tools (avec l'aide de Azure services)
- f) Plateforme CNR: plateforme pour la validation des résultats après traitement de fichiers de données génomiques (bruts) par la plateforme BioIT, en vue du couplage de données

- génomiques à des données épidémiologiques cliniques et de l'interprétation et de l'exécution d'analyses spécifiques liées au couplage de données telles le typage, les tests de résistance, les analyses de clusters, e. a. Ce composant contient les éléments suivants:
- i. moteur d'intégration CNR: moteur d'interface indépendant de la plate-forme permettant la gestion des informations par la transmission bidirectionnelle de nombreux types de messages
 - ii. CNR UM/EM: une application de messagerie pour un transfert sécurisé (chiffré) de données de HCO vers d'autres parties (telles que healthdata.be) à l'aide de la eHealthBox et du service eHealth Trusted Third Party (pseudonymisation d'ID)
 - iii. CNR enregistrement de données: Technologie SQL
- g) plate-forme eHealth (propriétaire = plate-forme eHealth): La plate-forme eHealth offre plusieurs services de base auxquels tous les acteurs de soins et leurs prestataires de services informatiques peuvent faire appel pour développer des services en ligne ou ouvrir des sources authentiques validées. Il peut être fait appel à ces services de base au moyen de l'infrastructure réseau actuelle. Ce composant contient les éléments suivants:
- i. TTP service : eHealth Platform
- h) intégration healthdata.be (propriétaire = HD Comité d'accompagnement, HD comité de pilotage, services fournis healthdata.be (Sciensano)): Couplage de données entrantes et séparation de données sortantes lorsque des services TTP s'avèrent nécessaires. Ce composant contient les éléments suivants:
- i. moteur d'intégration HD: moteur d'interface indépendant de la plate-forme permettant la gestion des informations par la transmission bidirectionnelle de nombreux types de messages
 - ii. HD UM/EM: une application de messagerie pour un transfert sécurisé (chiffré) de données de HCO vers d'autres parties (telles que healthdata.be) à l'aide de la eHealthBox et du service eHealth Trusted Third Party (pseudonymisation d'ID)
- i) datawarehouse healthdata.be (propriétaire = HD Comité d'accompagnement, HD comité de pilotage, services fournis healthdata.be (Sciensano)): Ce composant est responsable de la gestion des données, de l'analyse scientifique, de la visualisation des données (rapportage), e. a. Ce composant contient les éléments suivants:
- i. HD Data validation
 - ii. HD Data Storage
 - iii. HD Data Exploitation
 - iv. HD4RES v2 (HealthData for Researcher version 2): collecte de tables de données et visualisations relatives au monitoring de flux de données gérés par healthdata (Sciensano).
 - v. healthstat.be: application de visualisation de données de la plateforme healthdata.be.
 - vi. fair.healthdata.be : application open data de la plateforme healthdata.be
- j) outils pour transferts sécurisés à d'autres destinataires de données HERA telles les autorités sanitaires régionales, les administrations sanitaires fédérales, etc. En fonction du destinataire des données et de son mandat légal, le transfert des données sera répliqué de manière nominative, pseudonymisée, individuelle ou agrégée. Par acteur destinataire, la

méthode/l'outil de transfert crypté des données sera déterminé (par exemple, un serveur SFTP).

10. Les flux de données sont précisés au moyen de 33 flux.



- **Flux de données 1:** Le laboratoire (de biologie clinique) envoie des données à caractère personnel nominatives, des données de diagnostic et des données épidémiologiques cliniques dans un ou plusieurs messages selon le format HL7 FHIR standard. Ces données sont exportées à partir du système HCO local (LMIS) et dirigées vers le HD4DP v2 installé au niveau local au moyen d'une API (Application Programming Interface).
- **Flux de données 2:** Le personnel du laboratoire (de biologie clinique) peut fournir les données manuellement à l'aide de la version du formulaire des messages dans le flux de données 1 (étape facultative).
- **Flux de données 3:** Le HD4DP v2 installé localement envoie les messages (provenant du flux de données 1 ou 2) au moteur d'intégration HERA.
- **Flux de données 4:** Au départ du moteur d'intégration HERA, les messages (issus du flux de données 1 ou 2) sont transmis à HERA ODS.
- **Flux de données 5:** Pour des tests complémentaires concernant l'agent pathogène, le laboratoire (de biologie clinique) peut transmettre un échantillon, des données à caractère personnel nominatives, des données de diagnostic et des données cliniques

épidémiologiques au CNR en question. Si cela paraît souhaitable, les messages issus du flux de données 1 (ou 2) peuvent être utilisés à cet effet.

- **Flux de données 6:** si des analyses génomiques ont lieu, une plateforme WGS externe, c'est-à-dire non localisée dans le laboratoire du CNR, ou interne, c'est-à-dire localisée dans le laboratoire du CNR, peut être utilisée : le laboratoire CNR fournit l'échantillon et les données relatives à la demande à la plateforme WGS.
- **Flux de données 7:** Sont transmis au laboratoire CNR au départ de la plateforme WGS des fichiers de données génomiques (bruts) et des données génomiques techniques.
- **Flux de données 8:** Le CNR envoie des données à caractère personnel nominatives, des données de diagnostic et des données épidémiologiques cliniques dans un ou plusieurs messages selon le format HL7 FHIR standard. Ces données sont exportées à partir du système HCO local (LMIS) et dirigées vers le HD4DP v2 installé au niveau local au moyen d'une API (Application Programming Interface).
- **Flux de données 9:** Le personnel du CNR peut fournir les données manuellement à l'aide de la version du formulaire des messages dans le flux de données 8 (étape facultative).
- **Flux de données 10:** Le HD4DP v2 installé localement envoie les messages (provenant du flux de données 8 ou 9) au moteur d'intégration HERA.
- **Flux de données 11:** Le CNR envoie des informations structurées complémentaires, à caractère technique et génomique, requises pour l'analyse de données génomiques (brutes) sur la plateforme BioIT, exportées à partir du système HCO local (LMIS) et transférées vers la HD4DP v2 installée au niveau local à l'aide d'une API (Application Programming Interface). Un CNR peut aussi transmettre les interprétations génomiques spécifiques, c'est-à-dire les indicateurs génomiques, par le traitement bio-informatique des séquences de génomes. Ces messages sont envoyés via HD4DP v2 au moteur d'intégration BioIT.
- **Flux de données 12:** Le moteur d'intégration BioIT envoie les messages (provenant du flux de données 11) à BioIT Data Storage and Tools.
- **Flux de données 13:** Le laboratoire CNR envoie des fichiers de données génomiques (bruts) en vue de leur traitement sur la plateforme BioIT.
- **Flux de données 14:** Le moteur d'intégration HERA transmet les messages du flux de données 10 à HERA ODS.
- **Flux de données 15:** HERA ODS envoie les messages au moteur d'intégration HD. Ce message contient une clé technique unique et des données business (pas de NISS du patient).

- **Flux de données 16:** HERA ODS envoie la clé technique unique et le NISS du patient repris dans les messages à HERA UM/EM. Ces messages ne contiennent pas de données business (= données démographiques et données relatives à la santé dont les variables exactes peuvent varier en fonction du projet qui a recours à l'architecture Be-HERA).
- **Flux de données 17:** HERA UM/EM envoie la clé technique unique et le NISS du patient repris dans les messages au service TTP de eHealth. Ces messages ne contiennent pas de données business.
- **Flux de données 18:** Le service TTP de eHealth envoie la clé technique unique et le PSEUDO-NISS du patient repris dans les messages à HD UM/EM. Ces messages ne contiennent pas de données business.
- **Flux de données 19:** HD UM/EM envoie la clé technique unique et le PSEUDO-NISS du patient repris dans les messages au moteur d'intégration HD. Ces messages ne contiennent pas de données business.
- **Flux de données 20:** La plateforme BioIT transmet les interprétations génomiques spécifiques, c'est-à-dire les indicateurs génomiques, par le traitement bio-informatique des séquences de génome, au moteur d'intégration HD.
- **Flux de données 21:** Le moteur d'intégration HD consolide la clé technique, le PSEUDO NISS et les données business de messages antérieurs et les transmet à l'environnement HD Staging (DWH HD).
- **Flux de données 22:** Poursuite du traitement de messages antérieurs dans le DWH HD, en ce compris la publication éventuelle sur healthstat.be (plateforme de visualisation publique contenant des données agrégées) et le portail fair.healthdata.be (open data platform).
- **Flux de données 23:** HERA ODS envoie des messages à des partenaires externes appropriés en vue du traçage de contacts et de la maîtrise de foyers à risques.
- **Flux de données 24:** HERA ODS envoie des informations pertinentes nécessaires à la détection de clusters d'agents pathogènes à la plateforme CNR.
- **Flux de données 25:** BioIT Data Storage and Tools envoie le résultat des analyses génomiques au moteur d'intégration CNR.
- **Flux de données 26:** Le moteur d'intégration CNR envoie les données du flux de données 25 au CNR Data storage.
- **Flux de données 27:** Le CNR Data Storage envoie les messages au moteur d'intégration HD. Ce message contient une clé technique unique et des données business (pas de NISS du patient).

- **Flux de données 28:** Le CNR Data Storage envoie la clé technique unique et le NISS du patient repris dans les messages au CNR UM / EM.
 - **Flux de données 29:** Le CNR UM/EM envoie une clé technique unique et le NISS du patient repris dans les messages au service TTP de eHealth. Ces messages ne contiennent pas de données business.
 - **Flux de données 30:** Le service TTP de eHealth envoie la clé technique unique et le PSEUDO-NISS du patient repris dans les messages au HD UM/EM. Ces messages ne contiennent pas de données business.
 - **Flux de données 31:** Le HD UM/EM envoie une clé technique unique et le PSEUDO-NISS du patient repris dans les messages au moteur d'intégration HD. Ces messages ne contiennent pas de données business.
 - **Flux de données 32:** Le moteur d'intégration HD consolide la clé technique, le PSEUDO-NISS et les données business de messages antérieurs et le résultat d'analyses génomiques et envoie celles-ci à l'environnement HD Staging (DWH HD).
 - **Flux de données 33:** Poursuite du traitement de messages antérieurs et résultat d'analyses génomiques sur le DWH HD, en ce compris la publication éventuelle sur healthstat.be (plateforme de visualisation publique contenant des données agrégées) et air.healthdata.be portal (open data platform).
11. En ce qui concerne la plateforme BioIT, la plateforme CNR, la plateforme technique Be-HeRA et l'environnement healthdata.be, une gestion des utilisateurs et des accès en cascade est installée, ce qui permet de garantir que seul un nombre limité de collaborateurs de Sciensano aura accès aux informations les plus sensibles. Ces collaborateurs sont tenus contractuellement de respecter strictement le secret professionnel par la signature d'un accord de confidentialité lors de l'entrée en service et de traiter les données d'une manière déontologique et éthique. Dans chaque environnement, des outils sont installés pour la surveillance et la protection de l'activité des données en temps réel. Ces outils permettent de créer des loggings qui enregistrent de manière permanente tout utilisateur, tout accès, toute période d'accès, toute activité et tout résultat de cette activité et les rendent consultables. Pour les transferts de données provenant de l'environnement, des données de transaction seront également conservées concernant la date et l'heure des transferts de données, le contenu du transfert et l'identification des destinataires.
12. Étant donné que plusieurs services internes de Sciensano sont impliqués par les différentes plateformes qui traitent à la fois des données à caractère personnel nominatives et des données pseudonymisées, une stricte séparation de fonctions s'avère indispensable. Sciensano a élaboré, à cet effet, une politique comprenant notamment les mesures suivantes:
- Il existe des procédures opérationnelles standard pour l'accès aux environnements où le rôle du demandeur est contrôlé par les gestionnaires d'actifs concernés et/ou le DPD sur

la base a) de l'organigramme de Sciensano avec ses départements/services distincts et b) des principes du « need to know ».

- Les droits d'accès aux environnements séparés sont fournis ad nominatem et sont vérifiables au moyen d'outils de gestion des accès utilisateur.
- Utilisation d'outils permettant la surveillance et la protection de l'activité des données. Il peut à cet égard être vérifié qui a eu accès à quelles données et à quel moment.
- Par ailleurs, outre ces possibilités de surveillance concernant l'accès aux données, des mesures sont prises pour éviter un partage de données illicite (p.ex. entre personnes avec des droits d'accès différents). Les collaborateurs des laboratoires de Sciensano, les chercheurs du service Epidémiologie et les collaborateurs de healthdata.be travaillent directement sur les serveurs des centres de données ou datawarehouses sous-jacents. Aucune donnée n'est stockée sur les ordinateurs locaux. Seul le développement d'applications ne contenant pas de données peut avoir lieu sur les ordinateurs locaux (client-based computing). L'accès aux environnements contenant des données a lieu par le biais de portails d'accès sécurisés. Les collaborateurs des laboratoires de Sciensano, les chercheurs du service Epidémiologie et les collaborateurs de healthdata.be ne sont pas en mesure de charger ou de télécharger des données nominatives ou des données pseudonymisées.
- Engagements de confidentialité pour tous les collaborateurs de Sciensano et disponibilité d'une politique d'intégrité interdisant les conflits d'intérêts.

13. Toute plateforme liée à l'architecture Be-HERA dispose de ses propres organes de gestion. Pour certains composants de l'architecture, les organes de gestion se trouvent provisoirement encore dans la phase d'exploration ou de développement.

- Plateforme BioIT: service Activités transversales en génomique appliquée (Sciensano)
- Plateforme CNR: gouvernance des données sera basée sur les mandats juridiques actuels pour les CNR et élaborée plus en détail à l'avenir
- Plateforme technique Be-HERA: la gouvernance interfédérale sera élaborée plus en détail, ceci se déroule actuellement par le biais du Comité interfédéral Testing et Tracing SARS-CoV-26 ou de son successeur se composant de représentants des ministres fédéraux et régionaux compétents pour la santé publique, de représentants des administrations sanitaires régionales et de représentants de la plate-forme eHealth et de Sciensano.
- Datawarehouse de healthdata.be: Healthdata.be est géré par un Comité d'accompagnement et un comité directeur. Le Comité d'accompagnement veille notamment à l'exécution correcte des missions de healthdata.be, à ses finances, aux priorités, au planning annuel, aux objectifs service level et aux rapports d'activités. Ce comité se compose de représentants de la Commission Soins médicaux, de l'INAMI, du SPF Santé publique, de l'AFMPS, de Sciensano, de la cellule politique du Ministre fédéral de la Santé publique, de l'AIM et des entités fédérées. Le comité directeur de healthdata.be évalue, notamment, les projets présentés qui peuvent éventuellement être réalisés par la plateforme healthdata.be. Il se compose du chef de projet de healthdata.be, de médecins indépendants (cliniciens), de médecins scientifiques, de médecins des organismes assureurs, d'experts en informatique médicale et de représentants des organisations de patients ainsi que de

⁶ Ce comité a été institué par la Conférence interministérielle Santé publique, voir <https://www.corona-tracking.info/wp-content/uploads/2020/05/IMC-20200429-oprichting-IC-TT.pdf>

représentants de l'INAMI, du SPF Santé publique, du KCE, de l'AFMPS et de la Plateforme eHealth et des communautés/régions.

Le Comité de sécurité de l'information, chambre sécurité sociale et santé, sera informé sur les développements futurs concernant ces organes de gestion.

- 14.** Les projets qui souhaitent avoir recours à l'architecture Be-HERA doivent introduire une demande d'autorisation spécifique au projet, dans laquelle ils précisent notamment les composants de l'architecture qu'ils souhaitent utiliser, les variables de données qui seront recueillies et s'il sera fait appel à certaines sources authentiques ou banques de données externes ainsi que les destinataires des données. Une analyse d'impact relative à la protection des données est réalisée pour chaque projet. Dans le cadre de la proposition pour l'architecture Be-HERA, une analyse a été réalisée en ce qui concerne l'application de l'article 25 du RGPD, à savoir la protection des données dès la conception et la protection des données par défaut, et a été fournie au Comité de sécurité de l'information. Cette analyse est basée sur les lignes directrices du Comité européen de la protection des données.⁷

II. COMPETENCE

- 15.** Le Comité a pris connaissance de la création de l'Autorité européenne de préparation et de réaction en cas d'urgence sanitaire et de l'appel lancé aux Etats membres afin de se préparer à une prochaine pandémie éventuelle au moyen d'instruments adéquats pour une transmission des informations pertinentes en matière de lutte contre les maladies infectieuses concernées. Il constate que le demandeur envisage par Be-HERA une infrastructure durable, nationale qui traite les données génomiques de manière harmonisée et les couple à des données cliniques et épidémiologiques. Il rend une délibération pour la durée pendant laquelle l'architecture Be-HERA sera utilisée au sein du paysage de l'eSanté interfédéral, en collaboration avec tous les acteurs concernés et dans les cadres réglementaires, comme l'infrastructure de base pour
- la collecte centralisée de données génomiques ainsi que le couplage à des données cliniques et épidémiologiques permettant de détecter en temps utile et avec précision les variantes et/ou les épidémies
 - faciliter la déclaration obligatoire de maladies infectieuses aux autorités sanitaires fédérées
 - faciliter le rapportage aux autorités sanitaires internationales
 - le traitement transactionnel de gros volumes de données en cas d'épidémie ou de pandémie
- 16.** En vertu de l'article 42, § 2, 3° de la loi du 13 décembre 2006 portant dispositions diverses en matière de santé, la chambre sécurité sociale et santé du Comité de sécurité de l'information est compétente pour rendre une délibération de principe concernant toute communication de données à caractère personnel relatives à la santé.

⁷ Lignes directrices 4/2019 relatives à l'article 25 Protection des données dès la conception et protection des données par défaut https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_fr.pdf

17. L'article 11 de la loi du 21 août 2008 relative à l'institution et à l'organisation de la Plate-forme eHealth dispose que toute communication de données à caractère personnel par ou à la Plate-forme eHealth requiert une autorisation de principe de la chambre sécurité sociale et santé du Comité de sécurité de l'information.
18. Le Comité estime par conséquent qu'il est compétent pour se prononcer sur la présente demande d'autorisation; toutefois, il doit formuler des réserves quant à l'usage et à la consultation des données du Registre national qui relèvent des compétences du Ministre de l'Intérieur.

III. EXAMEN

A. ADMISSIBILITÉ

19. Le traitement de données à caractère personnel n'est licite que si, et dans la mesure où, au moins une des conditions mentionnées à l'article 6, §1^{er}, du RGPD est remplie. Ceci est notamment le cas lorsque le traitement est nécessaire à une obligation légale à laquelle le responsable du traitement est soumis.
20. Le traitement de données à caractère personnel relatives à la santé est en principe interdit. Conformément à l'article 9, 2, i) du RGPD, l'interdiction ne s'applique cependant pas lorsque 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. C'est le cas en l'espèce. Conformément à l'article 9, 2, j) du RGPD, l'interdiction ne s'applique pas non plus lorsque le traitement est nécessaire à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, conformément à l'article 89, paragraphe 1, sur la base du droit de l'Union ou du droit d'un État membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée.

Le Comité fait observer qu'il existe un cadre réglementaire pour différentes activités de traitement et/ou finalités.

L'arrêté royal du 3 décembre 1999 *relatif à l'agrément des laboratoires de biologie clinique* décrit notamment les normes d'agrément, les procédures et l'assurance qualité auxquelles les laboratoires cliniques doivent satisfaire. Les données à caractère personnel nominatives qui sont collectées en rapport avec les demandes de laboratoire et les rapports médicaux sont mentionnés dans les articles 21, 22 et 37.

Les communications de données à caractère personnel par les Centres nationaux de référence à Sciensano (l'ancien ISP) à des fins scientifiques, épidémiologiques et d'appui à la politique sont définies comme étant une tâche obligatoire des CNR à l'article 1^{er}, § 2, 5^o de l'arrêté

royal du 9 février 2011 *fixant les conditions de financement des centres de référence en microbiologie humaine.*

La communication de données nominatives par les acteurs ou établissement de soins concernés aux autorités sanitaires régionales (AViQ, AZG, COCOM, Ministère de la Communauté germanophone) pour les maladies infectieuses qui doivent être signalées, est régulée par la réglementation suivante:

- Le décret du Parlement flamand du 21 novembre 2003 relatif à la politique de santé préventive (article 44, § 3)
- L'arrêté du Gouvernement flamand du 19 juin 2009 relatif aux initiatives visant à prévenir l'extension des effets nocifs causés par des facteurs biotiques (articles 2-7)
- [Le décret du 2 mai 2019 modifiant le Code wallon de l'Action sociale et de la Santé](#) en ce qui concerne la prévention et la promotion de la santé (artikels 17-20)
- Le décret du [Parlement de la Communauté germanophone du 1er juin 2004](#) relatif à la promotion de la santé et à la prévention médicale (artikel 2)
- [L'ordonnance du 19 juillet 2007](#) relative à la politique de prévention en santé, région de Bruxelles-Capitale (artikel 12)
- L'arrêté du Collège réuni de la Commission communautaire commune relatif à la prophylaxie des maladies transmissibles du 23 avril 2009

La communication de données pseudonymisées au Centre européen de Prévention et de Contrôle des Maladies (CEPCM) est régie par la réglementation suivante:

- [La décision n° 1082/2013/UE](#) du Parlement européen et du Conseil du 22 octobre 2013 relative aux menaces transfrontalières graves sur la santé et abrogeant la décision du n° 2119/98/CE
- La décision n° 2119/98/CE du Parlement européen et du Conseil du 24 septembre 1998 instaurant un réseau de surveillance épidémiologique et de contrôle des maladies transmissibles dans la Communauté européenne;
- La décision n° 2000/96/CE du Parlement européen et du Conseil du 22 décembre 1999 concernant les maladies transmissibles que le réseau communautaire doit couvrir sur une base progressive en application de la décision n° 2119/98/CE.
- [ECDC founding regulation](#): Le règlement (CE) n° 851/2004 du Parlement Européen et du Conseil du 21 avril 2004 instituant un Centre européen de prévention et de contrôle des maladies.

La loi du 25 février 2018 portant création de Sciensano prévoit ce qui suit à l'article 4, § 4:

- *Art. 4. § 4^{er}. Sciensano assure le traitement, en ce compris la collecte, la validation, l'analyse, le rapportage et l'archivage, des données à caractère personnel notamment relatives à la santé publique ou en un lien avec la santé et d'autres informations scientifiques relatives à la politique de santé, dans le respect des lois applicables en la matière. A cette fin, Sciensano réalise des analyses scientifiques quantitatives et qualitatives sur la base des informations traitées en vue de soutenir*

la politique de santé. Sciensano peut également mettre des données et des informations traitées à disposition, moyennant les autorisations des comités sectoriels compétents. § 4/1. Dans le cadre de la gestion des crises touchant la santé publique, Sciensano a pour mission de coordonner et d'implémenter les aspects scientifiques qui y sont liés, de surveiller et d'évaluer les risques au moyen d'analyses spécifiques des données collectées, de fournir des avis et recommandations aux différentes autorités de santé du pays et d'organiser la communication au profit des autorités, des prestataires des soins de santé et du public.

En ce qui concerne le rôle du service healthdata.be de Sciensano, il peut être renvoyé à l'article 22, 20° de la loi du 14 juillet 1994 *relative à l'assurance obligatoire soins de santé et indemnités*, à la loi du 10 avril 2014 *portant des dispositions diverses en matière de santé* qui a créé un cadre permettant à l'INAMI de renforcer et de systématiser sa collaboration avec Sciensano (l'ancien ISP), en particulier en vue de la coordination et du soutien des collectes de données qui doivent augmenter la connaissance relative à la santé de la population.

21. Nonobstant cette réglementation, dans le prolongement de l'accord de coopération du 25 août 2020 entre l'Etat fédéral, la Communauté flamande, la Région wallonne, la Communauté germanophone et la Commission communautaire commune concernant le traitement conjoint de données par Sciensano et les centres de contact désignés par les autorités régionales compétentes ou par les agences compétentes, par les inspections sanitaires et par les équipes mobiles dans le cadre d'un suivi des contacts auprès des personnes (présumées) infectées par le coronavirus SARS-CoV-2 sur la base d'une base de données auprès de Sciensano, il sera élaboré un nouveau cadre réglementaire pour la gestion des infections SARS-CoV-2 ainsi que d'autres maladies infectieuses éventuelles. Il est possible que le nouveau cadre réglementaire intégrera aussi des aspects de l'architecture de Be-HERA. Sciensano tiendra la chambre sécurité sociale et santé du Comité de sécurité de l'information informée de nouvelles initiatives réglementaires éventuelles afin d'actualiser la délibération relative à l'architecture Be-HERA.
22. Le Comité estime par conséquent qu'il existe un fondement pour le traitement des données à caractère personnel relatives à la santé envisagé.

B. FINALITÉ

23. L'article 5 du RGPD autorise le traitement de données à caractère personnel uniquement pour des finalités déterminées, explicites et légitimes.
24. Les finalités de l'infrastructure Be-HERA sont les suivantes: la collecte de données en vue de la confirmation et/ou du diagnostic pour une surveillance accrue des agents pathogènes, la collecte et le traitement de données génomiques des agents pathogènes, la réalisation d'une étude d'appui à la politique et/ou scientifique sur la base de données pseudonymisées, la facilitation du signalement obligatoire de certaines maladies infectieuses aux autorités sanitaires régionales et la facilitation du rapportage aux autorités sanitaires internationales.

25. Le Comité estime que le traitement de données à caractère personnel envisagé poursuit effectivement des finalités déterminées, explicites et légitimes.

C. PROPORTIONNALITÉ

26. L'article 5 du RGPD dispose que les données à caractère personnel doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement.
27. Sciensano justifie le traitement des données à caractère personnel par finalité et par destinataire des données comme suit:

Finalité confirmation et/ou diagnostic d'agents pathogènes pour surveillance accrue pour laquelle des données sont mises à la disposition des centres nationaux de référence sur la plateforme CNR

- données d'identification nominatives (nom, prénom, numéro NISS): données nécessaires à l'identification unique du patient ou du citoyen.
- Données de diagnostic: données relatives au diagnostic présumé et/ou confirmé, par exemple, résultats d'examens de laboratoire ou d'examens radiologiques nécessaires pour la continuité des soins au patient et afin de satisfaire aux obligations réglementaires en matière de conservation minutieuse d'un dossier de patient.
- Données cliniques et épidémiologiques: données relatives à la situation clinique et épidémiologique du patient ou du citoyen (par exemple, données d'identification du prestataire de soins, état de vaccination, contacts sociaux) nécessaires au suivi épidémiologique.
- Données génomiques : données liées aux résultats du "séquençage haut débit", qui comprennent la lecture du génome d'un agent pathogène sous la forme de plusieurs séquences brutes et peuvent en outre inclure une séquence de consensus globale ou l'interprétation génomique spécifique, c'est-à-dire les indicateurs génomiques, par le traitement bioinformatique de la ou des séquences. Ces données sont nécessaires à la caractérisation des souches (p.ex. génotypage, étude des antigènes, étude de la résistance aux antibiotiques).

Finalité identification bioinformatique pour laquelle des données génomiques de l'agent pathogène de la plateforme BioIT sont partagées avec les centres nationaux de référence

- Données génomiques : données relatives aux résultats du "séquençage haut débit", qui comprennent la lecture du génome d'un agent pathogène sous la forme de plusieurs séquences brutes et qui peuvent, en outre, inclure une séquence de consensus globale ou l'interprétation génomique spécifique, c'est-à-dire les indicateurs génomiques, par le traitement bioinformatique de la ou des séquences. Ces informations sont nécessaires à la caractérisation des souches (p.ex. génotypage, étude des antigènes, étude de la résistance aux antibiotiques).
- Données techniques génomiques: données relatives au traitement bioinformatique des fichiers de données génomiques (bruts) après application du séquençage parallèle de

masse. Ces données sont nécessaires à la caractérisation des souches (p.ex. génotypage, étude des antigènes, étude de la résistance aux antibiotiques).

- Clé se composant de données non-nominatives en vue du couplage de données entre la plateforme BioIT et la plateforme CNR.

Finalité étude d'appui à la politique et/ou scientifique à l'occasion de laquelle des données pseudonymisées sont partagées à l'intervention de la plateforme Healthdata.be avec les épidémiologues de Sciensano ou de centres de recherche externes qui ont reçu une autorisation de la chambre sécurité sociale et santé du Comité de sécurité de l'information

- Pseudo-ID basé sur le NISS: nécessaire à l'identification unique de personnes et au couplage éventuel à d'autres banques de données si autorisé par le Comité de sécurité de l'information
- Données démographiques: données relatives au domicile, à l'âge ou au décès sont pertinentes pour les connaissances scientifiques et les statistiques d'appui à la politique concernant les groupes cibles dans lesquels la maladie infectieuse se manifeste ou non, les groupes cibles dans lesquels les tests sont effectués, les entités géographiques où l'agent pathogène est présent, etc.
- Données de diagnostic: données relatives au diagnostic présumé et/ou confirmé, par exemple, résultats d'examens de laboratoire ou d'examens radiologiques. Ces données sont nécessaires pour obtenir des statistiques précises et des informations pertinentes sur les tests effectués et l'incidence des agents pathogènes.
- Données cliniques et épidémiologiques: données relatives à la situation clinique et épidémiologique du patient ou du citoyen, par exemple, pseudoID du prestataire de soins, état de vaccination, contacts sociaux. Ces données sont nécessaires pour obtenir des informations sur les clusters d'infection, les sources potentielles d'infection, l'efficacité des vaccins, etc.
- Données génomiques : données relatives aux résultats du "séquençage haut débit", qui comprennent la lecture du génome d'un agent pathogène sous la forme d'interprétations génomiques spécifiques, c'est-à-dire les indicateurs génomiques, par le traitement bioinformatique de la ou des séquences. Ces données sont nécessaires à la caractérisation des souches (p.ex. génotypage, étude des antigènes, étude de la résistance aux antibiotiques).

Finalité faciliter le signalement obligatoire de certaines maladies infectieuses aux services d'inspection de la santé de l'administration sanitaire régionale

- données à caractère personnel nominatives: données relatives à l'identification du patient ou du citoyen, identification unique de personnes ainsi que la possibilité de couplage à d'autres banques de données (p.ex. Registre national) si autorisé
- Données de contact (si autorisé par le cadre réglementaire): données en vue de faciliter la prise de contact, le traçage de personnes non joignables et/ou du suivi dans le cadre de mesures de prévention de la santé
- Données de diagnostic: données relatives au diagnostic présumé et/ou confirmé, par exemple, résultats d'examens de laboratoire ou d'examens radiologiques. Données

indispensables aux actions préventives devant éviter la propagation de maladies infectieuses.

- Données cliniques et épidémiologiques: données relatives à la situation clinique et épidémiologique du patient ou du citoyen, par exemple, données d'identification du prestataire de soins, état de vaccination, contacts sociaux, qui sont nécessaires à la détermination d'actions préventives appropriées et à l'évaluation de la politique.
- Données génomiques : données relatives aux résultats du "séquençage haut débit", qui comprennent la lecture du génome d'un agent pathogène sous la forme de plusieurs séquences brutes et qui peuvent, en outre, éventuellement inclure une séquence de consensus globale ou l'interprétation génomique spécifique, c'est-à-dire les indicateurs génomiques, par le traitement bioinformatique de la ou des séquences (optionnel). Ces données sont nécessaires à la caractérisation des souches (p.ex. génotypage, étude des antigènes, étude de la résistance aux antibiotiques).
- Identité du médecin traitant: nécessaire à l'obtention d'informations complémentaires pour des actions préventives par les inspecteurs régionaux de la santé

Finalité faciliter le rapportage aux autorités sanitaires internationales (CEPCM, OMS, etc.)

- Données de diagnostic: données relatives au diagnostic présumé et/ou confirmé, par exemple, résultats d'examens de laboratoire ou d'examens radiologiques nécessaires pour esquisser la situation épidémiologique
 - Données cliniques et épidémiologiques: données pseudonymisées relatives à la situation clinique et épidémiologique nécessaires pour esquisser la situation épidémiologique
 - Données génomiques : données relatives aux résultats du "séquençage haut débit", qui comprennent la lecture du génome d'un agent pathogène sous la forme de plusieurs séquences brutes et qui peuvent, en outre, inclure une séquence de consensus globale ou l'interprétation génomique spécifique, c'est-à-dire les indicateurs génomiques, par le traitement bioinformatique de la ou des séquences (optionnel). Ces données sont nécessaires à la caractérisation des souches (p.ex. génotypage, étude des antigènes, étude de la résistance aux antibiotiques).
28. Les projets qui auront recours à l'architecture Be-HERA introduisent une demande d'autorisation spécifique au projet auprès de la chambre sécurité sociale et santé du Comité de sécurité de l'information dans laquelle les données sont concrétisées.
29. Les données à caractère personnel ne peuvent être conservées sous une forme permettant l'identification des personnes concernées au-delà du délai nécessaire à la réalisation des finalités pour lesquelles elles sont obtenues ou pour lesquelles elles sont traitées ultérieurement.
30. La suppression de données à caractère personnel nominatives sur la plateforme technique Be-HERA sera, en des temps non pandémiques, réalisée immédiatement dès finalisation des transferts vers les autres composants (administrations sanitaires régionales, datawarehouse de healthdata.be). La plateforme technique de Be-HERA concerne en effet une plateforme

d'échange ne nécessitant pas de conservation des données. Ce n'est qu'en période pandémique et moyennant la réglementation et/ou les autorisations requises que des données peuvent être conservées, dans le cadre de processus opérationnels de soutien par la plateforme technique Be-HERA, plus longtemps pour des activités spécifiques (p.ex. traçage des contacts à grande échelle).

La plateforme BioIT disposera, tant en période pandémique qu'en période non pandémique, uniquement de données génomiques (brutes) et non de données à caractère personnel.

La plateforme CNR disposera, dans le cadre de ses missions légales de soutien des laboratoires de biologie clinique en matière de soins de santé et d'études épidémiologiques, de données à caractère personnel pseudonymisées et/ou nominatives, tant en période pandémique que période non pandémique pendant une durée de 30 ans. Les données pseudonymisées ou nominatives qui sont nécessaires au sein de la plateforme CNR peuvent être spécifiques à l'agent pathogène et devront dès lors être précisées dans les demandes d'autorisation futures spécifiques au projet qui seront introduites auprès du Comité de sécurité de l'information. Le délai de conservation de 30 ans est nécessaire pour que les CNR puissent réaliser correctement leurs missions légales et pour garantir un suivi efficace des agents pathogènes. Cette période est également basée sur le délai de conservation des dossiers de patient comme prévu à l'article 35 de la loi du 22 avril 2019 relative à la qualité de la pratique des soins de santé.

Dans le cadre de la préparation, du suivi et de la réaction à une éventuelle épidémie de maladies infectieuses ainsi que pour comprendre le déroulement de la maladie dans une population donnée ou une partie de la population (qui a trait à, par exemple, l'âge, le sexe, etc.) et pour établir des modèles statistiques de la maladie qui permettent de prédire une tendance dans les maladies infectieuses, il est donc très important pour Sciensano de pouvoir conserver les données épidémiologiques pendant 30 ans à compter de leur enregistrement dans le datawarehouse healthdata.be. Le suivi épidémiologique de tendances est surtout important pour des périodes plus longues couvrant plusieurs années. Les données historiques sont importantes pour le suivi de tendances, la modélisation de développements à long terme tels l'impact de changements climatiques ou d'autres facteurs externes. Pour la modélisation d'évolutions génétiques et l'étude de l'impact de, par exemple, la vaccination sur l'adaptation génétique d'agents pathogènes sur le long terme, des séries temporelles plus longues couvrant plusieurs années s'avèrent nécessaires.

31. Le Comité estime qu'il est acceptable d'avoir recours, dans le cadre de l'exactitude des données et des objectifs de Be-HERA, aux sources authentiques suivantes: le Registre national moyennant l'autorisation du ministre de l'Intérieur, les registres Banque Carrefour pour les patients concernés qui ne sont pas enregistrés dans le Registre national et CoBRHA en ce qui concerne les données d'identification des prestataires de soins. Des informations exactes sont indispensables pour des informations politiques correctes en vue de la maîtrise des maladies infectieuses. Le fait de compléter les données par des données du Registre national, des registres Banque Carrefour, de CoBRHA a également pour objectif de diminuer la charge administrative des fournisseurs de données (principalement les acteurs des soins de santé), afin de faire en sorte que le système soit 'pandemic proof' en cas d'épidémie à grande échelle et que les acteurs des soins de santé puissent se consacrer autant que possible à la

prestation de soins. Cette justification en matière de simplification administrative est aussi considérée comme acceptable par le Comité. Le Comité prend acte du fait que les données exactes provenant de ces sources authentiques qui seront utilisées, seront précisées dans les autorisations spécifiques au projet.

32. Compte tenu de l'objectif, le Comité estime que le traitement de ces données à caractère personnel est en principe adéquat, pertinent et non excessif.

D. TRANSPARANCE

33. Conformément à l'article 14 du RGPD, le responsable du traitement fournit les informations nécessaires à la personne concernée lorsque les données à caractère personnel n'ont pas été collectées auprès de la personne concernée. Cette disposition ne s'applique cependant pas, notamment lorsque la fourniture de telles informations se révèle impossible ou exigerait des efforts disproportionnés. En pareils cas, le responsable du traitement prend des mesures appropriées pour protéger les droits et libertés ainsi que les intérêts légitimes de la personne concernée, y compris en rendant les informations publiquement disponibles.
34. Sciensano, en tant que responsable du traitement de la plateforme CNR, de la plateforme BioIT, de la plateforme technique Be-HERA et du datawarehouse healthdata.be prend des mesures adéquates pour que les personnes concernées reçoivent les informations visées aux articles 13 et 14 du RGPD et la communication visée aux articles 15 à 22 et à l'article 34 du RGPD concernant le traitement pour les finalités visées à l'article 3 de l'accord de coopération du 25 août 2020 d'une façon concise, transparente, compréhensible et aisément accessible et en des termes clairs et simples. Par ailleurs, Sciensano maintient et gère un système pour l'exercice des droits déterminés aux articles 15 à 22 et à l'article 34 du Règlement général relatif à la protection des données.
35. À cet effet, Sciensano créera et tiendra à jour une page internet sur laquelle seront publiées conformément à l'article 14 du RGPD des informations adéquates ainsi que les données de contact du délégué à la protection des données. Sur cette page internet, les différentes personnes concernées (patients, représentants de patients, prestataires de soins) trouveront des renseignements sur le traitement de données qui a lieu sur les plateformes précitées. Tout projet qui souhaite utiliser l'infrastructure Be-HERA publiera une déclaration de protection des données pour les personnes concernées sur la page internet centrale et/ou sur une page internet propre au projet.

E. MESURES DE SÉCURITÉ

36. En vertu de l'article 5 du RGPD, les données à caractère personnel doivent être traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité). Ces mesures devront assurer un niveau de protection adéquat compte tenu, d'une part, de l'état de la technique en la matière et des frais

qu'entraînent l'application de ces mesures et, d'autre part, de la nature des données à protéger et des risques potentiels.

37. Le Comité attire explicitement l'attention sur les dispositions du Titre 6. Sanctions de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, qui prévoient des sanctions administratives et pénales sévères dans le chef du responsable du traitement et des sous-traitants pour la violation des conditions prévues dans le RGPD et la loi du 30 juillet 2018 précitée.
38. Les données à caractère personnel relatives à la santé peuvent uniquement être traitées sous la surveillance et la responsabilité d'un professionnel des soins de santé. Même si cela n'est pas strictement requis par le RGPD, le Comité estime qu'il est préférable que de telles données soient traitées sous la responsabilité d'un médecin. Ce qui est le cas en l'espèce. Le Comité rappelle que lors du traitement de données à caractère personnel, le professionnel des soins de santé ainsi que ses préposés ou mandataires sont soumis au secret.
39. En vertu de l'article 89, § 1^{er}, du RGPD, le traitement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique, ou à des fins statistiques est soumis, conformément au RGPD, à des garanties appropriées pour les droits et libertés de la personne concernée. Ces garanties garantissent la mise en place de mesures techniques et organisationnelles, en particulier pour assurer le respect du principe de minimisation des données.
40. Le Comité rappelle également que dans le cadre du traitement à des fins scientifiques, le responsable du traitement doit respecter les dispositions du titre 4 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.
41. Les données à caractère personnel sont, toujours après pseudonymisation, communiquées par Sciensano aux épidémiologistes concernés à des fins d'étude scientifique, statistique et/ou d'appui à la politique. Conformément à l'article 5 du RGPD, les données à caractère personnel peuvent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées ou pour lesquelles elles sont traitées ultérieurement. Le Comité estime que les données peuvent être conservées par Sciensano sous forme pseudonymisée pendant une période de 30 ans. À l'issue de cette période, elles peuvent uniquement être conservées sous forme anonyme, c'est-à-dire sous une forme qui ne permet pas de les mettre en relation avec une personne identifiée ou identifiable.
42. Le Comité souligne que les résultats du traitement à des fins scientifiques ne peuvent pas être publiés sous une forme qui permet l'identification de la personne concernée.
43. Le Comité rappelle enfin qu'en vertu de l'article 9 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, le responsable du traitement prend les mesures supplémentaires suivantes lors du traitement de données génétiques, biométriques ou des données concernant la santé :

1° les catégories de personnes ayant accès aux données à caractère personnel, sont désignées par le responsable du traitement ou, le cas échéant, par le sous-traitant, avec une description précise de leur fonction par rapport au traitement des données visées;

2° la liste des catégories des personnes ainsi désignées est tenue à la disposition de l'autorité de contrôle compétente par le responsable du traitement ou, le cas échéant, par le sous-traitant;

3° il veille à ce que les personnes désignées soient tenues, par une obligation légale ou statutaire, ou par une disposition contractuelle équivalente, au respect du caractère confidentiel des données visées.

Par ces motifs,

la chambre sécurité sociale et santé du comité de sécurité de l'information

conclut que :

la communication des données à caractère personnel telle que décrite dans la présente délibération est autorisée moyennant le respect des mesures de protection de la vie privée qui ont été définies, en particulier les mesures en matière de limitation de la finalité, de minimisation des données, de limitation de la durée de conservation des données et de sécurité de l'information.

Bart VIAENE
Président

Le siège de la chambre sécurité sociale et santé du comité de sécurité de l'information est établi dans les bureaux de la Banque Carrefour de la sécurité sociale, à l'adresse suivante: Quai de Willebroeck 38 - 1000 Bruxelles (tél. 32-2-741 83 11).

Annexe 1: Principes, types de données, activités des données et gestion en lien avec les composants de l'architecture Be-HERA

