VERSION AOUT 2025

navify Sample Tracking

Annexe - Accord Spécifique de Traitement de Données à Caractère Personnel

entre

CLIENT

- le Responsable de Traitement -

- ci-après dénommé le CLIENT -

et

ROCHE DIAGNOSTICS FRANCE

- le Sous-Traitant -

- ci-après ROCHE -

1. CHAMP D'APPLICATION

(1) Application Le présent Accord Spécifique de Traitement de Données à Caractère Personnel ("l'Accord") est gouverné par les Conditions Générales Produits Numériques et Services associés et son annexe relative au traitement des données à Caractère Personnel. Tous les termes figurant avec une majuscule ont le sens défini dans le présent Accord ou le cas échéant dans les Conditions Générales Produits Numériques et Services associés et son annexe de traitement des données à caractère personnel.

(2) Parties. Dans cet Accord, le CLIENT a la qualité de Responsable de Traitement et ROCHE (incluant ses filiales), la qualité de Sous-traitant de Données à Caractère Personnel.

(3) Objet. L'objet de cet Accord résulte de l'Offre ROCHE.

(4) Durée. La durée de cet Accord correspond à la Durée de l'Offre.

2. SPECIFICATION

(1) La nature et la finalité du traitement par ROCHE pour le CLIENT des Données à caractère Personnel sont précisément déterminées dans l'Offre.

(2) Champ d'application géographique. Le traitement des Données à caractère Personnel contractuellement déterminé sera effectué selon les indications figurant dans l'Accord relatif au traitement des données.

(3) Catégories de Personnes Concernées. Les catégories de Personnes Concernées sont les suivantes :

a. Les patients du CIENT

(4) Type de données. Le traitement des Données à Caractère Personnel (les « Données ») concerne les types et catégories de Données suivants :

a) En ce qui concerne la collecte des informations relatives à l'Offre auprès du donneur d'ordre (par exemple, le professionnel de santé) et leur mise à la disposition du tiers (par exemple, le phlébotomiste, le laboratoire) Catégorie a) des Personnes concernées ci-dessous:

- Données démographiques du patient (ePHI, p. ex., âge, nom, prénom, sexe)

- Tests à effectuer (aucun résultat)
- Informations sur l'échantillon (ID de l'échantillon/type d'échantillon)

b) En ce qui concerne le recueil des informations d'échantillonnage auprès de tiers (p. ex. phlébotomiste, laboratoire) et leur envoi au client (p. ex. professionnel de santé) Catégorie a) des Personnes concernées ci-dessous:

- Données démographiques du patient (âge, nom, sexe)
- Informations sur l'échantillon (ID de l'échantillon/type d'échantillon)

c) En ce qui concerne la collecte des informations de transport auprès de tiers (par exemple, phlébotomiste, laboratoire) et leur envoi au client (par exemple, professionnel de santé), catégorie a) des Personnes concernées ci-dessous:

- Informations sur l'échantillon (ID de l'échantillon/ID du tube)
- Informations de commande (plusieurs tests à effectuer)

3. MESURES TECHNIQUES ET ORGANISATIONNELLES

(1) Les Mesures Techniques et Organisationnelles nécessaires sont indiquées à l'Annexe A au présent Accord et sont approuvées par le CLIENT. À la date d'effet du présent Accord, le CLIENT reconnaît qu'il considère les Mesures Techniques et organisationnelles qui y sont décrites comme appropriées, compte tenu de l'état des connaissances technologiques, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement, ainsi que du degré de probabilité et de gravité du risque pour les Personnes Concernées.

(2) Les mesures documentées constituent le fondement du présent Accord. Dans la mesure où le CLIENT demanderait que des modifications y soient apportées, celles-ci devraient être effectuées d'un commun accord.

4. SOUS-TRAITANCE

(1) ROCHE pourra faire appel à des sous-traitants (sous-traitants ultérieurs) selon les conditions de l'Accord. En outre, les sous-traitants ultérieurs suivants sont expressément agréés par le Client aux fins du présent Accord.

Sous-traitants de Roche	Addresse / pays	Service
Roche Group affiliates, incluant entre autres : Roche Diagnostics International AG, Rotkreuz, Suisse, Roche Information Solutions India Pvt Ltd in Pune, Inde, Roche Diagnostics SL. in San Cugat, Espagne		agissant en tant que sous-traitant des données de la filiale de Roche, qui a un contrat avec le Client. Le rôle des filiales de Roche est de fournir les services d'assistance et de maintenance. Toute activité de traitement des données repose sur l'accord de transfert de données intersociétés (RIDTA) du groupe Roche.

AWS	Frankfurt ou autres data centers situés EEA	agissant en tant que sous-traitant de Roche et en tant que fournisseur de l'hébergement de données (services cloud) dans la région respective, où la solution est déployée. Actuellement, Francfort-sur-le-Main.
Cloudflare	EEA	agissant en tant que sous-processeur de Roche et en tant que fournisseur de la protection d'accès au réseau et dans la région respective, où la solution est déployée.
Interoperability Health (UK) Limited d.b.a (applicable si le moteur d'inter opérabilité est en place)	EEA	Agissant en tant que sous-traitant de Roche et fournissant les services d'interopérabilité entre l'application et les systèmes SIL du client.

5. RECTIFICATION, LIMITATION ET EFFACEMENT DES DONNÉES À CARACTÈRE PERSONNEL

(1) ROCHE ne pourra de sa propre initiative rectifier les Données traitées pour le compte du client, les effacer ni en limiter le traitement. Elle ne peut le faire que sur instructions documentées de ce dernier. Dans la mesure où une Personne Concernée prendrait directement contact avec ROCHE aux fins de la rectification ou de l'effacement de Données ou afin d'en limiter le traitement, ROCHE devrait transmettrait cette demande au CLIENT dans les meilleurs délais.

(2) Dans la mesure où ces éléments s'inscriront dans le périmètre des prestations, ROCHE sera chargée de la politique en matière d'effacement, ainsi que du respect du « droit à l'oubli », à la rectification des données, à leur portabilité et du droit d'y accéder, dans le respect des instructions documentées du CLIENT et dans les meilleurs délais.

(3) Le CLIENT est informé du fait que ROCHE ne pourra, de sa propre initiative, assurer la portabilité des données, les rectifier, les effacer ni en limiter le traitement, en raison de leur chiffrement intégral et de la maîtrise exclusive par le CLIENT des clés de chiffrement. Ce dernier devra donc aider ROCHE à satisfaire toute demande de cet ordre et soit indemniser ROCHE de ses efforts soit assumer elle-même les obligations susvisées afin de les remplir directement par le biais de l'interface locale non chiffrée du CLIENT.

6. GARANTIE QUALITÉ ET AUTRES OBLIGATIONS DE ROCHE

1) Outre le respect des règles définies dans le cadre de l'Accord relatif au traitement des données applicable, ROCHE devra respecter les exigences définies aux Articles 28 à 33 du RGPD. Elle devra par conséquent respecter, en particulier, les exigences suivantes :

   a) La confidentialité devra être assurée, conformément à l'Article 28, Section 3, deuxième phrase, point b, ainsi qu'à l'Article 29 et à l'Article 32, Section 4 du RGPD. ROCHE ne confie le traitement des données dont il est question dans chaque Accord relatif au traitement des données qu'à ses salariés soumis à une obligation de confidentialité ou ayant souscrit un engagement en la matière et ayant préalablement acquis une bonne connaissance des règles de protection des données concernant leur emploi. Sauf exigence légale contraire, ROCHE et toute personne agissant sous son autorité et ayant accès aux Données ne devront les traiter que sur instructions du CLIENT, étant entendu que les pouvoirs conférés aux termes du présent Accord satisfont cette condition.

   b) Mise en œuvre et respect de l'ensemble des Mesures techniques et organisationnelles nécessaires dans le cadre de chaque Accord relatif au traitement des données, en vertu de l'Article 28, Section 3, deuxième phrase, point c et l'Article 32 du RGPD, et visées à l'Article 3 du présent Accord.

c) ROCHE et le CLIENT devront coopérer, sur demande, avec l'autorité de contrôle lors de l'accomplissement de leurs tâches respectives.

d) Le CLIENT devra être informé immédiatement de toutes inspections menées par l'autorité de contrôle et de toutes mesures prises par celle-ci, dans la mesure où elles auront un lien avec un Accord relatif au traitement des données. Il en serait de même dans le cas où ROCHE serait soumise ou partie prenante à une enquête menée par une autorité compétente sur des infractions à une loi civile ou pénale, à une règle administrative ou à un règlement ayant trait au traitement des Données, commises en lien avec un Accord relatif au traitement des données.

e) Dans la mesure où le CLIENT ferait l'objet d'une inspection menée par l'autorité de contrôle, d'une procédure administrative ou pour infraction mineure ou pénale, ou verrait engager sa responsabilité par une Personne Concernée ou par un tiers, ou formuler à son encontre une autre prétention en lien avec un Accord relatif au traitement des données, ROCHE devrait faire tout son possible pour lui apporter son soutien.

f) ROCHE devra périodiquement contrôler les processus internes et les Mesures techniques et organisationnelles afin de garantir la conformité du traitement relevant de sa responsabilité aux exigences des textes de droit ayant trait à la protection des données, ainsi que la protection des droits des personnes concernées.

g) Le CLIENT devra avoir la possibilité vérifier les Mesures techniques et organisationnelles mises en œuvre, au titre de ses pouvoirs de surveillance visés à l'Article 7 du présent Accord.

7. SOUS-TRAITANCE

(1) Dans le cadre du présent Accord, l'expression « sous-traitance ultérieure » fait référence à des services ayant un lien direct avec la fourniture du service principal. Ceux-ci ne comprennent pas les services accessoires tels que les services de télécommunication, les services postaux et de transport, de maintenance et d'assistance à l'utilisateur, les services d'élimination des supports de données, ni les autres services destinés à garantir la confidentialité, la disponibilité, l'intégrité et la résilience du matériel et des logiciels dont les équipements de traitement des données sont dotés. ROCHE devra cependant conclure des accords appropriés, juridiquement contraignants, et prendre des mesures d'inspection adéquates visant à garantir la protection des données et la sécurité des données du CLIENT, même en cas d'externalisation de services accessoires.

(2) ROCHE pourra avoir recours à des sous-traitants ultérieurs (d'autres sous-traitants chargés du traitement) expressément agréés par le CLIENT. Celui-ci consent à ce qu'il soit fait appel aux sous-traitants dont la liste figure dans l'Accord relatif au traitement des données applicables, à condition qu'un contrat soit conclu dans le respect de l'Article 28, sections 2 à 4 du RGPD

(3) Le recours à des sous-traitants ultérieurs ou un changement parmi les sous-traitants ultérieurs existants est autorisé lorsque :
- ROCHE soumet cette externalisation au CLIENT par écrit ou sous forme de texte en observant un préavis approprié ; et
- Le CLIENT ne s'oppose pas par écrit ou sous forme de texte à l'externalisation projetée, dans un délai de deux semaines suivant la communication visée au paragraphe ci-dessus ; et
- La sous-traitance ultérieure est fondée sur un contrat, dans le respect de l'Article 28, sections 2 à 4 du RGPD.

(4) Le transfert de Données du CLIENT au sous-traitant ultérieur et le début de leur traitement par ce dernier sont subordonnés au respect préalable de toutes les exigences.

(5) Si le sous-traitant ultérieur fournit le service convenu en dehors de l'Union européenne et de l'Espace économique européen, ROCHE devra garantir le respect de la Réglementation relative à la protection des données en vigueur dans l'Union européenne en prenant des mesures appropriées. Il en sera de même s'il est prévu d'avoir recours à des prestataires de services au sens de la deuxième phrase de la Section 1) ci-dessus.

(6) Toute externalisation par un sous-traitant ultérieur est subordonnée à l'accord exprès de ROCHE (qui devra le communiquer au minimum sous forme de texte).

(7) L'ensemble des stipulations arrêtées au long de la chaîne de contrats devront être communiquées à chaque sous-traitant ultérieur supplémentaire et faire l'objet d'un accord avec celui-ci.

8. POUVOIR DE SUPERVISION DU CLIENT

(1) Le CLIENT est en droit, après consultation de ROCHE, de procéder à des inspections ou de les confier à un contrôleur désigné au cas par cas. Il est en droit de s'assurer lui-même du respect par ROCHE, dans le cadre de ses opérations, d'un Accord relatif au traitement des données, aux moyens de contrôles aléatoires devant être ordinairement annoncés raisonnablement à l'avance

(2) ROCHE s'engage à communiquer au CLIENT, sur demande, les informations nécessaires et, en particulier, à démontrer la mise en œuvre des Mesures techniques et organisationnelles.

(3) La preuve de la mise en œuvre de ces mesures pourra être apportée :
- En prouvant le respect des codes de conduite visés à l'Article 40 du RGPD ; et/ou
- Par une certification conforme à une procédure approuvée s'inscrivant dans le cadre de l'Article 42 du RGPD ; et/ou
- Par des certificats, des rapports ou des extraits de rapports d'auditeurs actuels fournis par des personnes ou organismes indépendants (par exemple, un contrôleur, un délégué à la protection des données, un département en charge de la sécurité informatique, un contrôleur de la protection des données, un contrôleur qualité) ; et/ou
- Par une certification adéquate attribuée par un audit de sécurité informatique ou de protection des données (par ex. conformément à BSI-Grundschutz (une certification de protection informatique initiale développée par le Bureau fédéral allemand pour la sécurité des technologies (BSI) ou ISO/IEC 27001) ;

(4) Étant précisé que ROCHE pourra demander une rémunération en contrepartie de la possibilité qu'elle donnera au CLIENT de procéder à des inspections sans motif particulier.

9. COMMUNICATION EN CAS D'INFRACTIONS COMMISES PAR ROCHE

(1) ROCHE devra aider raisonnablement le CLIENT à remplir les obligations ayant trait à la sécurité des Données, au signalement des violations de données, aux analyses d'impact relatives à la protection des données et aux consultations préalables, dont il est question aux Articles 32 à 36 du RGPD. Cette obligation comprend :
   a) L'obligation de garantir un niveau approprié de protection des données grâce à des Mesures techniques et organisationnelles déterminées en fonction des circonstances, des finalités du traitement, ainsi que de la probabilité et de la gravité prévues d'une infraction à la loi susceptible de résulter de certains facteurs de vulnérabilité en matière de sécurité. Ces mesures devront permettre une détection immédiate des cas de violation et des infractions.

b) L'obligation de porter une violation de Données à la connaissance du CLIENT dans les meilleurs délais.
c) L'obligation d'aider le CLIENT à remplir celle qui lui incombe de communiquer des informations à la Personne Concernée ; et de fournir immédiatement au CLIENT toutes informations utiles à cet égard.
d) L'obligation d'aider le CLIENT à réaliser son analyse d'impact relative à la protection des données.
e) L'obligation d'aider le CLIENT à procéder à la consultation préalable de l'autorité de contrôle.

(2) ROCHE pourra réclamer une rémunération relative aux services d'assistance non compris dans le descriptif des services et qui n'auront pas à être fournis en raison de défaillance de la part de ROCHE.

POUVOIR DU CLIENT DANS L'ÉMISSION D'INSTRUCTIONS

(1) Le CLIENT devra immédiatement confirmer ses instructions verbales (au minimum sous forme de texte).

(2) ROCHE devra immédiatement informer le CLIENT si elle considère qu'une instruction est contraire à la réglementation relative à la protection des données. Elle sera en droit de suspendre l'exécution de l'instruction en question jusqu'à ce que le CLIENT la confirme ou la modifie.

(3) Le CLIENT devra obtenir l'ensemble des consentements et autorisations des Personnes Concernées qui pourraient être nécessaires ou obligatoires en vertu des textes de droit applicables s'agissant des Données devant être traitées par ROCHE et ses sous-traitants ultérieurs dans le cadre du Contrat et au titre de toute Commande.

11. SUPPRESSION ET RETOUR DE DONNÉES

(1) Aucune copie de Données ne saurait être produite sans que le CLIENT en ait connaissance, à l'exception des copies de sauvegarde qui seraient nécessaires pour en garantir un traitement en bon ordre, ainsi que des Données devant être conservées en vertu d'une exigence réglementaire. Le CLIENT reconnaît qu'en raison du chiffrement des Données, en raison duquel ces dernières ne sont pas divulguées à ROCHE, celle-ci ne sera pas en mesure de sauvegarder ni de restaurer des ensembles de données déterminés mais uniquement la base de données dans son intégralité (par exemple, sous forme d'instantané). C'est au CLIENT qu'il incombe de traiter les Données de manière individualisée.
(2) Après l'achèvement des prestations définies dans le cadre d'une Commande, ou plus tôt sur demande du CLIENT, et au plus tard au moment où la Commande en question aura été entièrement honorée, ROCHE devra anonymiser ou détruire tous les documents, les résultats d'un traitement et d'une utilisation, ainsi que les ensembles de données liés au contrat, dont elle aura été en possession, dans le respect des règles relatives à la protection des données. Il en sera de même de tous éléments ayant servi à des tests, tous déchets et tous éléments redondants et mis au rebut. L'enregistrement de la destruction, de l'anonymisation ou de la suppression réalisée devra être fourni sur demande.
(3) Les documents utilisés pour démontrer un traitement de données en bon ordre, conforme à l'Accord relatif au traitement des données applicable, devront être conservés par ROCHE après qu'une Commande aura été honorée, en se référant à la durée de conservation obligatoire. ROCHE pourra remettre ces documents au CLIENT au terme de la durée du contrat afin de se libérer de cette obligation contractuelle.

12. RESPONSABILITÉ

(1) Le CLIENT ne saurait formuler à l'encontre de ROCHE plus d'une demande relative au même dommage ; sans qu'il importe de savoir si une telle demande résulte d'une Commande ou du Contrat, ni si un paiement a été effectué en lien avec un dommage particulier dans le cadre d'un Accord relatif au traitement des données.

Si une demande a été formulée et suivie d'un paiement, le montant de toute autre demande concernant le même dommage sera réduit de celui du paiement d'ores et déjà effectué.

Pièce jointe A - Mesures Techniques et Organisationnelles pour navify Sample Tracking

Le système, es contrôles opérationnelles et procéduraux, les procédures et les mesures suivantes ont été mis en œuvre dans navify Sample Tracking Essentials dès la conception afin de promouvoir un traitement et un stockage sécurisés des données à caractère personnel, d'atténuer le ou les risques de cybersécurité connus et de faciliter le respect des obligations pertinentes en matière de données à caractère personnel.

(a) Contrôle d'accès (utilisateurs externes / clients)

Installation de traitement : toutes les installations de traitement des données sont protégées contre les accès non autorisés grâce à des mesures d'authentification sécurisées

Centres de données : les centres de données gérés par AWS qui hébergent des données sensibles sont à la pointe de la technologie et utilisent des approches architecturales et d'ingénierie innovantes. Les centres de données sont hébergés dans des installations anonymes situées au sein de l'UE, en particulier dans la région de Francfort en Allemagne. L'accès physique est strictement contrôlé à la foi au niveau du périmètre et aux points d'entrée du bâtiment par le personnel de sécurité professionnel qui utilise la vidéosurveillance, les systèmes de détection d'intrusion, et autres moyens électroniques. Le personnel AWS autorisé doit réussi l'authentification à deux facteurs au moins 2 fois pour accéder aux étages du centre de données. Tous les visiteurs et les sous-traitants doivent présenter une pièce d'identité s'enregistrer et être en permanence accompagnés par le personnel autorisé.

L'accès physique aux centres de donnés n'est autorisé qu'aux personnes qui présentent un besoin professionnel légitime vis-à-vis de ces privilèges. Cela est déterminé par le politiques et procédures d'AWS et comprend à la fois les employés autorisés et les sous-traitants approuvés qui exécutent les services convenus dans l'environnement physique. L'lorsqu'un collaborateur ou un prestataire n'a plus de besoin des privilèges, son accès est immédiatement révoqué, même s'il garde son statut au sein de l'entreprise ; Tous les accès physiques aux centres de données sont systématiquement considérés et vérifiés par le biais de jetons physiques (badges) et d'exigences d'authentification secondaires (jetons des données biométriques, des pin) en fonction de l'emplacement spécifique saisi dans le centre de données. Tous les emplacements de prise en charge des clients nécessitent une authentification multifactorielle comme indiqué par AWS.
Les centres de données sont surveillés par le personne AWS afin de détecter les systèmes et équipements électriques, mécaniques et le maintien des fonctions vitales de sorte que tout problème éventuel soit immédiatement identifié. L'entretien préventif est effectué pour assurer le fonctionnement opérationnel continu de l'équipement.

Controle.d'accès électronique
La Solution navify Core Integrator (ci-après « nI") ne fournit pas d'accès utilisateur au système.

b) Contrôle d'accès (utilisateurs Roche)
La Solution nST-E fonctionne selon des politiques de contrôles visant à garantir l'absence de lecture, de copie, de modification ou de suppression non autorisées des données au sein du système, l'accès est déterminé spécifiquement en fonction du rôle que la personne exerce. Le personnel de Roche qui a accès à l'infrastructure nST-E n'a pas de droits d'accès aux données client décryptées stockées sur disque ou dans les journaux d'application contenant des données personnelles. Dans le cas d'assistance où des informations spécifiques sont requises, le personnel formé peut avoir accès limité aux données du Client

afin de résoudre la demande d'assistance. Ces cas sont documentés et ne produiront qu'à la demande du Client.

c) Audits et certifications
navify Sample Tracking utilise navify CLOUD Infrastructure pour déployer les différents compostants. Cette infrastrucure est certifiée ISO27001, ISO27017, ISO27018 and ISO2770.

d) Sauvegarde et récupération
Etant donnée la nature transitoire des données, celles-ci ne sont pas sauvegardées.

(e) Gestion des modifications et des versions
NST-E suit le document "SOP Agile Development process for Unregulated Software " pour implémenter le contrôle de tous les logiciels mis en œuvre et de la documentation de son système.

f) Minimisation des données

Seules les Données à Caractère Personnel nécessaires pour faciliter l'utilisation du produit sont collectées, NST-E agit en tant que sous-traitant et al décision sur les données finales à inclure pour les champs facultatifs repose sur le responsable de traitement.

g) Droit des Personnes Concernées

Le nST-E n'est pas utilisé par les personnes concernées. Les tiers ou les hopitaux gèrent les données, les données disponibles chez ROCHE sont supprimées pendant une période de 31 jours.

h) Chiffrement

L'échange de données au sein du système navify Sample Tracking et d'un tiers utilise un protocole de communication HTTP sécurisé, la communication au sein des composants nST-Edge et nST-Cloud se fait par le biais d'un canal VPN sécurisé. L'échange de données avec les nCI est protégé par des identifiants et la charge utile est cryptée. Des commentaires supplémentaires sur le cryptage peuvent être fournis sur demande. Le cryptage au repos n'a pas été appliqué, car les données ne restent que pendant une courte durée (7 jours) dans la base de données avant d'être purgées. La communication au sein de nST-Edge et du SIL dans le laboratoire n'est pas cryptée (HL7 simple), cet échange de données a lieu dans le réseau du laboratoire (pas de sortie du laboratoire).

(i) Correctifs, numérisation et tests de l'environnement

Les OTSS sont surveillés et seront mis à jour à la demande de l'organisation PSPO

(j) Durcissement
En fonction des résultats de l'évaluation des risques de cybersécurité des mesures de renforcement sont appliquées le cas échéant. Ceux-ci comprennent, sans s'y limiter :

- Définition des autorisations pour le comptes des utilisateurs et techniques sur la base des principes de privilège minimal et de séparation des tâches
- Limiter les communications entrantes et sortantes autorisées de tous les services réseau aux ports et systèmes nécessaires

- Application des paramètres de confihuration sécurisés par défaut
- Détection des modifications non autorisées de la configuration du système et restauration automatique de l'état souhaité
- Suivre les meilleures pratiques de sécurité comme le benchmark CIS

k) Surveillance et réponse aux incidents
Définition de flux de travail réactifs et proactifs pour les opérations.

l) Validation des données d'entrée

nST-E n'a pas d'entrée manuelle à valider car aucune IU n'est fournie à l'utilisateur final. La communication est basée sur les événements standard Roche 1.1 et 2.0 qui sont validés conformément à la disposition standard. nST
nST-E utilise l'authentification par point final par le biais de la définition de contrats de données, de champs prédéfinis et d'un processus de standardisation afin de limiter les entrées aux fournisseurs de données autorisés uniquement. Les champs de données qui ne sont pas dans le champ d'application de nST-E mais qui peuvent être fournis par une source authentifiée sont ignorés et ne font pas l'objet d'un traitement ultérieur.

m) Système(s) de gestion des clés
Les clés de cryptage des communications entre la périphérie et le réseau dorsal sont générées à l'aide de [l'infrastructure AWS | un ordinateur portable d'entreprise Roche | etc.] et LetsEncrypt. Ces clés sont stockées à l'aide de l'infrastructure AWS et sont automatiquement mises en rotation tous les 3 mois.

n) Emplacement et hébergement
Les composants nST sont hébergés dans la région AWS de Francfort, mais cette politique est flexible en fonction des exigences transfrontalières.

o) Enregistrement et surveillance
La journalisation nST-E est intégrée dans kubernetes/le système de journalisation par télémétrie et hébergée dans la région de données AWS. Les évènements de journalisation ne contiennent aucune données personnelle/patient. Les données de journalisation sont directement communiquées à fluent bit et de là, à la plateforme splunk. Aucune donnée du journal de données local n'est stockée sur le cluster.

p) sécurité réseau
La sécurité du réseau est assurée grâce à l'utilisation combinée de :
- Meilleures pratiques de mise en réseau AWS (groupes de sécurité, points de terminaison V¨PC, NACL configurés selon le principe de confiance zéro)
- Liste blanche IP.

Le dispositif périphérique s'assure que les certificats TLS corrects du back-end sont utilisés et se connecte à l'aide d'une connexion réseau cryptée. Toute tentative de connexion de tiers aux services à l'aide d'une connexion réseau non cryptée est redirigée vers une connexion à réseau à canal crypté

q) Le profilage, y compris a prise de décision individuelle automatisée
S/O : nST(E n'effectue aucun type de profilage

r) Périodes de conservation et d'élimination des données
Les Données personnelles sont stockées dans la base de données pendant un maximum de 7 jours pour le débogage et la récupération.

s) Enregistrement d'audité sécurisé
L'infrastructure nST-E fournit deux types de journaux d'audit. Mise en œuvre initiale sur la plateforme navify où l'infrastructure nST-E est déployée. Deuxièmement, nST-E lui-même est livré avec un journal d'audit au niveau de l'application. Les journaux d'audit sont examinés sur demande, les vulnérabilités et les incidents sont signalés, avant et après les correctifs/versions, et au moins une par an.

t) Tests et analyses de sécurité
La chaîne d'outils de développement d'applications est protégée par des tests de sécurité d'application statique (SAST) pour analyser le code source à la recherche de vulnérabilité communes, exécutées pour chaque build (SOnarQube). Les OTSS sont surveillés et évalués pour chaque version.
Infrastructure Cloud, Dome9 Best Practices Hight Severity Ruleset est l'ensemble de règles standard pour tous les comptes de la plateforme navify et des produits. Il contient les meilleures pratiques du secteur en matière de règles de sécurité et est surveillé pour fournir des environnements de production.

nST-E a créé une évaluation des risques. Les menaces identifiées et les contrôles de sécurité correspondants sont analysés et examinés avec l'équipe de projet pour décider si elles doivent être évitées, transférées, atténuées ou acceptées. Si la décision est d'atténuer les menaces, les contrôles respectifs sont documentés, mis en œuvre et validés de la même manière que tous les autres contrôles de sécurité.

u) Gestion des risques tiers
nST gère ses activités de tiers dans le cadre de ses propres activités de traitement tout au long du processus d'approvisionnement. Le responsable du traitement des données sera informé de manière proactive des modifications. Seuls des tiers externes évalués seront impliqués dans le traitement des informations personnelles et des clients. Les changements dans la situation de tiers feront l'objet d'une évaluation et d'une mise à jour du DPIA ou de ses pièces jointes. Les tiers sous contrôle de la plateforme navify ou d'autres composants sous-jacents couramment utilisés chez Roche sont gérés par la plateforme sans impact sur la présente évaluation. Les tiers agissant en tant que partenaires de Roche dans le cadre de la finalité de nST sont évalués par le contrôleur des données et nST car ils doivent respecter les règles de traitement énoncées dans le DPIA de nST. Les partenaires intégrés sont répertoriés dans le nST DPIA.

v) Transparence
nST n'interagit pas activement avec les utilisateurs et les personnes concernées, mais uniquement avec les systèmes. L'avis de non-responsabilité réglementaire n'a pas de public. Les responsables du traitement et les partenaires sont informés du traitement par nST.