CONTRAT DE TRAITEMENT DE DONNÉES [redacted]

Entre les soussignés

[redacted]

Ci-après dénommé « l'Hôpital »

ET

3M Belgium dont les bureaux sont situés à Hermeslaan 7, 1831 Diegem sous le numéro d'entreprise 0402683721, [redacted]

Ci-après dénommé « Fournisseur »

Ci-après dénommées conjointement les « Parties »

Attendu que

le Fournisseur fournit des services au profit de l'Hôpital, tels que décrits dans le Contrat de base. Ces services impliquent le traitement de données à caractère personnel et les parties au présent Addendum souhaitent fixer les accords concernant le traitement des données à caractère personnel dans le cadre des services,

il est convenu de ce qui suit :

1. Cadre conceptuel

1.1. Aux fins du présent Addendum, les définitions suivantes s'appliquent :

- Règlement général sur la protection des données : 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, avec ses modifications et la législation européenne d'application ;

- Législation en matière de protection des données : le règlement général sur la protection des données, d'autres règlements européens contenant des dispositions relatives à la protection des données et à la vie privée, ainsi que les lois nationales applicables en matière de protection des données et de vie privée dans les États membres, avec leurs modifications et actes d'application.

- Données à caractère personnel, Traitement, Responsable du traitement, Sous-traitant, Personne concernée, Consentement : les définitions telles qu'indiquées dans le règlement général sur la protection des données ;

- Contrat de base : le contrat entre l'Hôpital et le Fournisseur du [redacted] concernant la participation et l'accès au 3M Benchmark Portal. Le Fournisseur fournira des services à l'Hôpital sur la base du Contrat de base et tel que défini dans celui-ci.

- La qualification suivante s'applique aux activités de traitement telles que définies à l'Annexe 1 du présent Addendum :

    - l'Hôpital détermine la finalité et les moyens du traitement et est donc responsable du traitement ;

    - le Fournisseur effectue le traitement des données à caractère personnel pour le compte de l'Hôpital en tant que responsable du traitement et est donc sous-traitant.

2. Champ d'application et lien avec le contrat de base

2.1. Le présent Addendum fait partie intégrante du Contrat de base conclu entre l'Hôpital et le Fournisseur. Les dispositions du présent Addendum sont pleinement applicables à tous les traitements de données à caractère personnel que le Fournisseur effectue dans le cadre de l'exécution des activités de traitement déterminées à l'Annexe 1.

2.2. Les dispositions du présent Addendum (et de ses annexes) prévalent sur les dispositions (éventuellement différentes) du Contrat de base relatives à la protection et au traitement des données.

3. Traitement conforme à la réglementation et aux instructions écrites de l'Hôpital

3.1. Lors du traitement de données à caractère personnel, les Parties agissent conformément à la législation sur la protection des données.

3.2. Le Fournisseur traite les données à caractère personnel exclusivement sur la base des instructions écrites de l'Hôpital, déterminées unilatéralement par l'Hôpital et figurant à l'Annexe 1 du présent Addendum. Si les instructions écrites ne sont pas claires, le Fournisseur doit en faire rapport par écrit à l'Hôpital, après quoi les instructions doivent être clarifiées en concertation.

3.3. Sauf disposition contraire dans le présent Addendum, le Fournisseur ne traitera pas les données à caractère personnel à ses propres fins ou à celles de tiers, ni ne les communiquera à des tiers.

Si la réglementation européenne ou nationale impose au Fournisseur d'effectuer un traitement particulier, le Fournisseur devra en informer l'Hôpital préalablement au traitement, sauf si cette réglementation interdit cette notification pour des motifs importants d'intérêt public.

3.4. L'Hôpital donne des instructions au Fournisseur conformément à la législation sur la protection des données et garantit que toutes les données à caractère personnel confiées au Fournisseur ont été obtenues légalement et peuvent être traitées dans le cadre du Contrat de base.

En particulier, l'Hôpital s'assurera que toutes les Personnes concernées aient donné tous les consentements nécessaires, ou que la base légale nécessaire au traitement (telle que le besoin de diagnostic et de traitement) soit respectée, et qu'elles aient reçu toutes les informations nécessaires pour assurer un traitement équitable et transparent de leurs données à caractère personnel. L'Hôpital déclare et garantit que tout traitement de données à caractère personnel de l'Hôpital relatives à la santé d'une personne aux fins décrites par la présente est autorisé en vertu de la législation sur la protection des données, en ce y compris l'article 9 du règlement général sur la protection des données.

4. Mesures techniques et organisationnelles appropriées

4.1. Les Parties prennent les mesures techniques et organisationnelles appropriées pour garantir un niveau de sécurité adapté au risque.

4.2. Les mesures sont déterminées en tenant compte de l'état des connaissances, des coûts de mise en œuvre, ainsi que de la nature, de la portée, du contexte, des finalités du traitement, et des risques pour les droits et libertés des personnes en termes de probabilité et de degré de gravité.

Le cas échéant, ces mesures comprennent, entre autres, ce qui suit :

a) la pseudonymisation et le chiffrement des données à caractère personnel ;
b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;

c) des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;
d) une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

4.3. Lors de l'évaluation du niveau de sécurité approprié, il est tenu compte en particulier des risques que présente le traitement, résultant notamment de la destruction, de la perte, de l'altération, de la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou de l'accès non autorisé à de telles données, de manière accidentelle ou illicite.

4.4. Le Fournisseur est tenu de mettre en œuvre les mesures techniques et organisationnelles appropriées en tout temps, ainsi que de fournir toutes les informations complémentaires sur les mesures prises dans un délai raisonnable suivant la demande de l'Hôpital à cet effet.

5. Traitement par un « sous-traitant ultérieur » ou un employé

5.1. Le Fournisseur garantit que les dispositions du présent Addendum sont respectées par ses représentants, agents, sous-traitants et employés.

Le Fournisseur garantit, en outre, que :

- les personnes autorisées à traiter les données à caractère personnel se sont engagées à respecter la confidentialité ou sont soumises à une obligation légale appropriée de confidentialité ;

- que des mesures ont été prises pour que toute personne physique agissant sous son autorité et ayant accès aux données à caractère personnel ne les traite que sur instruction de l'Hôpital, à moins qu'elle ne soit obligée de les traiter en vertu de réglementations européennes ou nationales.

5.2. Le Fournisseur n'emploiera aucun autre sous-traitant (« Sous-traitant ultérieur ») sans l'autorisation écrite préalable, spécifique ou générale, de l'Hôpital.

L'Hôpital autorise par la présente 3M à nommer, licencier ou remplacer un ou plusieurs sous-traitants ultérieurs, y compris les Sociétés associées de 3M, pour traiter les données à caractère personnel de l'Hôpital au nom de l'Hôpital : (i) dans la mesure nécessaire à l'exécution de ses obligations contractuelles en vertu du Contrat de base ; et (ii) à condition que 3M demeure responsable des actions ou omissions de ses sous-traitants de la même manière que pour ses propres actions et omissions ci-dessous. Une liste des sous-traitants ultérieurs actuels figure à l'Annexe 3.

En ce qui concerne le traitement des données par son sous-traitant Smart Analytics Inc., tel que mentionné à l'Annexe 3, 3M a conclu des clauses

contractuelles types avec Smart Analytics Inc. au nom de ses clients de benchmarking, y compris l'Hôpital. En signant ce Contrat de sous-traitance, l'Hôpital confirme à 3M que les clauses contractuelles types ont aussi été conclues au nom de l'Hôpital. Une copie de ces clauses contractuelles types a été ajoutée à l'Annexe 4. Les Parties se consulteront de bonne foi s'il faut faire appel à d'autres sous-traitants ultérieurs en dehors de l'EEE.

5.3. 3M impose à ses sous-traitants des obligations qui sont conformes aux obligations de 3M en tant que sous-traitant des données dans le présent Contrat de sous-traitance. 3M informera l'Hôpital (p. ex. par e-mail) à l'avance (sauf dans le cas de remplacements urgents) de tout changement prévu concernant l'ajout ou le remplacement de sous-traitants ultérieurs, permettant à l'Hôpital de présenter des objections. Si l'Hôpital ne s'y oppose pas dans les quinze (15) jours suivant la communication des informations par 3M, le ou les nouveaux sous- traitants ultérieurs seront réputés avoir été acceptés. Si l'Hôpital s'y oppose, 3M a le droit de remédier à l'objection ou 3M peut résilier le Contrat de base et le présent Contrat de sous-traitance sans indemnité, sous réserve d'un préavis de trente (30) jours.

5.4. Si le sous-traitant ultérieur ne remplit pas ses obligations en matière de protection des données, le Fournisseur reste entièrement responsable envers l'Hôpital du respect des obligations du sous-traitant ultérieur.

6. <u>Assistance pour les obligations de l'Hôpital en matière de politique de protection des données</u>

6.1. Compte tenu de la nature du traitement et des informations dont il dispose, le Fournisseur s'engage raisonnablement à fournir une assistance à l'Hôpital sous la responsabilité de l'Hôpital afin de respecter les obligations suivantes en matière de protection des données :

- l'adoption de mesures techniques et organisationnelles appropriées pour garantir un niveau de sécurité adapté au risque ;
- la notification à l'autorité de contrôle des brèches de sécurité par rapport aux données à caractère personnel ;
- la communication d'une brèche de sécurité par rapport aux données à caractère personnel à la personne concernée ;
- la réalisation d'une analyse d'impact relative à la protection des données ;
- la consultation préalable de l'autorité de contrôle si l'analyse d'impact relative à la protection des données montre que le traitement présenterait un risque élevé si l'Hôpital ne prend pas de mesures pour atténuer ce risque.

Le temps et les ressources que le Fournisseur consacre à la fourniture de l'assistance sont à la charge du Fournisseur.

6.2. Dans le prolongement de l'article 6.1, le Fournisseur informera l'Hôpital en détail et sans retard déraisonnable d'une brèche de sécurité (présumée) relative aux

données à caractère personnel dès que le Fournisseur en aura eu connaissance. La notification doit être faite de manière à ce que l'Hôpital puisse remplir en temps utile ses obligations légales en tant que responsable du traitement conformément à la législation sur la protection des données.

Le Fournisseur fournit également une assistance dans l'investigation, la limitation et la réparation de toute brèche de sécurité relative au traitement des données à caractère personnel. Ce faisant, il fournira également une assistance, entre autres, dans le cadre de la documentation des mesures telles que la protection des données dès conception et par défaut.

6.3. Le Fournisseur doit raisonnablement informer l'Hôpital de toute plainte, accusation ou demande (y compris de la part d'un organisme de réglementation) concernant le traitement des données à caractère personnel par le Fournisseur en vertu du Contrat de base. Le Fournisseur fournira tout le soutien et toute l'assistance nécessaires auxquels l'Hôpital peut raisonnablement s'attendre en ce qui concerne une telle plainte, accusation ou demande, y compris en fournissant des renseignements complets sur cette plainte, accusation ou demande ainsi qu'une copie des données à caractère personnel de la Personne concernée qui sont en possession du Fournisseur.

7. Assistance pour les demandes des Personnes concernées

7.1. Compte tenu de la nature du traitement, le Fournisseur assistera l'Hôpital par des mesures techniques et organisationnelles appropriées dans son obligation de répondre à des demandes d'exercice des droits des Personnes concernées, comme prévu par la législation sur la protection des données.

Cela implique, entre autres :

- que le Fournisseur transmette toutes les données à caractère personnel demandées par l'Hôpital, dans le délai (raisonnable) demandé par l'Hôpital, y compris dans tous les cas les détails complets et les copies de la plainte, de la communication ou de la demande et toutes les données à caractère personnel en sa possession concernant une Personne concernée ;

Le temps et les ressources que le Fournisseur consacre à la fourniture de l'assistance sont à la charge du Fournisseur.

7.2. Dans le prolongement de l'article 7.1, le Fournisseur s'engage à informer sans délai l'Hôpital s'il reçoit l'une des demandes suivantes d'une Personne concernée (ou d'un tiers agissant au nom d'une Personne concernée) :

- une demande d'accès aux données à caractère personnel de la Personne concernée qui sont traitées ;
- une demande de rectification des données à caractère personnel inexactes ;
- une demande d'effacement de données à caractère personnel ;

- une demande de limitation du traitement des données à caractère personnel ;

- une demande d'obtention d'une copie portable des données à caractère personnel ou de transfert d'une copie à un tiers ;

- une opposition à tout traitement de données à caractère personnel ; ou

- toute autre demande, plainte ou communication relative aux obligations de l'Hôpital en vertu de la législation sur la protection des données.

Le Fournisseur ne répond pas aux demandes et requêtes des Personnes concernées, à moins que l'Hôpital et le Fournisseur n'en conviennent autrement par écrit.

8. Droit de contrôle de l'Hôpital

8.1. L'Hôpital a toujours le droit de vérifier la conformité du Fournisseur à l'Addendum.

Le Fournisseur fournira à l'Hôpital tous les renseignements nécessaires pour démontrer le respect des obligations découlant de la législation sur la protection des données.

Le Fournisseur doit faciliter les audits, y compris les inspections, effectuées par l'Hôpital ou par un contrôleur autorisé par l'Hôpital, et y participer. Le Fournisseur doit collaborer pleinement à un tel audit et doit, à la demande de l'Hôpital, fournir une preuve de conformité à ses obligations en vertu du présent Addendum.

8.2. Le Fournisseur informera immédiatement l'Hôpital si, à son avis, une instruction en vertu de l'article 8.1 constitue une infraction à la législation sur la protection des données.

Sauf si la législation sur la protection des données l'exige, un contrôle est limité à une fois par période de douze mois et ne peut excéder trois jours ouvrables.

L'Hôpital informera 3M par écrit d'une inspection dans un délai raisonnable (au moins 60 jours civils, à moins qu'une autorité de protection des données ne demande à l'Hôpital de procéder à une inspection plus tôt).

L'hôpital et 3M déterminent à l'avance, en concertation, la portée et la nature du contrôle. Le contrôle est basé, dans la mesure du possible, sur des certifications et des rapports de contrôle ou d'autres vérifications disponibles afin de confirmer que 3M respecte le Contrat de sous-traitance et d'éviter les contrôles répétés.

L'Hôpital effectuera le contrôle dans des conditions raisonnables en termes de temps, lieu et méthode et 3M fournira une copie du rapport de contrôle.

L'Hôpital et 3M assumeront chacun leurs propres frais pour les contrôles.

9. Responsabilité

9.1. Chacune des Parties assume l'entière responsabilité de ses propres actions. La responsabilité visée au présent article concerne exclusivement la responsabilité résultant d'une infraction à la législation sur la protection des données et au présent Addendum.

9.2. Le Fournisseur est responsable et indemnise l'Hôpital de tous les dommages causés aux Personnes concernées, résultant directement d'un traitement de données à caractère personnel tel que défini dans le présent Addendum et pendant le traitement par le Fournisseur (i) lorsque les obligations spécifiquement imposées aux sous-traitants en vertu du RGPD n'ont pas été respectées, ou, (ii) lorsque ledit traitement a été effectué d'une manière différente ou va à l'encontre des instructions légitimes de l'Hôpital.

9.3. Les Parties s'indemnisent mutuellement contre les amendes infligées par l'autorité compétente en matière de protection de la vie privée, mais qui résultent directement et exclusivement (i) du non-respect par l'autre partie du présent Addendum ; ou (ii) du non-respect par l'autre partie de ses obligations en vertu de la législation sur la protection des données dans le cadre du traitement des données tel que défini par le présent Addendum. Les circonstances aggravantes de la part d'une partie, y compris, mais sans s'y limiter, le récidivisme ou la non-coopération, sont entièrement à la charge de la partie en question.

9.4. L'indemnisation est subordonnée à la condition que la personne qui reçoit la réclamation ou l'amende en informe immédiatement l'autre partie et lui donne la possibilité de coopérer à la défense et au traitement de la réclamation ou de l'amende.

9.5. À l'exception des dispositions de l'article 82 du RGPD relatives aux dommages causés aux Personnes concernées (qui conservent leur propre droit d'action contre le sous-traitant et le responsable du traitement), les parties ne sont pas mutuellement responsables des dommages consécutifs, tels que, mais non limités au manque à gagner, au préjudice subi, à la perte de clientèle, à l'arrêt des activités ou aux atteintes à la réputation. La responsabilité pour les dommages directs est limitée au montant facturé à l'Hôpital par 3M dans le cadre du Contrat de base dans l'année civile au cours de laquelle le dommage survient.

9.6. La limitation de responsabilité prévue à l'article 9.5 ne s'applique pas en cas d'intention ou de négligence volontaire de la part de la partie qui souhaite invoquer cette limitation.

9.7. Si l'Hôpital et le Fournisseur sont tous deux responsables des dommages causés par des activités de traitement contraires à la législation sur la protection des

données, chaque partie est responsable envers l'autre partie du montant du dommage correspondant à sa part de responsabilité dans le dommage.

9.8. L'Hôpital reconnaît que le Fournisseur dépend de l'Hôpital pour obtenir des instructions concernant les fins et la mesure dans laquelle le Fournisseur est autorisé à utiliser et à traiter les données à caractère personnel de l'Hôpital. Le Fournisseur n'est pas responsable, et l'Hôpital indemnise le Fournisseur de toute plainte (y compris toute plainte déposée par une Personne concernée) ou de tout dommage en rapport avec ou découlant : (i) du traitement par le Fournisseur de données à caractère personnel de l'Hôpital conformément au présent Contrat de sous-traitance ; et/ou (ii) du manquement de l'Hôpital à l'une de ses obligations en vertu du présent Contrat de sous-traitance et/ou de la législation sur la protection des données.

9.9. Les Parties veillent à ce que leur responsabilité soit couverte de manière adéquate.

10. Fin du contrat

10.1. Si le Fournisseur ne remplit pas correctement les obligations découlant du présent Addendum et ne prend pas les mesures appropriées dans un délai maximum de deux mois, l'Hôpital peut – sans préjudice des autres motifs de résiliation prévus dans le Contrat de base – résilier immédiatement le Contrat de base après le délai de deux mois mentionné ci-dessus et/ou mettre un terme à la mission de traitement.

10.2. Ce contrat fait partie intégrante du Contrat de base et suit donc le sort du Contrat de base. En cas de résiliation du Contrat de base, les dispositions du présent Addendum restent valables dans la mesure nécessaire à l'exécution des obligations conformément à la législation sur la protection des données.

10.3. Immédiatement après la résiliation ou l'expiration du Contrat de base, ou après l'expiration de la période de conversation, le Fournisseur devra – à la discrétion de l'Hôpital – retourner les données à caractère personnel à l'Hôpital et/ou les effacer complètement et irrévocablement, et supprimer les copies existantes. Dans le cas où l'Hôpital opte pour la suppression des données à caractère

personnel, le Fournisseur devra démontrer à la demande écrite de l'Hôpital que les données ont bel et bien été supprimées.

Le Fournisseur peut déroger au premier alinéa si les données à caractère personnel doivent être conservées en vertu de la législation européenne ou nationale.

11. Dispositions finales

11.1. En cas de nullité ou d'annulation d'une ou plusieurs dispositions du présent Addendum, les autres dispositions restent pleinement en vigueur.

11.2. Le présent Addendum est régi par le droit belge. Les litiges sont soumis au tribunal néerlandophone de Bruxelles, qui a compétence territoriale exclusive.

Ainsi convenu et signé en deux exemplaires à [redacted]

[redacted] 3M Belgium SPRL

[redacted]

Annexes

Annexe 1 : mission et instructions de traitement telles que déterminées par l'Hôpital
Annexe 2 : sécurité de l'information
Annexe 3 : Liste des sous-traitants
Annexe 4 : Standard contractual clauses

ANNEXE 1 - MISSION ET INSTRUCTIONS DE TRAITEMENT TELLES QUE DETERMINEES PAR L'HOPITAL

Note d'accompagnement

Dans la présente Annexe sont décrit les traitements spécifiques effectués par le Fournisseur à qui l'Hôpital en donne la mission au moment du Contrat de base ou à la signature du présent Addendum.

Les modifications et/ou ajouts à la présente Annexe 1 sont toujours effectués au moyen d'un document séparé joint à la présente Annexe 1 (Annexe 1 de l'Annexe 1 ; Annexe 2 de l'Annexe 1, etc.), daté et reprenant l'instruction et/ou l'autorisation explicite et écrite de l'Hôpital.

I. Finalité du traitement des données à caractère personnel

Le traitement des données à caractère personne par le Fournisseur aura lieu dans le cadre de l'exécution du Contrat de base sur la participation et l'accès au 3M Benchmark Portal.

Description des services prévus par le Contrat de base et de la nature et de la finalité du traitement des données à caractère personnel dans le cadre des services :

> Analyse des données hospitalières dans le but d'établir une comparaison entre les différents hôpitaux impliqués dans ce projet et de fournir des informations au moyen d'analyses et de rapports sur les indicateurs de performance et de qualité au niveau des hôpitaux.

II. Les catégories de données à caractère personnel que l'Hôpital fait traiter par le Fournisseur (indiquer ce qui est applicable et compléter si nécessaire) :

- ☒ données de contact
- ☐ données financières en cas de participation à CAMS
- ☐ données de facturation
- ☒ données salariales
- ☐ données médicales
- ☒ données marketing
- ☐ données sur l'utilisation par l'Hôpital des services et produits connexes du Fournisseur
- ☐ autre (à préciser) :
  Liste des médecins avec numéro d'identification interne (généralement le numéro INAMI)

III. Les catégories de Personnes concernées dont les données à caractère personnel font l'objet d'un traitement (indiquer ce qui est applicable et compléter si nécessaire) :

- ☐ les patients de l'Hôpital
- ☒ les personnes de confiance, les représentants et les personnes de contact des patients de l'Hôpital
- ☒ les prestataires de soins des patients de l'Hôpital
- ☒ le personnel de l'Hôpital

- autres (à préciser) :

IV. Le traitement des données à caractère personnel (indiquer ce qui est applicable et adapter/compléter si nécessaire) :

L'Hôpital donne par les présentes les instructions suivantes pour le traitement des données à caractère personnel (sans préjudice des instructions qui découlent directement des dispositions du Contrat de base ou du présent Addendum ou qui sont raisonnablement nécessaires à la bonne exécution par le Fournisseur de ses obligations) :

- Consultation des données du personnel

  Il s'agit des services du Fournisseur par lesquels les données du personnel de l'Hôpital peuvent être consultées par les employés ou les sous-traitants du Fournisseur, y compris, mais sans s'y limiter, le Service Desk, les Services de contrôle (à distance), les Services de gestion des systèmes, les Services de gestion des applications techniques, les Services d'analyse de la vulnérabilité, les Services de reporting en gouvernance, et les Services de gestion des actifs logiciels.

- Stockage des données des patients

  Il s'agit des services fournis par le Fournisseur dans le cadre desquels les données des patients de l'Hôpital sont stockées dans un système de stockage fourni par le Fournisseur, y compris, mais sans s'y limiter, les Services de stockage dans le cloud, les Services de sauvegarde dans le cloud, les Services de fichiers, les Services de répertoire, le transfert de fichiers géré, la messagerie électronique et l'agenda et le traitement des fichiers journaux.

- Transfert des données de patients

  Il s'agit des services du Fournisseur par lesquels les données des patients de l'Hôpital sont envoyées à partir, à destination ou entre des applications sur une plateforme gérée par le Fournisseur, tels que, mais sans s'y limiter, les Services LAN, les Services de réseau étendu, les Services d'interconnectivité de centres de données, la répartition de charge, les interconnexions d'îlots SAN et les Services fournis sur le protocole VoIP (Voice over Internet).

- Mise à jour ou modification des données de patients

  Il s'agit des services du Fournisseur où les données des patients de l'Hôpital peuvent être modifiées à la fois manuellement et de manière automatisée comme dans un flux de travail automatisé supporté par un système de planification des tâches.

- Test de logiciels

  Il s'agit des services fournis par le Fournisseur dans le cadre desquels des bases de données de l'Hôpital contenant des données de patients (données de patients pseudonymisées) sont utilisées en dehors de l'environnement de production (en test, acceptation...) dans le cadre du processus de test de l'application logicielle de l'Hôpital.

IV. Les périodes de conservation des (différentes catégories de) données à caractère personnel :

Le Fournisseur conservera les données à caractère personnel traitées de manière suffisamment sécurisée pendant la période nécessaire à l'exécution des instructions écrites de l'Hôpital et, pour les catégories suivantes de données à caractère personnel, durant la période indiquée ci-dessous

- pour toutes les catégories au minimum 3 ans et au maximum 4 ans

V. Le Délégué à la protection des données ou d'autres personnes de contact chargées de la protection des données et du traitement des données (à compléter) :

[redacted]

Pour le Fournisseur
Nom : [redacted]
Données de contact : E-mail : [redacted]@mmm.com

Questionnaire on information security and data protection for the processor

Name of the organisation (third party)	Name: 3M Belgium bvba/sprl Address: Hermeslaan 7 1831 Diegem Business number (Crossroads Bank): BE 0402.683.721
First name, Surname & e-mail address of the chief information security officer (CISO) (mandatory)	[redacted] [redacted]@mmm.com
First name, Surname & e-mail address of the information security contact person (assistant CISO) (optional)	....
First name, Surname & e-mail address of the data protection officer (DPO) (mandatory)	[redacted] [redacted]@mmm.com
First name, Surname & e-mail address of the local data protection contact person (assistant DPO or representative) (optional)	....

First name, Surname & e-mail address of the person responsible for day-to-day management (CEO, mandatory)	[redacted] [redacted]@mmm.com

Question	*Place cross (X) in the box corresponding to your answer*		Explain in the case of a 'no' response
1	Do you have a formal, up-to-date information security policy approved by the person responsible for day-to-day management?	☒ YES ☐ NO	
2	Do you have a risk assessment for each process/project for information security/data protection which you use for the provision of services?	☒ YES ☐ NO	
3	Within your organisation: • is there a department responsible for information security reporting directly to the person responsible for day-to-day management of the organisation?	☒ YES ☐ NO	
4	Do you have an information security plan approved by the person responsible for day-to-day management?	☒ YES ☐ NO	
5	How many hours are worked by the CISO and his/her team? • CISO • Team How many hours of training on information security have the DPO and his/her team followed? • DPO • Team	1) 200 hours/month 2) 200 hours/month 3) 4 hours/year 4) 4 hours/year	
6	Do you have procedures for the development of new systems or major changes to existing systems so that the project leader can take account of the security requirements described in the minimum security standards?	☒ YES ☐ NO ☐ N/A	
7	Do you take appropriate measures so that the professional, confidential and sensitive data stored on mobile media are accessible only to authorised persons?	☒ YES ☐ NO	

Question	*Place cross (X) in the box corresponding to your answer*		Explain in the case of a 'no' response
8	Do you take appropriate measures, depending on the access medium, for the information security of the access from outside your organisation to the professional, confidential and sensitive data?	☒YES ☐ NO	
9	Do you have teleworking facilities arranged in such a way that at the teleworking location (at home, in a satellite office or in another location) no information is stored on external appliances without encryption and that possible threats from the teleworking location do not reach the IT infrastructure?	☒YES ☐ NO	
10	Do you call the attention of each staff member each year to information security and data protection and do you carry out an annual evaluation of compliance with this policy in practice?	☒YES ☐ NO	
11	Have you secured access by means of a clear access procedure and have you implemented a (logical or physical) access system to prevent any unauthorised access?	☒YES ☐ NO	
12	Do you have a classification system for personal data for which you are providing the services and do you apply this classification system?	☒YES ☐ NO	
13	Have you processed the rules, specified in an 'E-mail, online communication and internet use' policy line, in an information security policy?	☒YES ☐ NO	
14	Have you appointed at least one access manager when you make use of remote access to the healthcare institution?	☐YES ☐ NO ☒ N/A	3M does not connect to the healthcare institution's infrastructure.
15	Have you encouraged your staff to read and apply extra security measures which the care provision imposes (if applicable)?	☐YES ☐ NO ☒ N/A	3M does not connect to the healthcare institution's infrastructure.

Question	*Place cross (X) in the box corresponding to your answer*		Explain in the case of a 'no' response
16	If you wish to apply 'cryptography': • do you have a formal policy for the use of cryptographic controls? • do you have a formal policy for the use, protection and life of cryptographic keys for the entire lifecycle?	☒YES ☐ NO	
17	Do you take the necessary measures to limit access to the buildings and premises to authorised persons and do you monitor this access both during and outside working hours?	☒YES ☐ NO	
18	Do you take the necessary measures to prevent loss, damage, theft or compromise of equipment and interruption of the activities?	☒YES ☐ NO	
19	In the case of reuse of the information carrier, do you use it again at a data classification level which is at least comparable?	☒YES ☐ NO	
20	Do you establish appropriate measures for the erasure of data contractually with the principal?	☒YES ☐ NO	
21	Do you apply the rules relating to logging of access as stipulated by the principal?	☐YES ☒ NO	We log everything according 3M rules
22	Have rules been laid down for the acquisition, development and maintenance of systems between the various parties concerned?	☒YES ☐ NO	
23	Do all staff members work with ICT resources for the purposes of the assignment on the basis of minimum authorisation for the performance of their task?	☒YES ☐ NO	
24	Have the access security requirements (identification, authentication, authorisation) been defined, documented, validated and communicated? Are these accesses logged?	☒YES ☐ NO ☒YES ☐ NO	

Question	*Place cross (X) in the box corresponding to your answer*		Explain in the case of a 'no' response
25	Are the security and data protection risks established contractually between you and any subcontractors?	☒YES ☐ NO	
26	Do you use a checklist so that the project leader can obtain the assurance that all the information security and data protection policy lines have been evaluated correctly and if necessary implemented during the development phase of the project?	☐YES ☒ NO	We don't use a checklist. Information security & data protection are subject of separate business logic (privacy analytics).
27	Each time a project is put into production, do you carry out a check that the security and data protection requirements laid down at the beginning of the project were also in fact implemented?	☒YES ☐ NO	
28	Under the supervision of the project leader, are there separated facilities for development, testing and/or acceptance and production – including the related separation of the responsibilities under the project?	☒YES ☐ NO	
29	Is each access to personal and confidential data logged in accordance with a logging policy and the applicable laws and regulations?	☐YES ☒ NO	No PHI data is stored in the DB.
30	Is it included in project specifications how access to and use of systems and applications will be logged to contribute to the detection of divergences with regard to information security and data protection?	☒YES ☐ NO	
31	Does the log management at least comply with the following objectives? • The information to be able to determine by whom, when and how access was obtained to which information • The identification of the nature of the information consulted • The clear identification of the person	☒YES ☐ NO	
32	Have the necessary tools been made available to allow the log data to be operated by the authorised persons?	☒YES ☐ NO	
33	Do the transactional/functional log data correspond to the storage period corresponding to the data themselves (e.g. 30 years for medical data)?	☒YES ☐ NO	

Question	*Place cross (X) in the box corresponding to your answer*		Explain in the case of a 'no' response
34	Are the project deliverables (processed data, documentation (source code, programs, technical documents, etc.) integrated in the back-up management system?	☒YES ☐ NO	
35	In the course of the project development, have the requirements with regard to continuity of service provision been formalised, in accordance with your expectations?	☐YES ☐ NO ☒ N/A	3M Benchmark Portal is not considered a mission critical system
36	Have your continuity plan and the related procedures been updated in line with the development of the project, including continuity tests?	☐YES ☐ NO ☒ N/A	3M Benchmark Portal is not considered a mission critical system
37	Is a risk analysis carried out at the beginning of the project to define the emergency procedures?	☐YES ☐ NO ☒ N/A	3M Benchmark Portal is not considered a mission critical system
38	In the course of the project development, are the procedures concerning incident management formalised and validated?	☐YES ☒ NO	Not required, we have other ways to handle incidents in the development phase
39	Is the CISO informed of security incidents and the DPO for incidents concerning data protection?	☒YES ☐ NO	
40	During the lifecycle of the project, is the documentation (technical, procedures, manuals, etc.) kept up to date?	☒YES ☐ NO	
41	Is all equipment, including purchased or developed systems added to the inventory of the operational resources?	☒YES ☐ NO	
42	Is appropriate cooperation given to audits carried out in the form of the personnel being made available, documentation, log management and other information which is reasonably available?	☒YES ☐ NO	
43	Are requirements concerning information security and data protection documented to mitigate risks concerning access to information tools?	☒YES ☐ NO	
45	Are all relevant requirements concerning information security and privacy drawn up and agreed between you and third parties/suppliers (who	☒YES ☐ NO	

Question	*Place cross (X) in the box corresponding to your answer*		Explain in the case of a 'no' response
	read, process, store, communicate information of the organisation or supply ICT infrastructure components and ICT services)?		
46	Are the services provided to you by third parties/suppliers monitored, evaluated and audited?	☒ YES ☐ NO	
47	Are the changes in the provision of services to you by the third party/supplier managed, including keeping records of existing policy lines, procedures/measures for information security and data protection?	☒ YES ☐ NO	
48	Do you have a 'Cloud computing' policy line when you call on cloud services?	☒ YES ☐ NO	
49	When you wish to process professional, confidential or sensitive data in a cloud, do you satisfy the minimum contractual guarantees?	☒ YES ☐ NO	
50	Do you have procedures for establishment and management of incidents relating to information security or data protection with the related responsibilities and have you made these procedures known in-house?	☒ YES ☐ NO	
51	Do you have an agreement with all staff members that each staff member (permanent or temporary, in-house or external) is required to report unauthorised access, use, alteration, disclosure, loss or destruction of information and information systems?	☒ YES ☐ NO	
52	Are the incidents and weaknesses of information security or data protection relating to information and information systems made known to the principal so that you and the principal can take appropriate corrective measures in good time?	☒ YES ☐ NO	
53	Does the supplier have a procedure to communicate/report incidents concerning information security/data protection in-house as quickly as possible?	☒ YES ☐ NO	

Question	*Place cross (X) in the box corresponding to your answer*		Explain in the case of a 'no' response
54	In the case of information security or data protection incidents, is the evidence collected correctly in accordance with statutory and regulatory requirements?	☒YES ☐ NO	
55	Is each information security or data protection incident formally validated so that procedures and control measures can be improved and are the lessons drawn from an incident communicated to your management for validation and approval of further actions?	☒YES ☐ NO	
56	Do you have a continuity plan for all critical processes and essential information systems?	☐YES ☐ NO ☒ N/A	3M Benchmark Portal is not considered a mission critical system
57	Are information security and data protection an integral part of your continuity management?	☐YES ☐ NO ☒ N/A	3M Benchmark Portal is not considered a mission critical system
58	Do you have your own continuity plan? Is this plan tested and adapted regularly with the necessary communication to your management for validation and approval?	☐YES ☐ NO ☒ N/A	3M Benchmark Portal is not considered a mission critical system
59	Do you carry out a conformity audit periodically with regard to the situation concerning information security and data protection?	☒YES ☐ NO	
60	Do you have a formal disciplinary process for employees who have breached information security and data protection?	☒YES ☐ NO	
61	Do you regularly collate all information to map the risks in connection with conformity with the GDPR and do you take the necessary actions as a result of a high 'residual' risk of non-conformity?	☒YES ☐ NO	
62	Do you have an up-to-date central register of the controller or of the processor and do you have formal accountability for non-implementation of control measures focusing on compliance with the European Regulation for the specific processing?	☒YES ☐ NO	

Date and signature of the CISO or data management officer (DPO) of the organisation (third party) (optional)	..... Date Signature
Date and signature of the person responsible for the day-to-day management of the organisation (third party) **(mandatory)**	3M BELGIUM BVBA [redacted]

******* END OF THIS DOCUMENT *******

ANNEXE 3 : LISTE DES SOUS-TRAITANTS

Cette annexe 3 fait partie intégrante du CONTRAT.

Nom	Localisation	Rôle
Smart Analytics Inc.	Russie	- Développement et maintenance du code source et; - maintenance et mises à jour de la base de données, sur la base ensembles de données RHM et Carenet pseudonymisées.
PlusServer	Allemagne	Serveurs de stockage des données.
LVA Health Consultancy	Belgique	- support de l'application ; - formation et support client ; - accès aux FEEDBACK, pas d'accès aux DONNÉES

ANNEXE 4: STANDARD CONTRACTUAL CLAUSES

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation:

3M Belgium BVBA*

Address: Hermeslaan 7, 1831 Diegem

Other information needed to identify the organisation

Registered under Company Number: 0402.683.721

(hereinafter referred to as "3M" or the "data exporter")

** On behalf of its benchmarking customers, being the hospitals in Belgium and Luxemburg that have entered into a written benchmarking agreement including data processing agreement with 3M Belgium BVBA.*

And

Name of the data importing organisation:

Smart Analytics Inc.

Address: 1250 Connecticut Ave NW, Suite 200, Washington DC, 20036

Other information needed to identify the organisation:

Registered under Company Number: 81-4309507

(hereinafter referred to as "SAI" or the "data importer")

each a 'party'; together 'the parties',

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

3M Belgium BVBA acts as a data processor under the benchmarking agreements it has entered into with its customers, being hospitals in Belgium and Luxembourg, for which it performs benchmarking services which includes the processing of personal data per the instruction of the hospitals. As part of the benchmarking activities performed by 3M as data processor, SAI, a company established in a third country, has access to the data and acts as a sub processor of 3M.

For practical reasons, 3M enters into these Standard Clauses with SAI directly on behalf of the hospitals having a signed benchmarking agreement with 3M.

Clause 1

Definitions

For the purposes of the Clauses:

(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ([1]);

(b) 'the data exporter' means the controller who transfers the personal data;

(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) 'the sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by

operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance

with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer ([2])

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

(ii) any accidental or unauthorised access; and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial

information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the

security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

Clause 9

Governing law

The Clauses shall be governed by the law of the Member State in which the data exporter is established, namely Belgium.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Sub-processing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses (3). Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

2. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by

contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established, namely Belgium.

4. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data-processing services

1. The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

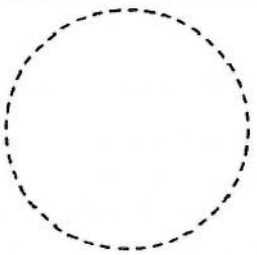
On behalf of the data exporter:

Name (written out in full): [redacted]

Position: [redacted]

Address: Hermeslaan 7, 1831 Diegem, Belgium

Other information necessary in order for the contract to be binding (if any):

	Signature [redacted]

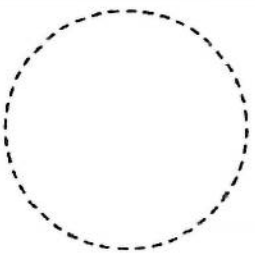
On behalf of the data importer:

Name (written out in full): [redacted]

Position: [redacted]

Address: 1250 Connecticut Ave NW, Suite 200, Washington DC, 20036…

Other information necessary in order for the contract to be binding (if any):

	Signature [redacted]

Appendix 1

to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

The Data is not transferred as such but resides on a private cloud infrastructure in Germany i.e. the Portal. There is only one secure way of uploading coded Data onto the Portal with the data protection tool. Once the coded Data is accepted it resides on the Portal during its entire lifetime of the benchmarking contract.

Data importer

The data importer is (please specify briefly activities relevant to the transfer):

The data importer has a secure access to the Portal to access the Data.

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

Hospital patients

Categories of data

The personal data transferred concern the following categories of data (please specify):

Identifiable Personal Data (see next category)

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

Health Data

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

Creation of benchmarking reports for various stakeholders of a hospital and providing related support.

DATA EXPORTER

Name: 3M Belgium BVBA, on behalf of its benchmarking customers

Authorised Signature:

DATA IMPORTER

Name: Smart Analytics Inc.

Authorised Signature ...

Appendix 2

to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Once the Data is received, the Data Exporter deidentifies the dataset so that original identifiers cannot be seen by people having access to the database unless they are authorized to do so. This means that developers (working from outside the EU) working on the databases on which the Portal operates will not see any identifiers. Deidentification is done using a third party software called Eclipse from Privacy Analytics.

The data flow, and the de-identification process (in green) can be visually described as in the chart below. Once the Data is uploaded to the 3M environment, the Data is transferred to the "3M ETL TEMP DB", where the Data is deidentified and transferred to the "3M ETL DB" . The original identifiers are stored in a separate DB "3M PHI", to which the development team does not have access. The original identifiers are only retrieved on the fly at time of analysis, when the data is retrieved by a login to which the access of the hospital's data is granted.