DATA PROTECTION AGREEMENT

ENGLISH / FRENCH VERSION

Data Protection Agreement

This Data Protection Agreement ("**Agreement**") executed with regard to the processing of PII (as defined below), in accordance with any applicable Distribution Agreement ("**Main Agreement**") entered into between you (the "**Controller**") and **I.M.E 2016 B.V.**, on behalf of itself and its affiliates (collectively, "**Processor**"). All defined terms contained herein shall have the same meaning as the definitions set forth in the Main Agreement.

In the event of any discrepancy between the English and French versions, the English version shall prevail.

Processor shall comply with the following in respect of personal data and/or personal identifiable information (as defined under Regulation (EU) 2016/679 (General Data Protection Regulation) ("**PII**" and "**GDPR**" respectively):

1. **Controller's Compliance**. Controller's instructions for processing of PII shall comply with all applicable privacy and data protection laws, including (as applicable) the GDPR and the French Data Protection Act n°78/17 6 January 1978. Controller shall have sole responsibility for the accuracy, quality and legality of PII and the means by which Controller acquired PII.

Contrat de Protection des Données (DPA)

Ce Contrat de Protection des Données (ci-après "**DPA**") est conclu dans le cadre du traitement de Données Personnelles (telles que définies ci-dessous), conformément à tout Contrat de Distribution applicable (ci-après "**Contrat principal**") conclu entre vous (ci-après, le "**Responsable de traitement**") et **I.M.E 2016 B.V**, en son nom et au nom de ses affiliés (collectivement, le "**Sous-traitant**"). Tous les termes définis contenus dans le présent DPA ont la même signification que les définitions énoncées dans le Contrat principal.

En cas de différence entre la version anglaise et la version française, la version anglaise prévaudra.

Le Sous-traitant doit se conformer à ce qui suit en ce qui concerne les Données Personnelles, telles que définies dans le Règlement (UE) 2016/679 dit « Règlement général sur la protection des données » (respectivement "**Données Personnelles**" et "**RGPD**") :

1. Conformité du Responsable de traitement. Les instructions du Responsable de traitement concernant le traitement des Données Personnelles doivent être conformes à toutes les lois applicables en matière de confidentialité et de protection des données, y compris (selon le cas) le RGPD et la loi française sur la protection des données n°78/17 du 6 janvier 1978. Le Responsable de traitement est seul responsable de l'exactitude, de la qualité et de la légalité des Données Personnelles et des moyens par lesquels le Responsable de traitement a collecté les Données Personnelles.

1. **Details of Processing**. The details of the processing activities to be carried out by Processor are specified in **Annex 1**.

2. **Processing only on documented instructions:** The Processor will only process PII on documented instructions from the Controller, unless required to do so by law to which Processor is subject. In such a case, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest. The parties agree that all documented instructions regarding the processing are contained within this Agreement and the Main Agreement. The parties also agree that any further instructions regarding the processing of PII must be provided in writing by the Controller to the Processor and they must be consistent with the Processor's preexisting obligations under this Agreement and the Main Agreement.

3. **Data Subjects Rights**. Processor shall assist Controller, by using appropriate technical and organizational measures, in the fulfillment of Controller's obligations to respond to requests by data subjects in exercising their rights under applicable laws.

2. Détails du traitement. Les détails des activités de traitement à effectuer par le Sous-traitant sont spécifiés à **l'Annexe 1**.

3. Traitement uniquement sur instructions documentées : Le Sous-traitant ne traitera les Données Personnelles que sur instructions documentées du Responsable du traitement, à moins que la loi à laquelle le Sous-traitant est soumis ne l'y oblige. Dans ce cas, le Sous-traitant informe le Responsable du traitement de cette exigence légale avant le traitement, à moins que cette loi n'interdise cette information pour des raisons importantes d'intérêt public. Les parties conviennent que toutes les instructions documentées concernant le traitement sont contenues dans le présent Contrat et dans le Contrat principal. Les parties conviennent également que toute instruction supplémentaire concernant le traitement des Données Personnelles doit être fournie par écrit par le Responsable du traitement au Sous-traitant et qu'elle doit être conforme aux obligations préexistantes du Sous-traitant en vertu du présent Contrat et du Contrat principal.

4. Droits des personnes concernées. Le Sous-traitant assiste le Responsable de traitement dans l'accomplissement de ses obligations quant aux demandes des personnes concernées dans l'exercice de leurs droits en vertu des lois applicables, en utilisant des mesures techniques et organisationnelles appropriées.

4. **Data Subject Information.** Controller represents and warrants that, where it provides any PII to Processor for processing or where it contacts any data subjects through the PII provided by Processor:

   (a) it has duly informed the relevant data subjects of their rights and obligations, obtained their consent if necessary, and in particular has informed them of the possibility of Processor processing their PII on the Controller's behalf and in accordance with its instructions;

   (b) it has complied with all applicable data protection legislation in the collection and provision to Processor of such PII. Specifically, the Controller ensures that any disclosure PII to Processor is PII that has been collected lawfully, i.e. processed on a legal basis as described in the articles 6-10 of the GDPR;

   (c) the processing of such PII in accordance with the instructions of Controller is lawful.

5. **Confidentiality**. Processor shall ensure that its personnel engaged in the processing of PII are bound by a confidentiality undertaking.

6. **Data Breach**. Processor will promptly notify Controller after becoming aware of any actual breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, PII ("**Data Breach**").

5. Informations sur les personnes concernées. Le Responsable de traitement déclare et garantit que, lorsqu'il fournit des Données Personnelles au Sous-traitant pour traitement ou lorsqu'il communique avec les personnes concernées en utilisant les Données Personnelles fournies par le Sous-traitant :

(a) il a dûment informé les personnes concernées de leurs droits et obligations, a obtenu leur consentement si nécessaire, et les a notamment informées de la possibilité pour le Sous-traitant de traiter leurs Données Personnelles pour son compte et conformément à ses instructions ;

(b) il s'est conformé à toute la législation applicable en matière de protection des données lors de la collecte et de la fourniture au Sous-traitant de ces Données Personnelles. Plus précisément, le Responsable de traitement s'assure que toute divulgation de Données Personnelles au Sous-traitant concerne des données collectées légalement, c'est-à-dire traitées sur une base légale telle que décrite dans les articles 6 à 10 du RGPD ;

(c) le traitement des Données Personnelles est conforme à ses instructions et est légal.

6. Confidentialité. Le Sous-traitant doit s'assurer que son personnel autorisé à traiter des Données Personnelles est lié par un engagement de confidentialité.

7. Violation des données. Le Sous-traitant informera rapidement le Responsable de traitement dès qu'il a connaissance de toute violation réelle de la sécurité de données entraînant la destruction, la perte, l'altération, la divulgation non autorisée des Données Personnelles ou l'accès à celles-ci de manière accidentelle ou illégale (ci-après "**Violation des Données**").

7. **Records**. Processor will maintain up-to-date written records of its processing activities, including, *inter alia*, Processor's and Controller's contact details, details of data protection officers (where applicable), the categories of processing, transfers of PII across borders and the technical and organizational security measures implemented by the Processor. Upon request, Processor will provide an up-to-date copy of these records to Controller.

8. Registres. Le Sous-traitant tiendra des registres écrits à jour de ses activités de traitement comprenant, entre autres, les coordonnées du Sous-traitant et du Responsable de traitement, les coordonnées des délégués à la protection des données personnelles (le cas échéant), les catégories de traitement, les transferts transfrontaliers de Données Personnelles et les mesures de sécurité techniques et organisationnelles mises en œuvre par le Sous-traitant. Sur demande, le Sous-traitant fournira une copie à jour de ses dossiers au Responsable de traitement.

8. **Sub-Processors**. Controller acknowledges and agrees that Processor may engage any of the third-party sub-processors listed in Annex 3. Such sub-processors shall be bound by data protection obligations no less protective than those in this Agreement to the extent applicable to the nature of the Services provided by such sub-processor. Processor shall not subcontract any processing of the PII to any other third party subprocessor without the prior written consent of the Controller. Notwithstanding this, the Controller consents to the Processor engaging third party subprocessors to process the PII provided that: (i) The Processor provides at least 14 calendar days' prior notice of the addition or removal of any subprocessor (including details of the processing it performs or will perform), which may be given by Processor emailing the Controller or by the Processor posting details of such addition or removal on a webpage that has been set up for this purpose and which Processor has provided the Controller with emailed notice about; (ii) Processor agrees data protection terms with any subprocessor that are no less protective than those in this Agreement to the extent applicable to the nature of the Services provided by such subprocessor; and (iii) Processor remains fully liable for any breach of this Agreement that is caused by an act, error or omission of its subprocessor. If the Controller refuses to consent to the Processor's appointment of a third party subprocessor on reasonable written grounds relating to the protection of the PII and the parties cannot resolve any concerns through good faith discussion, then either the Processor will not appoint the subprocessor or the Controller may elect to suspend or terminate this Agreement and the Main Agreement in accordance with relevant provisions in the Main Agreement.

9. Sous-traitants. Le Responsable de traitement reconnaît et convient que le Sous-traitant peut engager l'un de ses propres sous-traitants secondaires énumérés à **l'Annexe 3**, liste que le Sous-traitant peut mettre à jour ponctuellement. Ces sous-traitants secondaires sont liés par des obligations de protection des données non moindre que celles prévues au sein du présent DPA dans la mesure applicable à la nature des Services fournis par ledit Sous-traitant secondaire. Le Sous-traitant ne doit pas sous-traiter le traitement des Données Personnelles à un autre sous-traitant tiers sans le consentement écrit préalable du Responsable du traitement. Nonobstant ceci, le Responsable du traitement consent à ce que le Sous-traitant engage des sous-traitants tiers pour traiter les Données Personnelles à condition que : (i) Le Sous-traitant donne un préavis d'au moins 14 jours calendaires de l'ajout ou de la suppression de tout sous-traitant tiers (y compris les détails du traitement qu'il effectue ou effectuera), qui peut être donné par le Sous-traitant en envoyant un courriel au Responsable du traitement ou par le Sous-traitant en publiant les détails de cet ajout ou de cette suppression sur une page Web qui a été créée à cette fin et dont le Sous-traitant a informé le Responsable du traitement par courriel ; (ii) le Responsable du traitement convient avec tout sous-traitant tiers de conditions de protection des données qui ne sont pas moins protectrices que celles du présent Contrat dans la mesure où elles s'appliquent à la nature des Services fournis par ledit sous-traitant tiers ; et (iii) le Responsable du traitement demeure entièrement responsable de toute violation du présent Contrat qui est causée par un acte, une erreur ou une omission de son sous-traitant tiers. Si le Responsable du traitement refuse de consentir à la nomination par le Sous-traitant, d'un sous-traitant tiers, pour des motifs écrits raisonnables liés à la protection des Données Personnelles et que les parties ne peuvent pas résoudre les problèmes par une discussion de bonne foi, soit le Sous-traitant ne nommera pas le sous-traitant tiers, soit le Responsable du traitement pourra choisir de suspendre ou de résilier le présent Contrat et le Contrat principal conformément aux dispositions pertinentes du Contrat principal.

9. **Assistance**. Processor will assist Controller in ensuring compliance with Controller's obligations related to the security of the processing, notification and communication of Data Breaches, conduct of data protection impact assessments and any inquiry, investigation or other request by a supervisory authority. In the event that the Controller requests the Processor's assistance in relation to the PII processing for the Controller, such assistance services will be provided, subject to feasibility and acceptance by the Processor, at the rates of the Processor in force at that time.

10. **Possible Violation**. Where Processor believes that an instruction would result in a violation of any applicable data protection laws, Processor shall notify the Controller thereof.

11. **Information**. Processor will make available to Controller, upon request, information necessary to demonstrate compliance with the obligations set forth in this Agreement.

12. **Audits**. Upon Controller's request, Processor shall cooperate with audits and inspections of its compliance with the requirements and obligations herein and/or under applicable law. Such audits and inspections may be conducted by Controller or by any third party designated by Controller and may not exceed 2 audits per year. In consultation with Processor, Controller may engage a third party to perform its audit rights, provided that such third party is bound by an agreement of confidentiality with Processor. Processor shall be entitled to invoice the Controller on a time and material basis at the then-current applicable prices for any time expended for any such audit.

10. Assistance. Le Sous-traitant aidera le Responsable de traitement à assurer le respect de ses obligations liées à la sécurité du traitement, à la notification et à la communication des Violations de données, à la réalisation d'études d'impact sur la protection des données et à toute enquête, investigation ou autre demande émanant d'une autorité de contrôle. Dans le cas où le Responsable de traitement demande l'assistance du Sous-traitant en ce qui concerne le traitement des Données Personnelles pour le Responsable de traitement, les services d'assistance du Sous-traitant seront fournis, sous réserve de faisabilité et d'acceptation par celui-ci, aux tarifs du Sous-traitant en vigueur pour la période en cours.

11. Violation éventuelle. Lorsque le Sous-traitant estime qu'une instruction entraînerait une violation de toute loi applicable en matière de protection des données, le Sous-traitant en informe le Responsable de traitement.

12. Informations. Le Sous-traitant mettra à la disposition du Responsable de traitement, sur sa demande, les informations nécessaires pour démontrer le respect des obligations énoncées dans le présent DPA.

13. Audits. À la demande du Responsable de traitement, le Sous-traitant coopère aux audits et inspections visant à vérifier qu'il respecte les exigences et obligations énoncées dans le présent DPA et/ou en vertu du droit applicable. Ces audits et inspections peuvent être effectués par le Responsable de traitement et ne peuvent pas dépasser deux audits par an. En concertation avec le Sous-traitant, le Responsable de traitement peut engager un tiers pour exercer ses droits d'audit, à condition que ce tiers soit lié par un accord de confidentialité avec le Sous-traitant. Le Sous-traitant est en droit de facturer le Responsable de traitement en temps et en matériel aux prix applicables alors en vigueur pour tout temps consacré à un tel audit.

13. **Technical and Organizational Measures**.

14.1 Processor shall implement and maintain all technical and organizational measures that are required for protection of the PII and ensure a level of security that is appropriate to for dealing with and protecting against any risks to the rights and freedoms of the data subjects, and as required in order to avoid accidental or unlawful destruction, loss, alteration or unauthorized disclosure of, or access to PII and/or as otherwise required pursuant to the GDPR, including, *inter alia*, the measures set forth in **Annex 2**. When complying with Section 14 hereof, Processor shall take into consideration the state of technological development existing at the time and the nature, scope, context and purposes of processing as well as the aforementioned risks.

14.2. Processor shall regularly monitor its compliance with this Agreement and will provide Controller, upon request, with evidence that will enable verification of such monitoring activities. Processor shall ensure that all persons acting under its authority or on its behalf and having access to the PII, do not process the PII except as instructed by Controller and permitted herein.

14. **Transfer of PII to Third Countries**. Processor or any subprocessor will not transfer PII to a recipient located in a country that is not a Member State of the European Union or European Economic Area, unless that country is considered by the European Commission to have an adequate level of protection or pursuant to appropriate safeguards as set out by the GDPR, including the Standard Contractual Clauses of the European Commission.

15. **Return and Deletion of PII**. On the Controller's request, Processor shall return or destroy PII to the extent allowed by applicable law.

14. Mesures techniques et organisationnelles.

14.1 Le Sous-Traitant mettra en œuvre et maintiendra toutes les mesures techniques et organisationnelles requises pour la protection des Données Personnelles et assurera un niveau de sécurité approprié pour traiter et protéger celles-ci contre tout risque pour les droits et libertés des personnes concernées, et tel que requis afin d'éviter la destruction, la perte, l'altération ou la divulgation non autorisée des Données Personnelles, ou l'accès à celles-ci, de manière accidentelle ou illégale et/ou tel que requis par ailleurs par le RGPD, y compris les mesures énoncées à **l'Annexe 2**. Lorsqu'il se conforme à la Section 14 du présent Contrat, le Sous-traitant prend en considération l'état de la technique existant à cet instant et la nature, la portée, le contexte et les finalités du traitement ainsi que les risques susmentionnés.

14.2. Le Sous-traitant veille régulièrement au respect du présent DPA et fournit au Responsable de traitement, sur demande, les preuves qui permettront de vérifier cette vigilance. Le Sous-traitant veille à ce que toutes les personnes agissant sous son autorité ou pour son compte, et ayant accès aux Données Personnelles, traitent ces dernières uniquement sur instructions du Responsable de traitement et conformément au présent DPA.

15. Transfert des Données Personnelles vers des pays tiers. Le Sous-traitant ou tout sous-traitant tiers ne transférera pas les Données Personnelles à un destinataire situé dans un pays qui n'est pas un État membre de l'Union européenne ou de l'Espace économique européen, à moins que ce pays ne soit considéré par la Commission européenne comme ayant un niveau de protection adéquat ou conformément aux garanties appropriées prévues par le RGPD, y compris les Clauses contractuelles types de la Commission européenne.

16. Retour et suppression des Données Personnelles. À la demande du Responsable de traitement, le Sous-traitant restitue ou détruit les Données Personnelles dans la mesure autorisée par la loi applicable.

16. **Sensitive Data.** Controller is likely to process sensitive data as defined in article 9 of the GDPR. In this context, Controller and Processor undertake to comply with the measures specific to this category of data.

17. **Data Hosting Addendum.** In accordance with Article R.1111-11 of the French Public Health Code ("**FPHC**"), Controller and Processor enter into the Data Hosting Addendum found in Annex IV to this Agreement. Processor shall enter into a Data Hosting Addenum with it subprocessor, Itamar Medical Limited, which contains materially the same rights and obligations as those found in Annex IV to this Agreement. Processor shall also be responsible for ensuring that Itamar Medical Limited in turn has entered into a data hosting agreement with the actual data hosting providers, Amazon Web Services, Inc. and Amazon Web Services EMEA SARL, which contains materially the same rights and obligations as those found in Annex IV to this Agreement.

18. **Controller informing affected data subjects about the Data Hosting Addendum.** Controller must inform affected data subjects of the existence of of the Data Hosting Addendum which governs the hosting of their health data and the fact that Processor is contractually obligated to ensure that other addendums exist between all relevant parties which contain materially the same rights and obligations, including with the final data hosting providers.

19. **Controller's responsibility for data hosting certification.** Controller is themselves obligated to ensure that the data hosting providers (Amazon Web Services, Inc. and Amazon Web Services EMEA SARL) hold the correct certification for the activities included in the Data hosting Addendum.

17. Données sensibles. Le Responsable de traitement est susceptible de traiter des données sensibles telles que définies à l'article 9 du RGPD. Dans ce cadre, le Responsable de traitement et le Sous-traitant s'engagent à respecter les mesures spécifiques à cette catégorie de données.

18. Avenant relatif à l'hébergement des données. Conformément à l'article R.1111-11 du Code de la santé publique français ("**CSP**"), le Responsable du traitement et le Sous-traitant concluent l'Avenant relatif à l'hébergement des données figurant à l'Annexe IV du présent Accord. Le Responsable du traitement conclut avec son sous-traitant, Itamar Medical Limited, un avenant relatif à l'hébergement des données qui contient matériellement les mêmes droits et obligations que ceux figurant à l'Annexe IV du présent accord. Le Sous-traitant doit également s'assurer qu'Itamar Medical Limited a conclu à son tour un contrat d'hébergement de données avec les fournisseurs d'hébergement de données réels, Amazon Web Services, Inc. et Amazon Web Services EMEA SARL, qui contient matériellement les mêmes droits et obligations que ceux figurant à l'Annexe IV du présent Contrat.

19. Le responsable du traitement informe les personnes concernées de l'Avenant sur l'hébergement des données. Le Responsable du traitement doit informer les personnes concernées de l'existence de l'Avenant relatif à l'hébergement des données qui régit l'hébergement de leurs données de santé et du fait que le Responsable du traitement est contractuellement obligé de s'assurer que d'autres avenants existent entre toutes les parties concernées qui contiennent matériellement les mêmes droits et obligations, y compris avec les fournisseurs finaux d'hébergement de données.

20. Responsabilité du Responsable du traitement en matière de certification de l'hébergement des données. Le Responsable du traitement est lui-même tenu de s'assurer que les fournisseurs d'hébergement de données (Amazon Web Services, Inc. et Amazon Web Services EMEA SARL) détiennent la certification correcte pour les activités incluses dans l'Avenant sur l'hébergement de données.

20. **Contact of the DPO**

ItamarDPO@zoll.com

I.M.E 2016 B.V.

By/Par : _____

Title/Titre : _____

Date : _____

21. Contact du DPO

ItamarDPO@zoll.com

CONTROLLER: _____

By/Par : _____

Title/Tie:: _____

Date: _____

Annex I
Data Processing Description

This Annex I forms part of the Agreement and describes the processing that the Processor will perform on behalf of the Controller.

It should be noted that two separate types of products and services are described in this Annex. Namely: (1) On premises solutions (including "zzzPAT™ Software", "WatchPAT300" (this is both an on premises and cloud based solution) and "EndoPAT"); and (2) cloud based solutions (including "CloudPAT™ Software", "WatchPAT300" (this is both an on premises and cloud based solution), "WatchPAT ONE" and "SleePATh"). The details that apply will therefore depend on what type of product or service the Controller is using.

The practical data protection difference between the two types of products and services is that the on premises solutions involve the Controller undertaking all storage of PII itself, except for that required for technical support purposes, while the cloud based solutions involve the Processor (via its subprocessors, Amazon Web Services Inc. and Amazon Web Services EMEA SARL) undertaking all the storage of PII.

The processing details for these two types of products and services are otherwise the same except as specifically clarified in the table below.

Categories of data subjects whose personal data is transferred:	Patients, Health care professionals
Categories of personal data transferred:	Header Section: ● Patient ID ● Prefix ● First name ● Last name ● Office ● Gender ● Date of birth ● Referring Physician ● Mobile Phone

Annexe I
Description du traitement des données

La présente annexe I fait partie du Contrat et décrit le traitement que le Sous-traitant effectuera pour le compte du Responsable du traitement.

Il convient de noter que deux types distincts de produits et de services sont décrits dans la présente Annexe. À savoir : (1) solution sur site (y compris le logiciel zzzPAT™) ; et (2) solution basée sur le cloud (y compris le logiciel CloudPAT™). Les détails qui s'appliquent dépendront donc du type de produit ou de service que le Responsable de traitement utilise.
La différence pratique en matière de protection des données entre les deux types de produits et services est que la solutions sur site implique que le Responsable de traitement entreprend lui-même tout le stockage des données personnelles, à l'exception de ce qui est nécessaire à des fins d'assistance technique, tandis que la solutions basée sur le cloud implique que le Sous-traitant (via ses sous-traitants ultérieurs, Amazon Web Services Inc. et Amazon Web Services EMEA SARL) entreprend tout le stockage des données personnelles.

Les détails du traitement pour ces deux types de produits et services sont par ailleurs les mêmes, à l'exception de ce qui est spécifiquement précisé dans le tableau ci-dessous.

Catégories de personnes concernées dont les données personnelles sont transférées :	Patients, Professionnels de santé
Catégories de données personnelles transférées :	Section en entête : ● Identité du patient ● Préfixe ● Prénom ● Nom de famille ● Fonction ● Sexe ● Date de naissance

	• Email Personal Details: • Height • Weight • BMI • Neck circumference • EPWORTH SCORE • STOP-Bang score • PACEMAKER Logistic Comments • Edit field Contact Information • Street • City • ZIP Code • State • Country • Home phone • Work phone • Opt-out from communication Study Details • Bracelet Study • Request Script • Number of Nights dropdown. • Status Insurance Information • INSURANCE PROVIDER • GROUP NUMBER • OTHER Additional Information • Specialty

	• Médecin référant • Numéro de téléphone mobile • Adresse email Détails personnels : • Taille • Poids • BMI • Circonférence du cou • SCORE de EPWORTH • Score STOP-Bang • PACEMAKER Commentaires logistiques: • Champ d'édition Informations sur le contact : • Rue • Ville • Code postal • Département • Pays • Téléphone domicile • Téléphone professionnel • Désactiver la communication Détails de l'étude: • Étude sur les bracelets • Demander un script • Liste déroulante du nombre de nuits • Statut Information sur l'assurance :

	• Status • Custom Field1 to Custom Field5 (if configured for the office) <u>Compliance Data optional tab:</u> The Daily Compliance Graph shall show both the usage (h) and AHI (#) graphs. The compliance fields shall include the following: • Is Active: Y / N • Tx Manufacturer: • Days since Tx started: • Last update from CPAP: • WatchPAT AHI: • Treatment Date: The compliance table shall display columns for the last 30 days, 90 days, and 180 days and rows of % of days with CPAP, % of days with CPAP > 4h, Average number of hours, PAP Reported AHI. The compliance table shall show a red indicator if there were less than four hours per night of average use and a green indicator if more. The CPAP Reported AHI row shall include the following indications: an arrow when the value is higher than 10: • Less than 10: Green indication • More than 10 yet the reduction compared to the WP AHI > 50%: Yellow indication • More than 10 however the reduction compared to the WP AHI < 50%: Orange indication		• Fournisseur de l'assurance • Numéro de groupe • Autre Informations complémentaires : • Spécialité • Statut • Champ personnalisé 1 à Champ personnalisé 5 (si configuré pour le bureau) Onglet facultatif Données de conformité : le graphique de conformité quotidien doit montrer à la fois les graphiques d'utilisation (h) et d'AHI (#) Les champs de conformité doivent comprendre les éléments suivants : • Est actif : O / N • Fabricant Tx • Jours depuis le début Tx • Dernière mise à jour CPAP • WatchPAT AHI • Date du traitement Le tableau de conformité doit afficher des colonnes pour les 30 derniers jours, les 90 derniers jours et les 180 derniers jours et des lignes pour le % de jours avec CPAP, le % de jours avec CPAP > 4h, le nombre moyen d'heures, le PAP Report-ed AHI. Le tableau de conformité indique un indicateur rouge si l'utilisation moyenne est

	Study Details This tab shall contain the interpreter report if one was created. CP shall display the minimum desaturation that was used for AHI and RDI calculations, which can be 3% or 4%. CP shall allow downloading the raw data files of the study. CP shall allow downloading the PDF file and the secondary report if configured to this office (HTML or RTF) CP shall show links to files attached by the interpreting physician. Study Details screen shall include a dropdown called Min Desat for ODI with values of 3% or 4% but If the selected AHI is 4% the ODI must be 4% as well. The questionnaire answers PDF file shall be appended to the report once the questionnaires are completed or questionnaires timeout has been reached with no need to wait for the save and lock operation. The report shall include a subset of the following elements, please see full details in Appendix A: Header, Self-Reported Patient Details, Bedtime Questionnaire, Morning Questionnaire, Main Sleep Complaints, Prior Sleep Diagnosis,		inférieure à quatre heures par nuit et un indicateur vert si elle est supérieure. La ligne "AHI rapporté par CPAP" doit comporter les indications suivantes : une flèche lorsque la valeur est supérieure à 10: ● Moins de 10 : indication verte ● Plus de 10 mais la réduction par rapport à l'AHI du WP > 50% : indication jaune ● Plus de 10 mais la réduction par rapport à l'AHI du WP < 50% : indication orange Détails de l'étude Cet onglet doit contenir le rapport de l'interprète s'il a été créé. CP doit afficher la désaturation minimale utilisée pour les calculs de AHI et de RDI, qui peut être de 3 % ou 4 %. CP doit permettre de télécharger les fichiers de données brutes de l'étude. CP doit permettre de télécharger le fichier PDF et le rapport secondaire s'il est configuré pour ce bureau (HTML ou RTF). CP doit afficher les liens vers les fichiers joints par le médecin interprète. L'écran détails de l'étude doit inclure une liste déroulante intitulée Desat min pour ODI avec des valeurs de 3 % ou 4 %, mais si

	Breathing table, CVD Markers, Insomnia, Daytime Sleepiness, Insomnia Severity Index (ISI), Epworth sleepiness scale (ESS), Narcolepsy, Movement, RLS, Sleep Schedule, Circadian, Lifestyle, Diseases, Medications, Appendix including ISI ESS and STOP BANG. <u>Sleep Report (Done through the WP Device Interface)</u> CP shall produce a generic sleep report as a PDF file and a secondary report if configured to this office (HTML or RTF). The report shall include the output of the WP Interface process. Report generated during analysis shall include data from study analysis and the most recent patient data available at the time of analysis.		AHI sélectionné est de 4 %, ODI doit également être de 4 %. Le fichier PDF des réponses au questionnaire doit être joint au rapport une fois que les questionnaires sont remplis ou que le délai d'attente des questionnaires est atteint, sans qu'il soit nécessaire d'attendre l'opération de sauvegarde et de verrouillage. Le rapport comprendra un sous-ensemble des éléments suivants, voir les détails complets à l'annexe A : En-tête, données auto déclarées par le patient, questionnaire du coucher, questionnaire du matin, principales plaintes relatives au sommeil, diagnostic antérieur du sommeil, table de respiration, marqueurs CVD, insomnie, somnolence diurne, indice de gravité de l'insomnie (ISI), échelle de somnolence d'Epworth (ESS), narcolepsie, mouvement, RLS, horaire de sommeil, rythme circadien, mode de vie, maladies, médicaments, annexe comprenant ISI ESS et STOP BANG. Rapport de sommeil (réalisé par l'interface du dispositif WP) CP doit produire un rapport de sommeil générique sous forme de fichier PDF et un rapport secondaire s'il est configuré pour ce bureau (HTML ou RTF). Le rapport doit inclure la sortie du processus de l'interface WP.
Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for	**Sensitive data types** All categories of data listed above would likely be considered health data apart from: ● First name ● Last name ● Gender ● Date of birth ● Mobile Phone ● Email **Applied restrictions / safeguards**		

onward transfers or additional security measures:	The applied restrictions / safeguards that apply to this sensitive data are the same as apply to the data generally and which can be found in Annex II below.
The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):	**On premises solutions:** As and when needed for technical support reasons.
	Cloud based solutions: Continuous.
Nature of the processing:	**On premises solutions:** Access, use for technical support reasons, minimal storage as necessary for technical support reasons and any use as may be required by law.
	Cloud based solutions: Storage, providing access, use for technical support reasons and any use as may be required by law.
Purpose(s) of the data transfer and further processing:	**On premises solutions:** Incidental use for technical support reasons. Any use as may be required by law.
	Cloud based solutions: Storage and providing so as to provide the services. Use for technical support reasons. Any use as may be required by law.
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:	**On premises solutions:** As long as needed for technical support reasons or as may be required by applicable law.
	Cloud based solutions: On the Controller's request, and at the ending of the Main Agreement at the latest, Processor shall return or destroy PII to the extent allowed by applicable law.
For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:	As per above.

	Le rapport généré pendant l'analyse doit inclure les données de l'analyse de l'étude et les données les plus récentes du patient, disponibles au moment de l'analyse.
Données sensibles transférées (le cas échéant) et restrictions ou garanties appliquées qui tiennent pleinement compte de la nature des données et des risques encourus, comme par exemple une stricte limitation de la finalité, des restrictions d'accès (y compris l'accès réservé au personnel ayant suivi une formation spécialisée), la tenue d'un registre des accès aux données, des restrictions pour les transferts ultérieurs ou des mesures de sécurité supplémentaires :	**Types de données sensibles** Toutes les catégories de données énumérées ci-dessus sont susceptibles d'être considérées comme des données relatives à la santé, à l'exception des suivantes : ● Prénom ● Nom de famille ● Sexe ● Date de naissance ● Téléphone portable ● Courriel **Restrictions/garanties appliquées** Les restrictions/garanties appliquées à ces données sensibles sont les mêmes que celles qui s'appliquent aux données en général et qui figurent à l'Annexe II ci-dessous.
La fréquence du transfert (par exemple, si les données sont transférées de façon ponctuelle ou continue) :	**Solutions sur site :** Aussi fréquemment que nécessaire pour des raisons de support technique.
	Solutions basée sur le cloud : En continu.

Nature du traitement :	**Solution sur site :** Accès, utilisation pour des raisons d'assistance technique, stockage minimal si nécessaire pour des raisons d'assistance technique et toute utilisation pouvant être requise par la loi.
	Solutions basée sur le cloud : Stockage, accès, utilisation pour des raisons de support technique et toute utilisation requise par la loi.
Finalité(s) du transfert et du traitement ultérieur des données :	**Solutions sur site :** Utilisation occasionnelle pour des raisons de support technique. Toute utilisation requise par la loi.
	Solutions basée sur le cloud : Stockage et fourniture afin de fournir les services. Utilisation pour des raisons de support technique. Toute utilisation pouvant être requise par la loi.
La période pendant laquelle les données personnelles seront conservées ou, si cela n'est pas possible, les critères utilisés pour déterminer cette période :	**Solutions sur site :** Aussi longtemps que nécessaire pour des raisons de support technique ou que la loi applicable peut l'exiger.
	Solutions basée sur le cloud : À la demande du responsable du traitement, et au plus tard à la fin du contrat principal, le sous-traitant restitue ou détruit les données personnelles dans la mesure où la loi applicable le permet.
Pour les transferts à des (tiers) sous-traitants, préciser également l'objet, la nature et la durée du traitement :	Comme indiqué ci-dessus.

Annex II
Technical and Organisational Security Measures

Description of the technical and organisational measures implemented by the processor(s) / data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

The column entitled "Itamar" in the table directly below reflects the security measures of the Processor and its affiliate subprocessor, Itamar Medical Limited. These entities (jointly also referred to as "Itamar" below) only process the PII for the purposes of providing technical support and as may be required by law.

The column entitled "AWS" directly below contains both the "custom" data security measures that the Processor's subprocessor,

Annexe II

Mesures de sécurité techniques et organisationnelles

Description des mesures techniques et organisationnelles mises en œuvre par le(s) sous-traitant(s) / importateur(s) de données (y compris toute certification pertinente) pour garantir un niveau de sécurité approprié, compte tenu de la nature, de la portée, du contexte et de la finalité du traitement, ainsi que des risques pour les droits et libertés des personnes physiques.

La colonne intitulée " Itamar " dans le tableau directement ci-dessous reflète les mesures de sécurité du Responsable du traitement et de son sous-traitant secondaire affilié, Itamar Medical Limited. Ces entités (désignées conjointement sous le nom de " Itamar " ci-dessous) traitent les données à caractère personnel uniquement dans le but de fournir une assistance technique et dans la mesure où la loi l'exige.

Itamar Medical Limited, has elected to use from its further subprocessors, Amazon Web Services Inc. and Amazon Web Services EMEA SARL (together "AWS"), along with "standard" AWS data security measures from the data processing agreement that Processor's subprocessor, Itamar Medical Limited, has with AWS and which can be found here - https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf.
AWS processes the PII for the purposes of storage, providing access, providing technical support and as may be required by law.

Measures of pseudonymisation and encryption of personal data	Controller can easily delete all PII from files that are sent to Processor for technical support reasons. SSL (secure ciphers over TLS 1.2) is used as encryption method for any data transfers.	**Custom measures:** Controller can easily delete all PII from files that are sent to Processor and its subprocessors. SSL (secure ciphers over TLS 1.2) is used as encryption method for any data transfers.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	**Confidentiality** Itamar will only access PII if the Controller has specifically requested and approved that Itamar	**Confidentiality** **Custom measures:** All servers hosted with AWS have custom Firewall rules and additional security

La colonne intitulée " AWS " directement ci-dessous contient à la fois les mesures de sécurité des données " personnalisées " que le sous-traitant ultérieur du Sous-traitant, Itamar Medical Limited, a choisi d'utiliser auprès de ses autres sous-traitants ultérieurs, Amazon Web Services Inc. et Amazon Web Services EMEA SARL (ensemble " AWS "), ainsi que les mesures de sécurité des données AWS " standard " de l'accord de traitement des données que le sous-traitant ultérieur du Sous-traitant, Itamar Medical Limited, a conclu avec AWS et qui peut être trouvé ici - https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf.
AWS traite les données personnelles à des fins de stockage, de fourniture d'accès, d'assistance technique et dans la mesure où la loi l'exige.

Mesures de pseudonymisation et de cryptage des données personnelles	Le Responsable de traitement peut facilement supprimer toutes les données personnelles des fichiers envoyés au Sous-traitant pour des raisons d'assistance technique. SSL (secure ciphers over TLS 1.2) est utilisé comme méthode de cryptage pour tous les transferts de données.	**Mesures personnalisées** : Le Responsable du traitement peut facilement supprimer toutes les données personnelles des fichiers envoyés au Sous-traitant et à ses sous-traitants ultérieurs. SSL (secure ciphers over TLS 1.2) est utilisé comme méthode de cryptage pour tous les transferts de données.
Mesures visant à garantir en permanence la	**Confidentialité**	**Confidentialité**

	undertake a technical support activity which involves the viewing of PII (e.g. through screen sharing functionality). Itamar does not store PII on its own systems except as may be required by applicable law. Only a minimal amount of Itamar staff, who are subject to contractual obligations of confidentiality and whose access is password protected, will be provided with access to the Controller's PII. **Integrity** Itamar will only change PII if instructed to by Controller. **Availability** Availability is not applicable to the processing undertaken directly by Itamar as it does not actively involve data storage except as may be required by applicable law. **Resiliance**	measures employed by Itamar Digital Health Team in place. **Standard measures:** Network Security. The AWS Network will be electronically accessible to employees, contractors and any other person as necessary to provide the Services. AWS will maintain access controls and policies to manage what access is allowed to the AWS Network from each network connection and user, including the use of firewalls or functionally equivalent technology and authentication controls. AWS will maintain corrective action and incident response plans to respond to potential security threats. **Integrity** **Custom measures:** All servers hosted with AWS have custom Firewall rules and additional security measures employed by Itamar Digital Health Team in place. **Standard measures:** Network Security. The	confidentialité, l'intégrité, la disponibilité et la résilience des systèmes et services de traitement.	Itamar n'accèdera aux données personnelles que si le Responsable de traitement a spécifiquement demandé et approuvé qu'Itamar entreprenne une activité de support technique qui implique la visualisation des données personnelles (par exemple, par le biais d'une fonctionnalité de partage d'écran). Itamar ne stocke pas les données personnelles sur ses propres systèmes, sauf si la loi applicable l'exige. Seul un nombre minimal d'employés d'Itamar, qui sont soumis à des obligations contractuelles de confidentialité et dont l'accès est protégé par un mot de passe, aura accès aux données personnelles du Responsable de traitement**.** **Intégrité** Itamar ne modifiera que si le Responsable de tratitement le lui demande. **Disponibilité**	**Mesures personnalisées :** Tous les serveurs hébergés par AWS sont dotés de règles de pare-feu personnalisées et de mesures de sécurité supplémentaires utilisées par l'équipe de santé numérique d'Itamar. **Mesures standard :** Sécurité du réseau. Le réseau AWS sera électroniquement accessible aux employés, aux contractants et à toute autre personne nécessaire à la fourniture des services. AWS maintiendra des contrôles et des politiques d'accès pour gérer l'accès autorisé au Réseau AWS à partir de chaque connexion réseau et de chaque utilisateur, y compris l'utilisation de pare-feu ou de technologies fonctionnellement équivalentes et de contrôles d'authentification. AWS maintiendra des plans d'action correctifs et de

	Resiliance is not applicable to the processing undertaken directly by Itamar as it does not actively involve data storage except as may be required by applicable law.	AWS Network will be electronically accessible to employees, contractors and any other person as necessary to provide the Services. AWS will maintain access controls and policies to manage what access is allowed to the AWS Network from each network connection and user, including the use of firewalls or functionally equivalent technology and authentication controls. AWS will maintain corrective action and incident response plans to respond to potential security threats. **<u>Availability</u>** **Custom measures:** A backup concept for databases, configuration, servers and files is in place. **<u>Resiliance</u>** **Custom measures:** A data security testing concept is in place that involves constant testing for any data security vulnerabilities.

	La disponibilité n'est pas applicable au traitement entrepris directement par Itamar car il n'implique pas activement le stockage de données, sauf si la loi applicable l'exige. **Résilience** La résilience n'est pas applicable au traitement effectué directement par Itamar car elle n'implique pas activement le stockage de données, sauf si cela est requis par la loi applicable.	réponse aux incidents pour répondre aux menaces potentielles pour la sécurité. **Intégrité** **Mesures personnalisées :** Tous les serveurs hébergés par AWS ont des règles de pare-feu personnalisées et des mesures de sécurité supplémentaires employées par l'équipe de santé numérique d'Itamar. **Mesures standard :** Sécurité du réseau. Le réseau AWS sera électroniquement accessible aux employés, aux contractants et à toute autre personne nécessaire à la fourniture des services. AWS maintiendra des contrôles et des politiques d'accès pour gérer l'accès autorisé au Réseau AWS à partir de chaque connexion réseau et de chaque utilisateur, y compris

		Standard measures: Continued Evaluation. AWS will conduct periodic reviews of the security of its AWS Network and adequacy of its information security program as measured against industry security standards and its policies and procedures. AWS will continually evaluate the security of its AWS Network and associated Services to determine whether additional or different security measures are required to respond to new security risks or findings generated by the periodic reviews.
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	Availability and access are not applicable as the processing undertaken directly by Itamar does not involve data storage except as may be required by applicable law.	**Custom measures:** A backup concept for databases, configuration, servers and files is in place.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to	Itamar regularly runs internal testing to ensure that its data security measures are adequate.	**Custom measures:** A data security testing concept is in place that involves constant testing for any data security vulnerabilities.

		l'utilisation de pare-feu ou de technologies fonctionnellement équivalentes et de contrôles d'authentification. AWS maintiendra des plans d'action correctifs et de réponse aux incidents pour répondre aux menaces potentielles pour la sécurité. **Disponibilité** **Mesures personnalisées :** Un concept de sauvegarde pour les bases de données, la configuration, les serveurs et les fichiers est en place. **Résilience** **Mesures personnalisées :** Un concept de test de sécurité des données est en place et implique des tests constants pour détecter toute vulnérabilité en matière de sécurité des données.

ensure the security of the processing		**Standard measures:** Continued Evaluation. AWS will conduct periodic reviews of the security of its AWS Network and adequacy of its information security program as measured against industry security standards and its policies and procedures. AWS will continually evaluate the security of its AWS Network and associated Services to determine whether additional or different security measures are required to respond to new security risks or findings generated by the periodic reviews.
Measures for user identification and authorisation	Itamar will only access PII if the Controller has specifically requested and approved that Itamar undertake a technical support activity which involves the viewing of PII (e.g. through screen sharing functionality). Only a minimal amount of Itamar staff, who are subject to contractual obligations of confidentiality and whose access is password protected, will be provided	**Custom measures:** Access Control system in place across all Itamar Cloud systems inclduing authenticated access and password protection. **Standard measures:** Network Security. The AWS Network will be electronically accessible to employees, contractors and any other person as necessary to provide the Services. AWS will maintain access controls and policies to manage what access is allowed to

		Mesures standard : Évaluation continue. AWS procédera à des réévaluations périodiques de la sécurité de son réseau AWS et de l'adéquation de son programme de sécurité des informations par rapport aux normes de sécurité du secteur et à ses politiques et procédures. AWS évaluera continuellement la sécurité de son Réseau AWS et des Services associés afin de déterminer si des mesures de sécurité supplémentaires ou différentes sont nécessaires pour répondre aux nouveaux risques de sécurité ou aux découvertes générées par les examens périodiques.
Mesures visant à garantir la capacité de rétablir la disponibilité et l'accès aux données personnelles en temps utile en cas	La disponibilité et l'accès ne sont pas applicables car le traitement effectué directement par Itamar n'implique pas de stockage	**Mesures personnalisées :** Un concept de sauvegarde pour les bases de données, la configuration, les

	with access to the Controller's PII.	the AWS Network from each network connection and user, including the use of firewalls or functionally equivalent technology and authentication controls. AWS will maintain corrective action and incident response plans to respond to potential security threats.
Measures for the protection of data during transmission	The encryption standard used for PII in transit is SSL (secure ciphers over TLS 1.2).	**Custom measures:** The encryption standard used for data in transit is SSL (secure ciphers over TLS 1.2).
Measures for the protection of data during storage	Itamar does not actively store PII on its own systems except as may be required by applicable law.	**Custom measures:** The encryption standard used for data at rest is - AES256.
Measures for ensuring physical security of locations at which personal data are processed	Itamar does not actively store PII on its own systems as part of providing the technical support services. Only a minimal amount of Itamar staff, who are subject to contractual obligations of confidentiality and whose access is password protected, will be provided with access to the Controller's PII.	**Standard measures:** Physical Access Controls. Physical components of the AWS Network are housed in nondescript facilities (the "Facilities"). Physical barrier controls are used to prevent unauthorised entrance to the Facilities both at the perimeter and at building access points. Passage through the physical barriers at the Facilities requires either electronic

d'incident physique ou technique.	de données, sauf si la loi applicable l'exige.	serveurs et les fichiers est en place.
Processus permettant de tester, d'apprécier et d'évaluer régulièrement l'efficacité des mesures techniques et organisationnelles afin de garantir la sécurité du traitement.	Itamar effectue régulièrement des tests internes pour s'assurer que ses mesures de sécurité des données sont adéquates.	**Mesures personnalisées :** Un concept de test de sécurité des données est mis en place, qui implique des tests constants pour détecter toute vulnérabilité en matière de sécurité des données. **Mesures standard :** Évaluation continue. AWS procédera à des réévaluations périodiques de la sécurité de son réseau AWS et de l'adéquation de son programme de sécurité des informations par rapport aux normes de sécurité du secteur et à ses politiques et procédures. AWS évaluera continuellement la sécurité de son Réseau AWS et des Services associés afin de déterminer si des mesures de sécurité supplémentaires ou différentes sont

		access control validation (e.g., card access systems, etc.) or validation by human security personnel (e.g., contract or in-house security guard service, receptionist, etc.). Employees and contractors are assigned photo-ID badges that must be worn while the employees and contractors are at any of the Facilities. Visitors are required to sign-in with designated personnel, must show appropriate identification, are assigned a visitor ID badge that must be worn while the visitor is at any of the Facilities, and are continually escorted by authorised employees or contractors while visiting the Facilities. Limited Employee and Contractor Access. AWS provides access to the Facilities to those employees and contractors who have a legitimate business need for such access privileges. When an employee or contractor no longer has a business need for the access privileges assigned to him/her, the access			nécessaires pour répondre aux nouveaux risques de sécurité ou aux découvertes générées par les examens périodiques.
			Mesures d'identification et d'autorisation des utilisateurs	Itamar n'accèdera aux données personnelles que si le Responsable de traitement a spécifiquement demandé et approuvé qu'Itamar entreprenne une activité de support technique qui implique la visualisation des données personnelles (par exemple, par le biais d'une fonctionnalité de partage d'écran). Seul un nombre minimal d'employés d'Itamar, qui sont soumis à des obligations contractuelles de confidentialité et dont l'accès est protégé par un mot de passe, aura accès aux données personnelles du Responsable de traitement.	**Mesures personnalisées :** Système de contrôle d'accès en place sur tous les systèmes Itamar Cloud comprenant un accès authentifié et une protection par mot de passe. **Mesures standard :** Sécurité du réseau. Le réseau AWS sera électroniquement accessible aux employés, aux entrepreneurs et à toute autre personne nécessaire à la fourniture des services. AWS maintiendra des contrôles et des politiques d'accès pour gérer l'accès autorisé au Réseau AWS à partir de chaque connexion réseau et de chaque utilisateur, y compris l'utilisation de pare-feu ou de technologies

		privileges are promptly revoked, even if the employee or contractor continues to be an employee of AWS or its Affiliates. Physical Security Protections: All access points (other than main entry doors) are maintained in a secured (locked) state. Access points to the Facilities are monitored by video surveillance cameras designed to record all individuals accessing the Facilities. AWS also maintains electronic intrusion detection systems designed to detect unauthorised access to the Facilities, including monitoring points of vulnerability (e.g., primary entry doors, emergency egress doors, roof hatches, dock bay doors, etc.) with door contacts, glass breakage devices, interior motion-detection, or other devices designed to detect individuals attempting to gain access to the Facilities. All physical access to the Facilities by employees and contractors			fonctionnellement équivalentes et de contrôles d'authentification. AWS maintiendra des plans d'action correctifs et de réponse aux incidents pour répondre aux menaces potentielles pour la sécurité.
			Mesures de protection des données pendant la transmission	La norme de cryptage utilisée pour les données en transit est la suivante: SSL (chiffrements sécurisés sur TLS 1.2)	**Mesures personnalisées** : La norme de cryptage utilisée pour les données en transit est la suivante: SSL (chiffrements sécurisés sur TLS 1.2)
			Mesures de protection des données pendant le stockage	Itamar ne stocke pas activement les données personnelles sur ses propres systèmes, sauf si la loi applicable l'exige.	**Mesures personnalisées :** La norme de cryptage utilisée pour les données pendant stockage - AES256.
			Mesures visant à assurer la sécurité physique des lieux où sont traitées les données à caractère personnel	Itamar ne stocke pas activement les données personnelles sur ses propres systèmes dans le cadre de la fourniture des services d'assistance technique. Seul un nombre minimal d'employés d'Itamar, soumis à des obligations contractuelles de confidentialité et dont	**Mesures standard** : Contrôles d'accès physiques. Les composants physiques du réseau AWS sont hébergés dans des installations indéterminées (les " installations "). Des barrières physiques sont utilisées pour empêcher toute entrée

		is logged and routinely audited.
Measures for ensuring events logging	All events are logged and there is no way for the logs to be manipulated.	**Custom measures:** All events are logged and there is no way for the logs to be manipulated.
Measures for ensuring system configuration, including default configuration	Please refer to above and below.	**Custom measures:** All AWS systems are built and maintained by Itamar Medical's Digital Health Team in order to ensure an appropriate level of data security.
Measures for internal IT and IT security governance and management	Itamar has internal IT and IT security policies and / or procedures in place to ensure effective governance in this area. This includes relevant staff training.	**Standard measures**: Information Security Program. AWS will maintain an information security program (including the adoption and enforcement of internal policies and procedures) designed to (a) help Customer secure Customer Data against accidental or unlawful loss, access or disclosure, (b) identify reasonably foreseeable and internal risks to security and unauthorised access to the AWS Network, and (c) minimise security risks, including through risk assessment and regular testing. AWS will designate one or more employees to coordinate

	l'accès est protégé par un mot de passe, aura accès aux données personnelles du Responsable du traitement.	non autorisée dans les installations, tant au périmètre qu'aux points d'accès des bâtiments. Le passage à travers les barrières physiques des installations nécessite soit la validation d'un contrôle d'accès électronique (par exemple, des systèmes d'accès par carte, etc.), soit la validation par un personnel de sécurité humain (par exemple, un service de sécurité contractuel ou interne, un réceptionniste, etc.) Les employés et les contractants reçoivent un badge d'identification avec photo qu'ils doivent porter lorsqu'ils se trouvent dans l'une des installations. Les visiteurs sont tenus de s'inscrire auprès du personnel désigné, de présenter une pièce d'identité appropriée et de recevoir un badge d'identification qui doit être porté pendant toute la durée de leur présence dans les installations.

		and be accountable for the information security program.
Measures for certification/assurance of processes and products	Itamar is in the process of becoming ISO 27001 certified.	**Standard measures:** AWS ISO-Certification and SOC Reports. In addition to the information contained in this DPA, upon Customer's request, and provided that the parties have an applicable NDA in place, AWS will make available the following documents and information: (i) the certificates issued in relation to the ISO 27001 certification, the ISO 27017 certification and the ISO 27018 certification (or the certifications or other documentation evidencing compliance with such alternative standards as are substantially equivalent to ISO 27001, ISO 27017 and ISO 27018); and (ii) the System and Organization Controls (SOC) 1 Report, the System and Organization Controls (SOC) 2 Report and the System and Organization Controls (SOC) 3 Report (or the reports or other documentation describing the controls AWS GDPR Data Processing

		Les visiteurs doivent s'inscrire auprès du personnel désigné, présenter une pièce d'identité appropriée, recevoir un badge d'identification qu'ils doivent porter lorsqu'ils se trouvent dans les installations, et être accompagnés en permanence par des employés ou des sous-traitants autorisés lorsqu'ils visitent les installations. Accès limité des employés et des sous-traitants. AWS fournit l'accès aux installations aux employés et contractants qui ont un besoin professionnel légitime pour de tels privilèges d'accès. Lorsqu'un employé ou un contractant n'a plus besoin des privilèges d'accès qui lui ont été attribués, les privilèges d'accès sont rapidement révoqués, même si l'employé ou le contractant continue d'être un employé

		Addendum 5 implemented by AWS that replace or are substantially equivalent to the SOC 1, SOC 2 and SOC 3). 10.2 AWS Audits. AWS uses external auditors to verify the adequacy of its security measures, including the security of the physical data centers from which AWS provides the Services. This audit: (a) will be performed at least annually; (b) will be performed according to ISO 27001 standards or such other alternative standards that are substantially equivalent to ISO 27001; (c) will be performed by independent third party security professionals at AWS's selection and expense; and (d) will result in the generation of an audit report ("Report"), which will be AWS's Confidential Information. 10.3 Audit Reports. At Customer's written request, and provided that the parties have an applicable NDA in place, AWS will provide Customer with a copy of the Report so that Customer can reasonably verify AWS's compliance			d'AWS ou de ses affiliés. **Protections de sécurité physique** : Tous les points d'accès (autres que les portes d'entrée principales) sont maintenus dans un état sécurisé (verrouillé). Les points d'accès aux installations sont surveillés par des caméras de vidéosurveillance conçues pour enregistrer toutes les personnes accédant aux installations. AWS maintient également des systèmes électroniques de détection d'intrusion conçus pour détecter les accès non autorisés aux installations, y compris la surveillance des points de vulnérabilité (par exemple, les portes d'entrée principales, les portes de sortie d'urgence, les trappes de toit, les portes de quai, etc.) avec des capteurs d'ouverture de porte, des dispositifs de bris

		with its obligations under this DPA.
Measures for ensuring data minimisation	Data minimisation is a Controller responsibility.	Data minimisation is a Controller responsibility.
Measures for ensuring data quality	Data quality is a Controller responsibility.	Data quality is a Controller responsibility.
Measures for ensuring limited data retention	Limited data retention is a Controller responsibility. Itamar also does not actively store PII on its own systems except as may be required by applicable law.	Limited data retention is a Controller responsibility.
Measures for ensuring accountability	Accountability is primarily a Controller responsibility. However, Itamar's accountability is also set out above.	Accountability is primarily a Controller responsibility. However, AWS's accountability is also set out above.
Measures for allowing data portability and ensuring erasure	Itamar does not actively store PII on its own systems except as may be required by applicable law.	**Standard measures**: At any time up to the Termination Date, and for 90 days following the Termination Date, subject to the terms and conditions of the Agreement, AWS will return or delete Customer Data when Customer uses the Service Controls to request such return or deletion. No later than the end of this 90-day period, Customer will close all AWS accounts containing Customer Data.

		de verre, des détecteurs de mouvement intérieurs ou d'autres dispositifs conçus pour détecter les personnes tentant d'accéder aux installations. Tous les accès physiques aux installations par les employés et les contractants sont enregistrés et régulièrement contrôlés.
Mesures pour assurer l'enregistrement des événements	Tous les événements sont enregistrés et il n'y a aucun moyen de manipuler les journaux.	**Mesures personnalisées :** Tous les événements sont enregistrés et il n'y a aucun moyen de manipuler les journaux.
Mesures pour assurer la configuration du système, y compris la configuration par défaut	Veuillez vous référer à ce qui précède et à ce qui suit.	**Mesures personnalisées** : Tous les systèmes AWS sont construits et maintenus par l'équipe de santé numérique d'Itamar Medical afin d'assurer un niveau approprié de sécurité des données.
Mesures relatives à la gouvernance et à la gestion de l'informatique interne et de la sécurité informatique	Itamar a mis en place des politiques et/ou des procédures internes en matière d'informatique et de sécurité informatique afin de garantir une gouvernance efficace dans ce domaine. Cela inclut la	**Mesures standard** : Programme de sécurité de l'information. AWS maintiendra un programme de sécurité des informations (incluant

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller (and, for transfers from a processor to a sub-processor, to the data exporter).

Please refer to above.

	formation du personnel concerné.	AWS maintiendra un programme de sécurité de l'information (y compris l'adoption et l'application de politiques et de procédures internes) conçu pour (a) aider le Client à sécuriser les Données du Client contre la perte, l'accès ou la divulgation accidentels ou illégaux, (b) identifier les risques prévisibles et internes pour la sécurité et l'accès non autorisé au Réseau AWS, et (c) minimiser les risques de sécurité, notamment par une évaluation des risques et des tests réguliers. AWS désignera un ou plusieurs employés pour coordonner le programme de sécurité de l'information et en être responsable.
Mesures de certification/assurance des processus et des produits	Itamar est en passe d'obtenir la certification ISO 27001.	**Mesures standard** : La certification ISO d'AWS et les rapports SOC. Outre les informations contenues dans le présent DPA, à la demande du Client et à condition que les

		parties aient conclu un accord de confidentialité applicable, AWS met à disposition les documents et informations suivants : (i) les certificats émis en relation avec la certification ISO 27001, la certification ISO 27017 et la certification ISO 27018 (ou les certifications ou autres documents attestant de la conformité à des normes alternatives substantiellement équivalentes à ISO 27001, ISO 27017 et ISO 27018) ; et (ii) le rapport sur les contrôles du système et de l'organisation (SOC) 1, le rapport sur les contrôles du système et de l'organisation (SOC) 2 et le rapport sur les contrôles du système et de l'organisation (SOC) 3 (ou les rapports ou autres documents décrivant les contrôles AWS GDPR Data Processing Addendum 5 mis en

		œuvre par AWS qui remplacent ou sont substantiellement équivalents aux rapports SOC 1, SOC 2 et SOC 3). 10.2 Audits d'AWS. AWS fait appel à des auditeurs externes pour vérifier l'adéquation de ses mesures de sécurité, y compris la sécurité des centres de données physiques à partir desquels AWS fournit les Services. Cet audit : (a) sera effectué au moins une fois par an ; (b) sera formé selon les normes ISO 27001 ou toute autre norme alternative qui est substantiellement équivalente à ISO 27001 ; (c) sera effectué par des professionnels de la sécurité tiers indépendants à la sélection et aux frais d'AWS ; et (d) résultera en la génération d'un rapport d'audit (" Rapport "), qui sera l'information confidentielle d'AWS. 10.3 Rapports d'audit. À la demande écrite du

		Client, et à condition que les parties aient mis en place une NDA applicable, AWS fournira au Client une copie du Rapport afin que le Client puisse raisonnablement vérifier la conformité d'AWS avec ses obligations en vertu du présent DPA.
Mesures visant à assurer la minimisation des données	La minimisation des données est une responsabilité du Responsable du traitement.	La minimisation des données est une responsabilité du Responsable du traitement.
Mesures visant à garantir la qualité des données	La qualité des données est une responsabilité du Responsable du contrôle.	La qualité des données est une responsabilité du Responsable du contrôle.
Mesures visant à garantir une conservation limitée des données	La conservation limitée des données est une responsabilité du Responsable du traitement. Itamar ne stocke pas non plus de manière active les données personnelles sur ses propres systèmes, sauf si la loi applicable l'exige.	La conservation limitée des données est une responsabilité du Responsable du traitement.
Mesures visant à garantir la responsabilité	La responsabilité est avant tout celle du Responsable de traitement. Cependant, la responsabilité d'Itamar est également exposée ci-dessus.	La responsabilité est avant tout celle du Responsable de traitement. Cependant, la responsabilité d'Itamar est également exposée ci-dessus.

Mesures visant à permettre la portabilité des données et à assurer l'effacement].	Itamar ne stocke pas activement les données personnelles sur ses propres systèmes, sauf si la loi applicable l'exige..	**Mesures standard** : À tout moment jusqu'à la Date de résiliation, et pendant 90 jours après la Date de résiliation, sous réserve des termes et conditions du Contrat, AWS renverra ou supprimera les Données du Client lorsque le Client utilisera les Contrôles du Service pour demander ce retour ou cette suppression. Au plus tard à la fin de cette période de 90 jours, le Client fermera tous les comptes AWS contenant des Données du Client.

Pour les transferts à des sous-traitants tiers, décrivez également les mesures techniques et organisationnelles spécifiques que le sous-traitant tiers doit prendre pour être en mesure de fournir une assistance au responsable du traitement (et, pour les transferts d'un sous-traitant à un sous-traitant tiers, à l'exportateur de données).

Veuillez vous référer à ce qui précède.

Annex III

Subprocessors

The controller has authorised the use of the following sub-processors:

Sub-processor name	Processing location	Processing description
Amazon Web Services EMEA SARL	Germany	Cloud computer / storage services
Itamar Medical Ltd.	Israel	Customer and technical support
Itamar Medical (UK) Limited	United Kingdom	Technical support

Annexe III

Sous-traitant tiers

Le responsable du traitement a autorisé le recours aux filliales et sous-traitants tiers suivants:

Nom du sous-traitant	Lieu du traitement	Description du traitement
Amazon Web Services EMEA SARL	Allemagne	Services de Cloud et de stockage
Itamar Medical Ltd.	Israël	Assistance à la clientèle et support technique
Itamar Medical (UK) Limited	Royaume-Uni	Support technique

Annex IV **Data Hosting Addendum**	**Annexe IV** **Avenant relatif à l'hébergement des données**
Preamble: It is agreed between the parties that the Controller shall have all the rights and obligations of the party described as the "Customer" in the Data Hosting Addendum below. It is also agreed between the parties that Processor shall have all the rights and obligations of the party described as "AWS" in the Data Hosting Addendum below. **AWS HEALTH DATA HOSTING FRANCE ADDENDUM** This Health Data Hosting Addendum ("**HDS Addendum**") is effective as of the day the last party signs this Addendum and is entered into by and among Amazon Web Services, Inc. and the AWS Contracting Party or AWS Contracting Parties (as applicable) under the Agreement (together "**AWS**") and the Customer specified in the table below. This HDS Addendum supplements the AWS GDPR Data Processing Addendum available at https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf or other agreement between Customer and AWS governing the processing of Customer Data pursuant to the GDPR (the "**AWS GDPR DPA**"). This HDS Addendum applies when the Applicable Regulation applies to Customer's use of the Services to process Health Data. Unless otherwise defined in this HDS Addendum or	**Il est PREALABLEMENT exposé ce qui suit : Il est convenu entre les parties que le Responsable du Traitement disposera de l'ensemble des droits et obligations de la partie désignée comme le « Client » dans l'Avenant sur l'hébergement des données ci-après. Il est également convenu entre les parties que le Sous-traitant disposera de l'ensemble des droits et obligations de la partie désignée comme « AWS » dans l'Avenant sur l'hébergement des données ci-après.** **AVENANT SUR L'HÉBERGEMENT DES DONNÉES DE SANTÉ AWS FRANCE** Le présent Avenant sur l'hébergement des données de santé (l'« **Avenant HDS** ») prendra effet lorsque la dernière partie le signera, et est conclu entre Amazon Web Services, Inc. et la Partie contractante AWS ou les Parties contractantes d'AWS (selon le cas) au titre du Contrat (ensemble, « **AWS** ») et le Client indiqué dans le tableau ci-après. Le présent Avenant HDS complète l'Avenant relatif au Traitement des Données RGPD d'AWS disponible à l'adresse https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf ou tout autre accord entre le Client et AWS régissant le traitement des Données du Client conformément au RGPD (l' « **Avenant**

the Agreement, capitalised terms used in this HDS Addendum will have the meanings given to them in the AWS GDPR DPA. **1. AWS HDS Certification.** 1.1 To date, the AWS Management System is certified under version 1.1 of "Hébergeur de Données de Santé" (the "**HDS Certification**") by Bureau Veritas Certification under the number FR071635 dated January 14, 2022, on sub-domains 1, 2, 3, 4, 5 and 6. 1.2 The HDS Certification is available on AWS Artifact. **2. Description of the Services.** 2.1 The Services which are made available by AWS or its Affiliates are described on the AWS Site. The Services are described on the AWS Site at https://aws.amazon.com/products (and any successor or related locations designated by AWS), as may be updated by AWS from time to time. Services do not include Third Party Content. 2.2 The service level agreements that AWS offers with respect to the Services are located at https://aws.amazon.com/legal/service-level-agreements/ (and any successor or related locations designated by AWS), as may be updated by AWS from time to time. 2.3 AWS makes available Service Controls that Customer may elect to use in relation to the availability, integrity, confidentiality and auditability of the Health Data. The Service Controls are described in the AWS GDPR DPA and in the Documentation.	**RGPD d'AWS** »). Le présent Avenant HDS s'applique lorsque la Réglementation Applicable s'applique à l'utilisation par le Client des Services pour traiter les Données de Santé. Sauf définition contraire du présent Avenant HDS ou du Contrat, les termes commençant par une majuscule utilisés dans le présent Avenant HDS auront la signification qui leur est attribuée dans l'Avenant RGPD d'AWS. **1. Certification HDS d'AWS.** 1.1 À ce jour, le Système de Gestion AWS est certifié selon la version 1.1 de l' « Hébergeur de Données de Santé » (la « **Certification HDS** ») par le Bureau Veritas Certification sous le numéro FR071635 en date du 14 janvier 2022, dans les sous-domaines 1, 2, 3, 4, 5 et 6. 1.2 La Certification HDS est disponible sur le lien d'AWS Artifact. **2. Description des Services.** 2.1 Les Services mis à disposition par AWS ou ses Sociétés Affiliées sont décrits sur le Site AWS. Les Services sont décrits sur le Site AWS à l'adresse https://aws.amazon.com/products (et tout lien qui lui succède ou lié à celui-ci, désigné par AWS), tel que mis à jour par AWS, le cas échéant. Les Services n'incluent aucun Contenu de Tiers. 2.2 Les accords de niveau de service qu'AWS propose concernant les Services sont disponibles à l'adresse https://aws.amazon.com/legal/service-level-agreements/ (et tout

Customer is responsible for implementing such measures and properly configuring the Services and taking such steps as Customer considers adequate and appropriate in relation to the availability, integrity, confidentiality and auditability of Health Data.	lien qui lui succède ou lié à celui-ci, désigné par AWS), tel que mis à jour par AWS, le cas échéant.
3. Location of Processing.	
3.1 Customer can specify the location(s) where Health Data will be processed within the AWS Network (each, a "**Region**"). Once Customer has made its choice, AWS will not transfer Health Data from Customer's selected Region(s), except as necessary to provide the Services initiated by Customer, or as necessary to comply with the law or binding order of a governmental body.	2.3 AWS met à disposition les Contrôles de Service que le Client peut choisir d'utiliser en ce qui concerne la disponibilité, l'intégrité, la confidentialité et l'auditabilité des Données de Santé. Les Contrôles de Service sont décrits dans l'Avenant RGPD d'AWS et dans la Documentation. Le Client est responsable de la mise en œuvre de ces mesures et de la configuration adéquate des Services et de la prise des mesures que le Client estime utiles et appropriées en ce qui concerne la disponibilité, l'intégrité, la confidentialité et l'auditabilité des Données de Santé.
3.2 It is Customer's responsibility to select the Region(s) for which AWS is certified under the HDS Certification. More information on these Regions is available on the HDS Certification (available on AWS Artifact).	**3. Lieu du Traitement.** 3.1 Le Client peut préciser le(s) lieu(x) où les Données de Santé seront traitées au sein du Réseau AWS (chacune, une « **Région** »). Lorsque le Client aura fait son choix, AWS ne transférera pas de Données de Santé depuis la ou les Région(s) sélectionnée(s) par le Client, sauf cas de nécessité pour fournir les Services initiés par le Client ou pour se conformer à la loi ou à toute décision contraignante d'une autorité administrative. 3.2 Il incombe au Client de sélectionner la ou les Région(s) pour lesquelles AWS est certifiée selon la Certification HDS. De plus amples informations sur ces Régions sont disponibles sur la Certification HDS (disponible sur le lien d'AWS Artifact).
4. Protection of Data Subjects.	**4. Protection des Personnes Concernées.**
4.1 **Controls, Features and Functionalities available to Customer.** AWS makes available many Service Controls that Customer may elect to use to comply with its obligations towards data subjects. These measures are described in the AWS GDPR DPA and in the Documentation. 4.2 **Right to Data Portability.** Customer can use Service Controls to assist it with its obligations under the Applicable Regulation, including its obligations to respond to data portability requests from data subjects.	

4.3 Security Breach Notification. 4.3.1 AWS will (a) notify Customer of a Security Incident without undue delay after becoming aware of the Security Incident, and (b) take appropriate measures to address the Security Incident, including measures to mitigate any adverse effects resulting from the Security Incident. 4.3.2 To enable Customer to notify a Security Incident to supervisory authorities or data subjects (as applicable), AWS will cooperate with and assist Customer by including in the above notification such information about the Security Incident as AWS is able to disclose to Customer, taking into account the nature of the processing, the information available to AWS, and any restrictions on disclosing the information, such as confidentiality. Taking into account the nature of the processing, Customer agrees that it is best able to determine the likely consequences of a Security Incident. 4.3.3 Notification(s) of Security Incidents, if any, will be delivered to one or more of Customer's administrators by any means AWS selects, including via email. **4.4 Audits.** 4.4.1 Upon Customer's request, and provided that the parties have an applicable NDA in place, AWS will make available the following documents and information: (a) the certificates issued for the ISO 27001 certification, the ISO 27017 certification, the ISO 27018 certification,	4.1 **Contrôles, fonctions et fonctionnalités à la disposition du Client.** AWS met à disposition de nombreux Contrôles de Service que le Client peut choisir d'utiliser pour se conformer à ses obligations vis-à-vis des personnes concernées. Ces mesures sont décrites dans l'Avenant RGPD d'AWS et dans la Documentation. 4.2 **Droit à la portabilité des données.** Le Client peut utiliser des Contrôles de Service pour l'assister dans ses obligations au titre de la Réglementation Applicable, y compris ses obligations de réponse aux demandes de portabilité des données émanant des personnes concernées. **4.3 Notification de Violation de Sécurité.** 4.3.1 AWS (a) informera le Client de tout Incident de Sécurité dans les meilleurs délais après en avoir pris connaissance et (b) prendra les mesures adéquates pour traiter l'Incident de Sécurité, y compris des mesures visant à atténuer tout effet préjudiciable de l'Incident de Sécurité. 4.3.2 Afin de permettre au Client de notifier un Incident de Sécurité aux autorités de contrôle ou aux personnes concernées (selon le cas), AWS collaborera avec le Client et l'assistera en intégrant à l'information susvisée les informations relatives à l'Incident de Sécurité qu'AWS est en mesure de divulguer au Client, en tenant compte de la nature du traitement, des informations à la disposition d'AWS et de toute restriction relative à la divulgation des informations, telle que la confidentialité. Compte tenu de la nature du traitement, le Client convient qu'il est le plus apte à déterminer les conséquences probables d'un Incident de Sécurité.

and the ISO 27701 certification (or the certifications or other documentation evidencing compliance with such alternative standards as are substantially equivalent to ISO 27001, ISO 27017, ISO 27018, and ISO 27701); and (b) the System and Organization Controls (SOC) 1 Report, the System and Organization Controls (SOC) 2 Report and the System and Organization Controls (SOC) 3 Report (or the reports or other documentation describing the controls implemented by AWS that replace or are substantially equivalent to the SOC 1, SOC 2 and SOC 3). 4.4.2 AWS uses external auditors to verify the adequacy of its security measures, including the security of the physical data centers from which AWS provides the Services. This audit: (a) will be performed at least annually; (b) will be performed according to ISO 27001 standards or such other alternative standards that are substantially equivalent to ISO 27001; (c) will be performed by independent third party security professionals at AWS's selection and expense; and (d) will result in the generation of an audit report ("**Report**"), which will be AWS's Confidential Information. 4.4.3 At Customer's written request, and provided that the parties have an applicable NDA in place, AWS will provide Customer with a copy of the Report so that Customer can reasonably verify AWS's compliance with its obligations under this HDS Addendum.	4.3.3 La ou les Notification(s) d'Incidents de Sécurité seront, le cas échéant, envoyées à un ou plusieurs administrateur(s) du Client par tout moyen choisi par AWS, y compris par email. **4.4 Audits.** 4.4.1 À la demande du Client, et à condition que les parties disposent d'un Accord de Confidentialité applicable, AWS mettra à disposition les documents et informations suivants : (a) les certificats délivrés pour la certification ISO 27001, la certification ISO 27017, la certification ISO 27018 et la certification ISO 27701 (ou les certifications ou autres documents attestant de la conformité à des normes alternatives sensiblement équivalentes aux normes ISO 27001, ISO 27017, ISO 27018 et ISO 27701) ; et (b) le Rapport sur les Contrôles de Système et d'Organisation (*System and Organization Controls* ou SOC) 1, le Rapport sur les Contrôles de Système et d'Organisation (*System and Organization Controls* ou SOC) 2 et le Rapport sur les Contrôles de Système et d'Organisation (*System and Organization Controls* ou SOC) 3 (ou les rapports ou autres documents décrivant les contrôles mis en œuvre par AWS qui remplacent ou sont sensiblement équivalents aux SOC 1, SOC 2 et SOC 3).

4.4.4 Customer chooses to conduct any audit, including any inspection, it has the right to request or mandate on its own behalf, and on behalf of its controllers when Customer is acting as a processor, under the GDPR or the Standard Contractual Clauses, by instructing AWS to carry out the audit described in this Section 4.4. **5. Communication.** With regard to the notification of Security Incidents under Section 4.3, it is Customer's sole responsibility to ensure Customer's administrators maintain accurate contact information, including name/surname, email address and phone number, on the AWS management console and secure transmission at all times. **6. Service Level Agreements.** In addition to the service level agreements that AWS offers, as referred to under Section 2.2, AWS publishes information on service availability on the AWS Service Health Dashboard (and any successor or related site designated by AWS), as may be updated by AWS from time to time. **7. Sub-processing. Authorised Sub-processors.** 7.1 Customer provides general authorization to AWS's use of sub-processors to provide processing activities on Health Data on behalf of Customer ("**Sub-processors**") in accordance with this Section.	4.4.2 AWS fait appel à des auditeurs externes pour vérifier l'adéquation de ses mesures de sécurité, y compris la sécurité des centres de données physiques à partir desquels AWS fournit les Services. Cet audit : (a) sera réalisé au moins une fois par an ; (b) sera réalisé conformément à la norme ISO 27001 ou aux autres normes alternatives sensiblement équivalentes à la norme ISO 27001 ; (c) sera réalisé par des professionnels de la sécurité tiers indépendants aux frais et choisis par AWS ; et (d) donnera lieu à la production d'un rapport d'audit (le « **Rapport** »), lequel constituera une Information Confidentielle d'AWS. 4.4.3 À la demande écrite du Client, et à condition que les parties aient mis en place un Accord de confidentialité applicable, AWS remettra au Client une copie du Rapport afin que le Client puisse raisonnablement vérifier le respect par AWS de ses obligations au titre du présent Avenant HDS. 4.4.4 Le Client choisit de réaliser tout audit, y compris toute inspection, qu'il est en droit de demander ou de mandater pour son propre compte, et pour le compte de ses responsables du traitement lorsque le Client agit en qualité de sous-traitant, au titre du RGPD ou des Clauses Contractuelles Types, en donnant instruction à AWS de réaliser l'audit décrit au présent Article 4.4. **5. Communication.** En ce qui concerne la Notification des Incidents de Sécurité prévue à l'Article 4.3, il incombe exclusivement au Client de s'assurer que les administrateurs du Client disposent de coordonnées exactes, y compris le

7.2 Where AWS authorises a Sub-processor as described in this Section 7: (a) AWS will restrict the Sub-processor's access to Health Data only to what is necessary to provide or maintain the Services in accordance with the Documentation, and AWS will prohibit the Sub-processor from accessing Health Data for any other purpose; (b) AWS will enter into a written agreement with the Sub-processor and, to the extent that the Sub-processor performs the same data processing services provided by AWS under this HDS Addendum, AWS will impose on the Sub-processor the same contractual obligations that AWS has under this HDS Addendum; and (c) AWS will remain responsible for its compliance with the obligations of this HDS Addendum and for any acts or omissions of the Sub-processors that cause AWS to breach any of AWS's obligations under this HDS Addendum. **8. Means used to regulate Health Data access.** 8.1 AWS has implemented and will maintain the technical and organisational measures for the AWS Network as described in the AWS Security Standards and in this Section 8. In particular, AWS has implemented and will maintain the following technical and organisational measures, as described in the AWS Security Standards:	nom/prénom, l'adresse électronique et le numéro de téléphone, sur la console de gestion AWS et de sécuriser la transmission à tout moment. **6. Accords de niveau de service.** En plus des accords de niveau de service qu'AWS propose, tels que visés à l'Article 2.2, AWS publie des informations sur la disponibilité du service sur le AWS Service Health Dashboard (et tout site qui lui succède ou lié à celui-ci, désigné par AWS), tel que mis à jour par AWS, le cas échéant. **7. Sous-traitance ultérieure. Sous-traitants ultérieurs autorisés.** 7.1 Le Client autorise de manière générale le recours par AWS à des sous-traitants ultérieurs pour fournir des activités de traitement des Données de Santé pour le compte du Client (les « **Sous-traitants Ultérieurs** ») conformément au présent Article. 7.2 Lorsque AWS autorise un Sous-traitant Ultérieur tel que décrit au présent Article 7 : (a) AWS limitera l'accès du Sous-traitant Ultérieur aux Données de Santé au strict nécessaire pour fournir ou maintenir les Services conformément à la Documentation, et AWS interdira au Sous-traitant Ultérieur d'accéder aux Données de Santé à quelque autre fin ; (b) AWS conclura un accord écrit avec le Sous-traitant Ultérieur et, dans la mesure où ce dernier exécute les mêmes services de traitement de données que ceux

(a) security of the AWS Network; (b) physical security of the facilities; (c) measures to control access rights for AWS employees and contractors for the AWS Network; and (d) processes for regularly testing, assessing and evaluating the effectiveness of the technical and organisational measures implemented by AWS. 8.2 Customer can elect to implement technical and organisational measures to protect Health Data. Such technical and organisational measures include the following which can be obtained by Customer from AWS as described in the Documentation, or directly from a third party supplier: (a) pseudonymisation and encryption to ensure an appropriate level of security; (b) measures to ensure the ongoing confidentiality, integrity, availability and resilience of the processing systems and services that are operated by Customer; (c) measures to allow Customer to backup and archive appropriately in order to restore availability and access to Health Data in a timely manner in the event of a physical or technical incident; and (d) processes for regularly testing, assessing and evaluating the effectiveness of the technical and organisational measures implemented by Customer.	fournis par AWS au titre du présent Avenant HDS, AWS imposera au Sous-traitant Ultérieur les mêmes obligations contractuelles qu'AWS au titre du présent Avenant HDS ; et (c) AWS demeurera responsable du respect des obligations du présent Avenant HDS et de toute action ou omission des Sous-traitants Ultérieurs en conséquence de laquelle AWS violerait l'une quelconque de ses obligations au titre du présent Avenant HDS. **8. Moyens mis en œuvre pour encadrer l'accès aux Données de Santé.** 8.1 AWS a mis en œuvre et maintiendra les mesures techniques et organisationnelles pour le Réseau AWS décrites dans les Normes de Sécurité d'AWS et au présent Article 8. En particulier, AWS a mis en œuvre et maintiendra les mesures techniques et organisationnelles suivantes, telles que décrites dans les Normes de Sécurité d'AWS : (a) la sécurité du Réseau AWS ; (b) la sécurité physique des installations ; (c) des mesures de contrôle des droits d'accès pour les salariés et sous-traitants d'AWS pour le Réseau AWS ; et (d) des processus permettant de tester, d'apprécier et d'évaluer régulièrement l'efficacité des mesures

9. Modification of the Services. 9.1 Customer and AWS each represents and warrants to the other that it will comply with all applicable laws, rules, regulations and ordinances in the performance of this HDS Addendum (and, in the case of Customer, the use of the Services). 9.2 AWS may change or discontinue any of the Service Offerings, from time to time, including to comply with the Applicable Regulation. AWS will provide Customer at least 12 months' prior notice if AWS discontinues a material functionality of a Service that the Customer is using, or materially alter a customer-facing API that the Customer is using in a backwards-incompatible fashion, except that this notice will not be required if the 12 month notice period (a) would pose a security or intellectual property issue to AWS or the Services, (b) is economically or technically burdensome, or (c) would cause AWS to violate legal requirements. **10. Availability Restoration Features.** AWS makes available many Service Controls that Customer can elect to use. Customer is responsible for using the Service Controls to allow Customer to restore availability and access to Health Data in a timely manner in the event of a physical or technical incident, and taking such steps as Customer considers adequate to maintain appropriate security, protection, and deletion of Health Data. **11. Data Privacy.** AWS will not access or use Health Data, except as necessary to maintain or provide the Service Offerings, or as necessary to comply with the law or a binding order of a governmental body.	techniques et organisationnelles mises en œuvre par AWS. 8.2 Le Client pourra choisir de mettre en œuvre des mesures techniques et organisationnelles pour protéger les Données de Santé. Ces mesures techniques et organisationnelles comprennent les éléments suivants qui peuvent être obtenus par le Client auprès d'AWS tel que décrit dans la Documentation, ou directement auprès d'un prestataire tiers : (a) pseudonymisation et chiffrement afin d'assurer un niveau de sécurité approprié ; (b) des mesures visant à garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et services de traitement exploités par le Client ; (c) des mesures permettant au Client une sauvegarde et un archivage adéquates afin de rétablir la disponibilité et l'accès aux Données de Santé en temps utile en cas d'incident physique ou technique ; et (d) des processus permettant de tester, d'apprécier et d'évaluer régulièrement l'efficacité des mesures techniques et organisationnelles mises en œuvre par le Client. **9. Modification des Services.** 9.1 Le Client et AWS déclarent et garantissent réciproquement qu'ils se conformeront à l'ensemble des lois, règles,

12. Return or Deletion of Health Data. At any time up to the HDS Addendum Termination Date, and for 90 days following the HDS Addendum Termination Date, subject to the terms and conditions of the Agreement, AWS will return or delete Health Data when Customer uses the Service Controls to request such return or deletion. No later than the end of this 90-day period, Customer will close all AWS accounts containing Health Data. **13. Law Enforcement Request.** If a governmental body sends AWS a demand for Health Data, AWS will attempt to redirect the governmental body to request that data directly from Customer. As part of this effort, AWS may provide Customer's basic contact information to the governmental body. If compelled to disclose Health Data to a governmental body, then AWS will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless AWS is legally prohibited from doing so. **14. Customer Compliance.** Customer is responsible for taking such steps as Customer considers necessary or appropriate to comply with the requirements of the Applicable Regulation. If Customer is subject to the French "Politique générale de sécurité des systems d'information de santé" (PGSSI-S), Customer agrees that its use of the Services complies at all times with the PGSSI-S. **15. Customer Point of Contact.** Customer is responsible for providing AWS with proper point of contact. It is Customer's sole responsibility to ensure Customer's administrators maintain accurate contact information on the AWS management console	réglementations et ordonnances applicables dans le cadre de l'exécution du présent Avenant HDS (et, s'agissant du Client, l'utilisation des Services). 9.2 AWS pourra parfois modifier ou interrompre l'une quelconque des Offres de Services, y compris pour se conformer à la Réglementation Applicable. AWS remettra au Client une notification avec préavis d'au moins 12 mois si AWS interrompt une fonctionnalité significative d'un Service que le Client utilise, ou modifie de manière significative une API destinée au client que le Client utilise de manière rétrocompatible, étant toutefois précisé que cette notification ne sera pas requise si le préavis de 12 mois (a) est susceptible de poser un problème de sécurité ou de propriété intellectuelle à AWS ou aux Services, (b) est économiquement ou techniquement complexe ou (c) contraindrait AWS à enfreindre toute exigence légale. **10. Fonctionnalités de restauration de la disponibilité.** AWS met à disposition de nombreux Contrôles de Service que le Client peut choisir d'utiliser. Il incombe au Client d'utiliser les Contrôles des Services afin de pouvoir rétablir la disponibilité et l'accès aux Données de Santé en temps utile en cas d'incident physique ou technique, et de prendre les mesures que le Client considère adéquates pour maintenir une sécurité, une protection et une suppression appropriées des Données de Santé. **11. Protection des données.** AWS s'interdit d'accéder aux Données de Santé ou de les utiliser, sauf cas de nécessité pour maintenir ou fournir les Offres de Services ou pour se conformer à la loi ou à toute décision contraignante d'une autorité administrative.

and secure transmission at all times, and that this point of contact is able to provide AWS with the name of a health professional so that AWS may comply with the request of a competent authority for such information. **16. Duration.** This HDS Addendum shall continue in force until the earlier of (a) the Termination Date, or (b) the date AWS loses its HDS Certification as defined under Section 1, whether by virtue of its non-renewal, withdrawal or suspension ((a) or (b), the "**HDS Addendum Termination Date**"). **17. Nondisclosure.** Customer agrees that the details of this HDS Addendum are not publicly known and constitute AWS's Confidential Information under the confidentiality provisions of the Agreement or NDA. If the Agreement does not include a confidentiality provision protecting AWS Confidential Information and Customer and AWS or its Affiliates do not have an NDA in place covering this HDS Addendum, then Customer will not disclose the contents of this HDS Addendum to any third party except as required by law. **18. Entire Agreement; Conflict.** Except as supplemented by this HDS Addendum, the AWS GDPR DPA and the Agreement will remain in full force and effect. If there is a conflict between the terms of this HDS Addendum and the terms of either the Agreement or the AWS GDPR DPA, the terms of this HDS Addendum will control. **19. Counterparts and Facsimile or Email Delivery.** This HDS Addendum may be executed in two or more counterparts, each of which will be deemed an original and all of which taken together will be deemed to constitute one and the same	**12. Restitution ou suppression des Données de Santé.** À tout moment jusqu'à la Date de Fin de l'Avenant HDS, et pendant 90 jours à compter de la Date de Fin de l'Avenant HDS, sous réserve des dispositions et conditions du Contrat, AWS restituera ou supprimera les Données de Santé si le Client a recours aux Contrôles des Services pour solliciter cette restitution ou suppression. Au plus tard à la fin de cette période de 90 jours, le Client clôturera tous les comptes AWS renfermant des Données de Santé. **13. Demande d'application de la loi.** Si une autorité administrative ou gouvernementale envoie à AWS une demande de Données de Santé, AWS tentera de rediriger ladite autorité afin qu'elle sollicite ces données directement auprès du Client. À cet effet, AWS pourra fournir les coordonnées de base du Client à cette autorité administrative ou gouvernementale. En cas d'obligation de divulgation des Données de Santé à une autorité administrative ou gouvernementale, AWS informera le Client dans un délai raisonnable de la demande afin de permettre au Client de solliciter une décision contraignante ou tout autre recours approprié, sauf interdiction légale applicable à AWS. **14. Conformité du Client.** Il incombe au Client de prendre les mesures qu'il juge nécessaires ou adéquates pour se conformer aux exigences de la Réglementation Applicable. Si le Client est soumis à la Politique générale de sécurité des systèmes d'information de santé (PGSSI-S), le Client accepte que son utilisation des Services soit en permanence conforme au PGSSI-S. **15. Point de contact du Client.** Le Client est tenu de fournir à AWS un point de contact approprié. Il incombe exclusivement au

document. The parties may deliver this HDS Addendum by facsimile or email transmission. **20. Definitions.** **"Applicable Regulation"** means Articles L. 1111-8 and seq. of the French Public Health Code, together with the HDS certification reference standard issued by the French Digital Healthcare Agency (Agence du Numérique en Santé (ANS)). **"Health Data"** means Customer Data when its processing is regulated under the Applicable Regulation and constitutes "data concerning health" (as defined in the GDPR).	Client de s'assurer que les administrateurs du Client maintiennent des coordonnées exactes sur la console de gestion AWS et sécurisent la transmission à tout moment, et que ce point de contact soit en mesure de fournir à AWS le nom d'un professionnel de santé pour qu'AWS puisse se conformer à toute demande d'informations émanant d'une autorité compétente. **16. Durée.** Le présent Avenant HDS demeurera en vigueur jusqu'à la première des dates suivantes : (a) la Date de Fin ou (b) la date à laquelle AWS perd sa Certification HDS telle que définie à l'Article 1, que ce soit du fait de son non-renouvellement, de son retrait ou de sa suspension ((a) ou (b), la « **Date de Fin de l'Avenant HDS** »). **17. Non-divulgation.** Le Client convient que les détails du présent Avenant HDS ne sont pas connus du public et constituent des Informations Confidentielles d'AWS au regard des dispositions de confidentialité du Contrat ou de l'Accord de Confidentialité. Si le Contrat ne prévoit aucune disposition de confidentialité protégeant les Informations Confidentielles d'AWS et si le Client et AWS ou ses Sociétés Affiliées n'ont pas mis en place d'Accord de Confidentialité couvrant le présent Avenant HDS, le Client ne divulguera le contenu du présent Avenant HDS à aucun tiers sauf disposition légale contraire. **18. Intégralité de l'Avenant ; Conflit.** À l'exception des éléments complétés par le présent Avenant HDS, l'Avenant RGPD d'AWS et le Contrat demeureront en vigueur et de plein effet. En cas de conflit entre les dispositions du présent Avenant HDS et les dispositions du Contrat ou de l'Avenant RGPD d'AWS, les dispositions du présent Avenant HDS prévaudront.

	19. Exemplaires et envoi par télécopie ou par email. Le présent Avenant HDS pourra être signé en deux exemplaires ou davantage, dont chacun sera réputé un original et dont l'ensemble constituera un seul et même acte. Les parties pourront remettre le présent Avenant HDS par télécopie ou transmission par email. **20. Définitions.** **« Réglementation Applicable »** désigne les articles L. 1111-8 et suivants du Code de la santé publique, ainsi que le référentiel de certification HDS délivré par l'Agence du Numérique en Santé (ANS). **« Données de Santé »** désigne les Données du Client lorsque leur traitement est réglementé en vertu de la Réglementation Applicable et constitue des « données concernant la santé » (telles que définies dans le RGPD).