TB CAD Data Processing Agreement Template

June 2021

AGREEMENT TABLE OF CONTENTS

Introduction

This Data Processing Agreement (the "DPA") establishes the terms and measures for the sharing and processing of data among the undersigned parties (the “Data Controller” and “Data Processor”) and may be required by law or regulation to which the parties are subject.

The Data Controller and Data Processor agree as follows:

1. Definitions

All capitalized terms used in this DPA will have the meaning given to them here. Terms not defined here will have the meaning as set forth in the Principal Agreement.

"Additional Instructions" means any instructions from Data Controller to the Data Processor that arise after the execution of this DPA.

"Data Concerning Health" means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

"Data Protection Laws" means all data protection and privacy laws and regulations applicable to the processing of data under this DPA, including in the countries of the Data Controller and Data Processor and, if applicable, EU Data Protection Law.

"Data Protection Officer" means an individual or team of individuals working as personnel or agents of the Data Processor who are fully informed and responsible for communicating with the Data Controller about the Data Processor's technical and organizational measures for the confidentiality, security, and integrity of the Data Controller's Personal Data.

"Data Subject" means an identified or identifiable individual who can be identified directly or indirectly by reference to an identifier such as a name, an ID number, location data, an online ID, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

"EU Data Protection Law" means Regulation (EU) 2016/679 (the General Data Protection Regulation or GDPR) of the European Parliament and of the Council together on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (repealing Directive 95/46/EC) together with any subordinate legislation or regulation implementing the General Data Protection Regulation.

"Instructions" means the written, documented instructions issued by the Data Controller to the Data Processor and directing the Data Processor to perform a specific or general action (i.e., Processing) regarding Personal Data.

"Personal Data" means any information relating to an identified or identifiable natural person (i.e., a Data Subject) who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

"Process" or "Processing" means any operation or set of operations that is performed on Personal Data or sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

"Principal Agreement" is the main contract that establishes the terms for the Data Processor's provision of goods and services to the Data Controller.

"Security Incident" means any unauthorized or unlawful breach of security that leads to the accidental or unlawful destruction, loss, alteration, or unauthorized disclosure of or access to Personal Data.

"Services" means any product or service provided by the Data Processor to the Data Controller pursuant to and as described in this DPA.

"Supervisory Authority" means an independent public authority that is established pursuant to Data Protection Laws, including the EU Data Protection Law.

"Sub-Processor" means a third-party subcontractor engaged by the Data Processor as required to perform the Services under this DPA to Process the Data Controller's Personal Data.

2. Scope and Subject Matter

2.1 This DPA applies to the Data Processor's Processing of Personal Data on behalf of the Data Controller. The Data Processor will Process Personal Data as necessary to perform the Services under the Principal Agreement and as further instructed by the Data Controller during the Data Controller's use of the Services. This DPA regulates the measures to protect Personal Data in accordance with Data Protection Laws, including, if applicable, the EU Data Protection Law.

2.2 This DPA will not be interpreted in a way that conflicts with rights or obligations provided for in Data Protection Laws, including, if applicable, the EU Data Protection Law.

2.3 The Personal Data Processed by the Data Processor under this DPA and the details of the Processing are described in Annex 1: Data Processing Description.

2.4 Additional Instructions or terms (if any) outside the scope of this DPA require a prior written agreement between the Data Processor and Data Controller. An agreement on any additional fees payable by Data Controller to the Data Processor for carrying out Additional Instructions must also be established in writing between the Data Processor and Data Controller.

3. Docking Clause

3.1 An entity that is not a party to this DPA may, with the agreement of the Data Controller(s) and Data Processor, accede to this DPA at any time as a Data Controller by providing its information and signature in the List of Parties at the end of the agreement.

3.2 Once the entity has provided its information and signature, the acceding entity will become a party to this DPA and have the rights and obligations of a Data Controller.

3.3 The acceding entity will have no rights or obligations arising under this DPA from the period prior to becoming a party to the agreement.

4. Confidentiality

4.1 The Data Processor will treat all Personal Data as confidential and is obliged to ensure that all its personnel, agents, and Sub-Processors authorized to Process the Data Controller's Personal Data have committed themselves in writing to confidentiality or are under a legally binding statutory obligation of confidentiality before taking up the Processing of the Data Controller's data. The Data Processor will further ensure that its personnel, agents, and Sub-Processors are sufficiently informed of Data Protection Laws, including, if applicable, the EU Data Protection Law, and are familiar with this DPA and the Instructions of the Data Controller.

4.2 The Data Processor will further ensure the confidentiality of the Data Controller's Personal Data in line with Annex 2: Technical and Organizational Measures for Confidentiality, Security, and Integrity.

4.3 The Data Controller will be obliged to respect the confidentiality of all the Data Processor's business secrets and data protection measures which may be disclosed within the framework of the contractual relationship established by this DPA or the Principal Agreement.

4.4 The confidentiality obligations of the Data Processor and Data Controller will continue to apply after the termination of their contractual relationship for a period of five years.

5. Data Controller Responsibilities and Rights

5.1 The Data Controller will be responsible within the framework of this DPA for complying with Data Protection Laws, including, if applicable, the EU Data Protection law, particularly in relation to the Instructions it provides the Data Processor.

5.2 The Data Controller has the right to give Instructions, in writing, to the Data Processor regarding all Services and Processing of its Personal Data, in cases of Security Incidents, and for any additional data security measures. These Instructions may subsequently be amended, supplemented, or replaced by written Additional Instructions of the Data Controller to the Data Processor.

5.3 The Data Controller has the right to inspect or audit the Data Processor's activities, including its Processing, to ensure adequate data security, confidentiality, and data protection measures in line with this DPA and Data Protection Laws. An independent auditor may also perform these audits on behalf of the Data Controller.

6. Data Processor Responsibilities

6.1 The Data Processor will be responsible within the framework of this DPA for complying with Data Protection Laws, including, if applicable, the EU Data Protection Law, and protecting the rights of Data Subjects under Data Protection Laws in all its Processing and provision of Services.

6.2 The Data Processor will only process the Data Controller's Personal Data on documented instructions from the Data Controller and only to the extent required for the provision of the Services, unless required to do so by law to which the Data Processor is subject. In such a case, the Data Processor will inform the Data Controller of that legal requirement before Processing, unless the law prohibits the sharing of such information on important grounds of public interest.

6.3 The Data Processor will maintain a record of its Processing activities pursuant to this DPA and make these records and any other relevant information available to the Data Controller to demonstrate its compliance with this DPA and Data Protection Laws and contribute to inspections and audits conducted by the Data Controller, an independent auditor mandated by the Data Controller, or a Supervising Authority.

6.4 The Data Processor, considering the nature of the Processing, will assist the Data Controller by appropriate technical and organizational measures in the fulfillment of

the Data Controller's obligations to respond to requests from Data Subjects to exercise their rights under Data Protection Laws.

7. Data Security and Integrity

7.1 The Data Processor, considering the state of the art, the costs of implementation, the nature, scope, context, purposes, and risks involved in the Services and Processing, and the rights of Data Subjects under Data Protection Laws, will implement appropriate technical and organizational measures to protect against Security Incidents and ensure the confidentiality, security, and integrity of the Data Controller's Personal Data, including during transmission, as described in Annex 2: Technical and Organizational Measures for Confidentiality, Security, and Integrity.

7.2 The Data Processor will take reasonable steps to ensure all its personnel, agents, and Sub-Processors authorized to Process the Data Controller's Personal Data are aware of and, to the extent necessary, have been trained on the implementation and maintenance of the Data Processor's technical and organizational measures to ensure the confidentiality, security, and integrity of the Data Controller's Personal Data as described in Annex 2: Technical and Organizational Measures for Confidentiality, Security, and Integrity.

7.3 The Data Processor will appoint a Data Protection Officer to be the primary point of contact for the Data Controller for information or concerns related to the confidentiality, security, and integrity of the Data Controller's Personal Data and for assistance in fulfilling the reasonable requests of Data Subjects, including those arising from Data Protection Laws. The Data Processor will appoint a Data Protection Officer to be the primary point of contact for the Data Controller for information or concerns related to the confidentiality, security, and integrity of the Data Controller's Personal Data. The Data Processor will provide the Data Controller with the name and contact details of the Data Protection Officer.

7.4 The Data Processor will immediately inform the Data Controller in the event of a Security Incident, comply with and assist the Data Controller in complying with all Data Protection Laws implicated by the Security Incident, and explain to the Data Controller the measures it is taking to address and mitigate any damage resulting from the Security Incident and to protect the Data Controller's Personal Data. Among other things, the Data Processor will describe to the Data Controller the nature and duration of the Security Incident, the Services impacted, the approximate number of Data Subjects affected, and the likely consequences.

8. Data Subjects Rights

8.1 The Data Processor will assist the Data Controller in responding to inquiries and requests made by Data Subjects, including those arising from Data Protection laws, for access to or rectification, erasure, restriction, portability, blocking, or deletion of their Personal Data, including any Data Concerning Health.

8.2 Data Subjects may invoke and enforce this DPA as third-party beneficiaries against the Data Processor or Data Controller under Data Protection Laws to the extent they have suffered actual harm or damages resulting from the Processing of their Personal Data, including any Data Concerning Health.

8.3 When both the Data Processor and Data Controller are responsible for harm or damages caused to a Data Subject resulting from the Processing of their Personal Data, including any Data Concerning Health, they will be jointly and severally liable, and the Data Subject will be entitled to bring an action in court against either or both the Data Processor and Data Controller.

9. Sub-Processors

9.1 The Data Processor may only engage Sub-Processors based on the Data Controller's prior authorization and upon reasonable advance notice.

9.2 The Data Processor will enter into a written agreement with each Sub-Processor committing the Sub-Processor to comply with Data Protection Laws and the relevant provisions of this DPA related to the confidentiality, security, and integrity of the Data Controller's Personal Data. The Data Processor will be responsible for all the Sub-Processor's acts or omissions within the framework of this DPA.

9.3 The Data Processor will verify and document a Sub-Processor's capacity to comply with Data Protection Laws and this DPA before seeking the Data Controller's authorization to engage the Sub-Processor. The Data Processor will further confirm and document the Sub-Processor's capacity in regular intervals as long as the Sub-Processor is involved in the Processing of the Data Controller's Personal Data under this DPA.

9.4 The Data Controller may object in writing to the Data Processor's engagement of a Sub-Processor on reasonable grounds relating to data confidentiality, security, or integrity in writing within five business days of its receipt of the Data Processor's notification expressing its intent to engage the Sub-Processor. The Data Controller's notice of objection will explain its grounds for the objection and, if required, the Data Controller will discuss its concerns in good faith with the Data Processor with a view to reaching a reasonable resolution.

9.5 All Sub-Processors engaged by the Data Processor to Process the Data Controller's Personal Data will be added to Annex 3: List of Sub-Processors.

10.Term and Data Deletion or Return

10.1 The term and duration of this DPA will follow the term and duration of the Principal Agreement.

10.2 The Data Processor will, at the choice of the Data Controller, delete all the Data Controller's Personal Data and certify that it has done so or return all the Data Controller's Personal Data and delete all existing copies at the end of the provision of Services as determined by the Principal Agreement or upon the request of the Data Controller.

10.3 The Data Processor will notify all Sub-Processors of the termination of the Principal Agreement or a request from the Data Controller to delete or return its Personal Data and ensure the Sub-Processors delete or return, as requested by the Data Controller, all the Data Controller's Personal Data.

11.Liability and Indemnity

11.1 The Data Processor indemnifies the Data Controller and holds the Data Controller harmless against all claims, actions, third-party claims, losses, damages, and expenses incurred by the Data Controller arising out of a breach of this DPA or Data Protection Laws, including the EU Data Protection Law, by the Data Processor.

11.2 The Data Controller indemnifies the Data Processor and holds the Data Processor harmless against all claims, actions, third-party claims, losses, damages, and expenses incurred by the Data Processor arising out of a breach of this DPA or Data Protection Laws, including the EU Data Protection Law, by the Data Controller.

11.3 The Data Controller and Data Processor will be liable to the other party for any material or non-material damages it causes the other party by any breach of this DPA.

11.4 Liability as between the Data Controller and Data Processor is limited to actual damage suffered; punitive damages are excluded.

11.5 The Data Processor is liable for any act or omission on the part of a Sub-Processor in breach of this DPA. The Data Processor may not invoke the conduct of a Sub-Processor to avoid its own liability.

12.Governing Law, Jurisdiction, and Venue

12.1 This DPA will be governed by the law of the Data Controller's country.

12.2 Any disputes arising from or in connection with this DPA will be brought exclusively before the competent court of [COVENIENT COURT IN DATA CONTROLLER'S JURISDICTION].

12.3 In the event of any inconsistency between the provisions of this DPA and the Principal Agreement, the provisions of this DPA will prevail.

List of Parties

Executed by the parties authorized representatives:

[TB CAD USER 1]

Data Controller 1

Signature: _____

Name: _____

Title: _____

Email: _____

Date: _____

Corporate Entity Name:

_____

Corporate Entity Address:

_____

_____

_____

[TB CAD SUPPLIER]

Data Processor

Signature: _____

Name: _____

Title: _____

Date: _____

[TB CAD USER 2]

Data Controller 2

Signature: _____

Name: _____

Title: _____

Email: _____

Date: _____

Corporate Entity Name:

_____

Corporate Entity Address:

_____

_____

_____

[TB CAD USER 3]

Data Controller 3

Signature: _____

Name: _____

Title: _____

Email: _____

Date: _____

Corporate Entity Name:

_____

Corporate Entity Address:

_____

_____

_____

Data Controller 4

Signature: _____

Name: _____

Title: _____

Email: _____

Date: _____

Corporate Entity Name:

_____

Corporate Entity Address:

_____

_____

_____

Data Controller 5

Signature: _____

Name: _____

Title: _____

Email: _____

Date: _____

Corporate Entity Name:

_____

Corporate Entity Address:

_____

_____

_____

[Add additional Data Controllers here]

Appendix

Annex 1: Data Processing Description

Categories of Data Subjects

The Data Controller's Personal Data Processed by the Data Processor will come from the following categories of Data Subjects:

- [List categories of data subjects here, such as Patients; Members of communities undergoing systematic screening for tuberculosis; etc.]

Types of Personal Data to Be Processed

The Data Controller's Personal Data Processed by the Data Processor will include the following types, inclusive of Data Concerning Health:

- [List types of data here, such as Data Concerning Health; Unique identification numbers; Ages of patients of other individuals; Chest radiograph (i.e., x-ray) images in common image file formats, including DICOM, JPEG, and PNG; etc.]

Frequency of Data Processing

The Processing will occur:

- [List estimated frequency of the data processing, such as all at one time; on a daily basis; on a weekly basis; etc.]

Nature and Purpose of the Data Processing

The Processing will include the following operations and purposes:

- [List operations and purposes here, such as Storage, analysis, transfer, and other Processing necessary to provide, maintain, and improve the Services provided to the Data Controller; Numeric probability scores, abnormality heatmaps, or radiology-style reports; Technical support for the Data Controller; etc.]

Nature and Purpose of the Sub-Processors Data Processing

The Sub-Processor(s)' Processing of the Data Controller's Personal Data will include the following operations and purposes:

- [List operations and purposes here, such as Storage, analysis, transfer, and other Processing necessary to assist the Data Processor in providing, maintaining, or improving the Services provided to the Data Controller; etc.]

Annex 2: Technical and Organizational Measures for Confidentiality, Security, and Integrity

The Data Processor, considering the state of the art, the costs of implementation, the nature, scope, context, purposes, and risks involved in the Services and Processing, and the rights of Data Subjects under Data Protection Laws, will implement and require all Sub-Processors implement some or all the following measures as necessary to ensure the confidentiality, security, and integrity of the Data Controller's Personal Data:

- ⇒ Data De-Identification and Anonymization.
- ⇒ Data Encryption in transit and at rest, such as by Transport Layer Security (TSL) protocols, Self-Encrypting Drives, the Advanced Encryption Standard (AES), RSA (Rivest–Shamir–Adleman) encryption, or other methods.
- ⇒ Passwords and Multi-Factor Authentication (MFA).
- ⇒ Data and Network Access Controls, such as Role-Based Access Control, Virtual Private Networks (VPNs), Antivirus Software, and Auto-Lock.
- ⇒ Network Segmentation,
- ⇒ Measures to restore the availability and access to personal data in a timely manner in the event of a Security Incident.
- ⇒ Regular network and system maintenance and upkeep.
- ⇒ [Add additional measures here.]

Annex 3: List of Sub-Processors

Sub-Processor	Purpose	Location
1.		
2.		
3.		