Section 7: IDX DATA PROTECTION PLAN

In response to the RECIPIENT's request, PROVIDER asks that the RECIPIENT and the RECIPIENT SCIENTIST agree to abide by the following terms in protecting the DATA:

1. All Devices receiving, storing and/or transmitting IDx data must be configured according to the relevant standards outlined in HS 9457 Minimum Security Standards for Network Devices, including, but not limited to:

a. Devices must be running a supported version of the operating system.

b. The operating system and applications must be kept up to date on patches.

c. A current anti-virus program must be running and virus definitions must be kept up to date.

d. A unique ID and complex password or biometric identifier must be used to access the device.

e. A password-protected screen saver must come up after 15 minutes of inactivity.

f. The host-based firewall should be enabled.

g. Any required UCLA Health security software must be installed.

2. Data access will only occur through UCLA Health IT secured laptops, desktops, or servers. UCLA Health IT proof of encryption may be required. Personal devices may not be used unless current proof of encryption by UCLA Health IT can be provided.

3. Passwords must comply with UCLA Health MedNet standards:
https://mednet.uclahealth.org/it-files/master-password-faq.pdf

4. Encryption of devices and removable media must comply with HS Policy 9453-C, "Device and Removable Media Encryption". Individually identifiable information must not be stored on unencrypted USB drives or other removable media.

5. Any devices holding data should be stored securely in locked compartments or rooms when not in use. Any printouts of data or data outputs should be stored securely in locked compartments or rooms when not in use; and shredded once no longer needed.

6. IDx data will be transferred to the recipient via UCLA Health Box. If the recipient wants to provide IDx data to other personnel, those personnel must have approval to access the data from IDx and the UCLA IRB; and data may only be transferred to these personnel via UCLA Health Box. Data may not be transmitted over email or as an email attachment (either over the Internet, an Intranet system, or within a local area network).

7. All files containing PHI data must be destroyed at the completion of the project.

☐ Agree

Section 8: AGREEMENT FOR THE TRANSFER OF HUMAN DATA

In response to the RECIPIENT's request, PROVIDER asks that the RECIPIENT and the RECIPIENT SCIENTIST agree to the following before the PROVIDER transmits the DATA:

1. The above DATA is the property of the PROVIDER and is made available as a service to the research community.

2. THIS DATA WILL NOT BE USED TO TREAT OR DIAGNOSE HUMAN SUBJECTS.

3. The DATA will be used for teaching or research purposes only.

4. Research staff who have access to the Data Set must be listed under Key Personnel (with the appropriate data access authorizations) on the IRB application associated with this Agreement.

5. The Data may not be shared with any external third parties, academic or private. Data sharing plans for NIH grants need to be reviewed and approved by the relevant UCLA Health Data Release Committee(s) in advance of submission. There is a separate review process for studies seeking to share Health Data with external third parties.

6. In the event that the PI or any study team members leave UCLA, they shall not take a copy of the Data with them. The Data will remain within UCLA Health unless approval from the appropriate UCLA Health data release committee(s) has been granted.

7. The DATA will not be disclosed or further distributed to others without the PROVIDER's written consent. The RECIPIENT shall refer any request for the DATA to the PROVIDER.

8. Data User shall report to Covered Entity (CompOffice@mednet.ucla.edu) within one (1) business day of Data User becoming aware of any use or disclosure of the Data Set in violation of this Agreement or applicable law.

9. The Data User and study team will be responsive (within 48 hours) to any requests from IDx and UCLA Health Office of Compliance Services.

10. The RECIPIENT SCIENTIST agrees to acknowledge the contribution of the PROVIDER in all written or oral public disclosures concerning RECIPIENT's research using the DATA by including the following acknowledgement statement:

This work was supported by funds from the Integrated Diagnostics Program, Department of Radiological Sciences & Department of Pathology and Laboratory Medicine, David Geffen School of Medicine at UCLA.

11. RECIPIENT agrees to supply the PROVIDER with copies of public materials based on the use of the DATA.

12. The RECIPIENT agrees to provide any corrections that are identified as discrepancies during the course of analysis.

13. THE PROVIDER MAKES NO REPRESENTATIONS AND EXTENDS NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED. THERE ARE NO EXPRESS OR IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, OR THAT THE USE OF THE DATA WILL NOT INFRINGE ANY PATENT, COPYRIGHT, TRADEMARK, OR OTHER PROPRIETARY RIGHTS. Unless prohibited by law, RECIPIENT assumes all liability for claims for damages against it by third parties which may arise from the use, storage or disposal of the DATA.

14. The RECIPIENT agrees to use the DATA in compliance with all applicable statutes, regulations, and policies.

15. The DATA has been collected from human subjects. Personally identifiable information will not be provided unless the RECIPIENT SCIENTIST is a collaborator on the Integrated Diagnostics Program, UCLA Internal Review Board application. If the DATA being provided is coded (de-identified), the PROVIDER will not release, and the RECIPIENT will not request, the key to the code.

16. RECIPIENT will not contact or make any effort to identify individuals who are or may be the sources of DATA without specific written approval from PROVIDER.

17. DATA will be used by RECIPIENT SCIENTIST solely in connection with the Research Project described in the application. The data may not be used for any other purposes without approval of the relevant Program Scientific Advisory Board and Program stakeholders.

18. The RECIPIENT will not attempt to identify patients by associating information from the release of de-identified DATA with information from other identifiable DATA sources or requests.

19. Data provisioning is prioritized in part based on responsive and accurate communication. Lack of such communication may move the data request to the bottom of the prioritization list.

20. Violation of this Agreement is a serious offense and may result in disciplinary action up to and including termination of employment with the University and other actions as determined by the University.

a. 21. Covered Entity's Rights of Access and Inspection. From time to time upon reasonable notice, or upon a reasonable determination by Covered Entity that Data User has breached this Agreement, Covered Entity may inspect the facilities, systems, books and records of Data User to monitor compliance with this Agreement. The fact that Covered Entity inspects, or fails to inspect, or has the right to inspect, Data User's facilities, systems and procedures does not relieve Data User of its responsibility to comply with this Agreement, nor does Covered Entity's (1) failure to detect or (2) detection of, but failure to notify Data User or require Data User's remediation of, any unsatisfactory practices constitute acceptance of such practice or a waiver of Covered Entity's enforcement or termination rights under this Agreement. The parties' respective rights and obligations under this Section 21 shall survive termination of the Agreement.

21. IDx/Covered Entity may terminate this Agreement:

i. immediately if Data User is named as a defendant in a criminal proceeding for a violation of HIPAA or the HIPAA Regulations;

ii. immediately if a finding or stipulation that Data User has violated any standard or requirement of HIPAA, the HIPAA Regulations, or any other security or privacy laws is made in any administrative or civil proceeding in which Data User has been joined;

iii. immediately if Covered Entity determines that Data User has breached or violated a material term of this Agreement;

iv. immediately if Covered Entity determines that Data User no longer has a work-related need to access the Data Set.

v. immediately if it is in the best interest of Covered Entity, as deemed by Covered Entity in its sole discretion to do so; or

vi. pursuant to Section 21 of this Agreement.

22. Reporting to United States Department of Health and Human Services. In the event of a material breach or violation of this Agreement, Data User shall cooperate with Covered Entity to cure the breach or end the violation. If Covered Entity determines that the breach or violation is not curable, Covered Entity reserves the right to report Data User's breach or violation to the Secretary of the United States Department of Health and Human Services. Data User agrees that it shall not have or make any claim(s), whether at law, in equity, or under this Agreement, against Covered Entity with respect to such report(s).

This agreement is effective for a period of three (3) years from the date of final signature. Either Party may terminate this Agreement with thirty (30) days written notice to the other Party. Violation of the terms of this agreement render this agreement null and void. When the Research Project is completed, this Agreement expires, or this Agreement is terminated, whichever comes first, RECIPIENT shall promptly return to PROVIDER or, at PROVIDER'S option, destroy all copies of DATA, including copies and derivative versions. Upon PROVIDER's request, RECIPIENT shall confirm to its destruction though the IDx Certificate of Destruction.

☐ Agree