



AGREEMENT FOR DISCLOSURE AND TRANSFER OF CONFIDENTIAL INFORMATION AND PROTECTED HEALTH INFORMATION

This **Agreement for Disclosure and Transfer of Confidential Information and Protected Health Information** (“**Agreement**”) is effective as of the date of the last signature below by and between _____, located at _____ (“**Discloser**”) and Duke University, a tax-exempt research and educational institution located in Durham, North Carolina, acting for and on behalf of its Duke Clinical Research Institute (“**Duke**”).

WHEREAS, the NATIONAL INSTITUTE ON MINORITY HEALTH AND HEALTH DISPARITIES of the National Institutes of Health (“**Awarding Agency**”), has engaged Duke to serve as the Coordination and Data Collection Center (“**CDCC**”) for a federally-funded program of clinical research involving human subjects entitled: “*Rapid Acceleration of Diagnostics for Underserved Populations Coordination and Data Collection Center*” also referred to as “**RADx-UP CDCC**” (FAIN: U24MD016258, CFDA #93.310) (Duke IRB # Pro00106873) (the “**Project**”) under the direction of Duke’s investigator, Michael Cohen-Wolkowicz, MD (“**Duke Investigator**”);

WHEREAS, the Project aims to provide overarching support and guidance to the Awarding Agency on its administrative operations and logistics, facilitating effective use of COVID-19 testing technologies, supporting community and health system engagement and providing overall infrastructure for data collection, integration and sharing for Awarding Agency’s *Rapid Acceleration of Diagnostics for Underserved Populations* (“**RADx-UP**”) program;

WHEREAS, Discloser, under the direction of its lead investigator, [Project PI name] (“**Discloser Investigator**”), has received an award from the Awarding Agency to participate in the RADx-UP program and, accordingly, has agreed to share data with the Project;

WHEREAS, RADx-UP program includes the formation of a consortium (“**RADx-UP Consortium**”) to facilitate cooperation among various entities participating in RADx-UP program; Duke as the CDCC and Discloser are members of the RADx-UP Consortium;

WHEREAS, Duke has assisted the Awarding Agency to develop minimum necessary common data elements to guide RADx-UP program participants to submit research subjects’ data in support of the RADx-UP program (“**RADx-UP Common Data Elements**”);

WHEREAS, Discloser wishes to share with Duke, or Duke will be given access to (i) research subjects’ information that constitutes Protected Health Information (“**PHI**”), as defined in the Health Insurance Portability and Accountability Act of 1996, as amended (“**HIPAA**”), including, but not limited to, research subjects’ contact information and (ii) other information that Discloser considers to be confidential (“**Discloser Confidential Information**”) to enable Duke to: (a) obtain research subjects’ written informed consent/HIPAA authorization (“**Subject Authorization**”), RADx-UP Common Data Elements, related questionnaires, surveys and forms for performing data analyses and for collecting follow up data from research subjects; (b) better understand COVID-19 testing patterns among underserved and vulnerable populations; (c) strengthen the understanding of the impact of relevant data on disparities in infection rates, disease progression, and outcomes; (d) develop strategies to reduce disparities in COVID-19 testing; and (e) fulfill Duke’s obligation as the CDCC under the Project to provide de-identified Project data and the results of its analyses to the Awarding Agency (collectively, “**Duke Purpose**”); and

WHEREAS, Duke will share with Discloser, or Discloser will have access to, reports and resources in the Project’s RADx-UP resource library, confidential testing-related documentation, and other information that Duke considers to be confidential (“**Duke Confidential Information**”) to inform Discloser’s decisions and response to the COVID-19 crisis (“**Discloser Purpose**”). PHI, Discloser Confidential Information and Duke Confidential Information shall be collectively referred to hereinafter as “**Information**”.

NOW, THEREFORE, the parties hereby agree to the following terms and conditions:

1. Each party agrees that it shall treat Information it receives from the other party in strict confidence and shall avoid disclosure of the Information to any other person, firm or corporation, other than those who have a need to know the Information in order to carry out each party's respective Purpose, and who are subject to confidentiality obligations sufficient to carry out the intent of this Agreement.
2. Discloser certifies that (i) PHI was collected with the Subject Authorization of the individuals to whom it relates, that such Subject Authorizations do not prevent the use of PHI for the Duke Purpose set forth herein, and that release of PHI for the Duke Purpose shall be approved by Discloser's Institutional Review Board ("**IRB**"), or (ii) a waiver or alteration of consent and HIPAA authorization has been granted by Discloser's IRB. Each party is responsible for obtaining and complying with any review or approval required by the respective party's IRB or organizational policies.
3. Neither party shall transfer or sell the Information it receives to third parties or, as it relates to Duke, attempt to identify or contact any research subjects to whom the PHI pertains, except as necessary to fulfill each party's respective Purpose, and as authorized by the relevant party's IRB or by the Subject Authorization.
4. Excluding PHI, for which the following exceptions do not apply, neither party shall have any obligation, with respect to the other party's Information or any part thereof that:
 - a. is already known at the time of the disclosure from a source not associated with the Project or the RADx-UP program;
 - b. becomes publicly known without the wrongful act or breach of this Agreement by a party;
 - c. is rightfully received by the receiving party from a third party not associated with the Project or the RADx-UP program on a nonconfidential basis;
 - d. is approved for release by written authorization of the disclosing party;
 - e. is independently developed by a party without use of or reliance upon the other party's Confidential Information; or
 - f. is required to be disclosed by law or a court order, subject to the protections provided by the Certificate of Confidentiality provided by the Awarding Agency to all RADx-UP Consortium members.
5. Except as expressly provided in Section 1, Duke shall keep all PHI described in this Agreement in strict confidence. Each party's obligations of confidentiality with respect to the other party's Confidential Information (not PHI) shall continue for a period of five (5) years after the first to occur of termination of this Agreement or until the party returns or destroys the other party's Confidential Information pursuant to Section 10 below. PHI shall be kept in strict confidence without limitation of time.
6. All records containing PHI shall be maintained under appropriate electronic and physical security. Discloser shall encrypt all PHI in transit. All transmission of PHI shall be through the Project's Microsoft PowerApps portal. Duke shall report to Discloser any use or disclosure of PHI not provided for in this Agreement of which Duke becomes aware, and Duke shall take reasonable steps to limit any further such use or disclosure.
7. Discloser shall adopt, implement, and maintain appropriate physical and electronic security controls to protect against unauthorized access of any PHI or personally identifiable information of research subject(s), or any Duke employees, agents or customers in accordance with the requirements set forth in the Security Controls attached hereto as **Exhibit A**. Each party accepts responsibility and liability for its unauthorized disclosure of the other party's Information, shall immediately notify the other party of any breach of data security or other

unapproved release of the other party's Information or other personally identifiable information, and shall take appropriate steps to limit any further such use or disclosure.

8. Each party shall use the other party's Information solely for the receiving party's respective Purpose and shall not be entitled to make any other use of the other party's Information. No license or additional rights are provided to either party under any patent applications, copyrights, trade secrets, or other proprietary rights of the other party, and all Information provided to a party hereunder shall remain the property of the disclosing party.
9. The parties agree that neither shall receive any remuneration or compensation from other for the provision of Information to the receiving party under this Agreement, and as such, neither party's Financial Conflict of Interest policy shall apply.
10. Upon completion of each party's Purpose, the relevant party shall return all Information received from the disclosing party to that party, or at the disclosing party's election, destroy all Information and provide the disclosing party with written certification of such destruction. Notwithstanding the foregoing, Duke shall be permitted to provide de-identified Project data and the results of Duke's analyses to the Awarding Agency in order to fulfill the Duke Purpose and pursuant to the obligations of the RADx-UP Consortium. This Agreement shall terminate upon the return or destruction of all Information received from the other party; provided, however, that the obligations of confidentiality set forth herein shall continue as set forth in Section 5 above. Each party may retain one copy of the other party's Confidential Information (not PHI) for the purpose of monitoring its obligations of confidentiality hereunder.
11. Should Duke commit a material breach of this Agreement with respect to PHI, which is not cured within thirty (30) days after Duke receives notice of such breach from Discloser, then Discloser will discontinue disclosure of PHI and will report the breach to the Secretary, Department of Health and Human Services.
12. This Agreement may not be assigned by either party without the prior written consent of the other.
13. This Agreement represents the entire understanding between the parties, and supersedes all other agreements, express or implied, between the parties as to its subject matter. Any alteration, modification, or amendment to this Agreement must be in writing and signed by authorized representatives of each party.

IN WITNESS WHEREOF, the parties have signed or caused this Agreement to be signed as of the dates indicated below.

DUKE UNIVERSITY

[Institution Name]

By: _____
Susan E. Hayden, J.D.
Director, Research Program Collaborations
Office of Research Contracts
Date signed: _____

By: _____
Name: _____
Title: _____
Date signed: _____

[Exhibit A follows]

EXHIBIT A SECURITY CONTROLS

Discloser represents, warrants, covenants, and agrees that, with respect to the Information, Discloser has adopted, implemented, and maintains (and shall ensure that its employees, contractors and agents adopt, implement and maintain) the security controls as described below (“**Security Controls**”), to: (1) ensure the confidentiality, integrity, and availability of the Information the Discloser creates, receives, processes, maintains, or transmits on Duke’s behalf; (2) protect against any reasonably anticipated threats or hazards to the security or integrity of such information; (3) protect against any reasonably anticipated uses or disclosures of such information that are not permitted by applicable law and this Agreement; and (4) ensure compliance by its workforce, including its contractors, developers, employees and agents.

1. **Maintain a formal Information Security Program, with a named individual responsible for its overall execution.** Discloser’s Information Security Program must have executive support, and be defined based on the characteristics of its business. It must include documented security plans, policies, and procedures designed to protect the confidentiality, integrity, and availability of its information assets. Discloser maintains staffing and technical resources at an appropriate level to ensure the Information Security Program’s plans, policies, procedures, ongoing operations, monitoring, and continuous improvement.
2. **Periodically conduct an Information Technology (IT) security risk assessment.** As part of the Information Security Program, Discloser periodically conducts an IT risk assessment to identify threats and vulnerabilities that may affect the systems that are used to complete the Purpose. Discloser prioritizes identified risks based on potential business impact and likelihood of occurrence. Discloser develops remediation plans for identified vulnerabilities, and prioritizes resources to implement remediation plans based on the prioritization of the associated risks. Risk assessment findings, remediation plans, and exceptions are reviewed and approved by Discloser’s senior management. Risk assessment is updated periodically on a regular cycle or after significant changes to the Discloser’s IT environment.
3. **Maintain formal documented instructions for reporting security breaches.** Discloser maintains documentation for reporting security breaches, and Discloser’s users are trained on the process. In the event of a security breach involving the Information, Discloser will notify the Duke’s Information Security Office in writing with a detailed description of the breach, actions taken, and an action plan to prevent future incidents.
4. **Assess and manage security risks associated with vendors and subcontractors.** Discloser maintains a documentation for assessing and managing information security risks associated with its vendors and subcontractors that have physical or logical access to Discloser’s IT systems and networks. As appropriate, required security requirements should be incorporated into contracts between Discloser and its vendors and subcontractors.
5. **Maintain employee on-boarding and off-boarding policies and procedures.** Ensure that new employees receive a level of screening appropriate for their roles, including, but not necessarily limited to, professional reference checks, and criminal background checks. Require that new employees complete security awareness training, which should include relevant information on HIPAA and the handling of PHI, within 30 days of their hire date. Upon employee termination, ensure that access to Discloser’s systems and networks (including remote access via VPN) is discontinued in a timely fashion, and any Discloser-issued IT assets (e.g. laptops, mobile phones, or portable storage media) are collected prior to the employee’s separation from the company. Discloser must ensure that terminated employees are not able to access systems or information related to the completion of the Purpose.
6. **Ensure continuing employee awareness of and education on security policies, standards, and procedures.** Discloser will provide formal security training to all employees and contract staff. Formal procedures and

scope of administrator's roles and security procedures are specified. All Discloser users will go through security training annually. Discloser maintains security policies, rules, procedures, and instructions for continued security awareness and education.

7. **Evaluate and install security patches in a timely fashion.** Discloser will maintain formally documented security patch management procedures. Discloser will evaluate, test, and install security patches based on a risk-based schedule prioritized by the Common Vulnerability Scoring System (CVSS) score, or a functionally equivalent approach. Security patches identified as a high priority, generally those that address vulnerabilities with a CVSS base score of 7.0 to 10.0, should be installed with 30 calendar days of release, including any system reboots that may be necessary to fully install the patch. Discloser will maintain a formal exception management process to review and address risks associated with high priority patches that cannot be installed during this window.
8. **Protect systems against self-propagating malware.** Endpoint security software is installed and maintained on all Discloser hardware workstations and servers. The software will be properly configured and maintained with an up to date scan engine and anti-virus definition files. Endpoint security software will be configured to periodically perform an automated full scan of the system, as well as to actively scan incoming and outgoing network traffic (e.g. through email or web browsing) for viruses.
9. **Use standardized secure build processes to harden servers, workstations, laptops, and other network devices against attack.** Discloser has policies and procedures in place for building all systems, including workstations, laptops, mobile devices, and network devices, in a manner that hardens them against attacks. Secure build procedures should disable or remove unnecessary network services, applications, and data from systems before placing them into production use.
10. **All storage of Duke Confidential Information on Discloser hardware or systems is prohibited.** If any storage of Duke's Confidential Information on Discloser hardware or systems is identified, Discloser will notify Duke and will use industry best practices, such as those outlined in NIST Special Publication 800-88, to remove Duke Confidential Information from all media types, including hard drives, portable storage devices, backup tapes, and paper files.
11. **Use of offshore service providers and/or data center facilities is prohibited unless approved in writing by Customer.** Duke reserves the right to terminate this Agreement if Discloser makes use of unapproved offshore service providers or data center facilities.
12. **Access Duke Network using Duke approved secure remote access.** Discloser agrees to only access Duke network using Duke provided solutions. All Discloser activities during remote access may be monitored by Duke. Discloser accounts will be registered in Duke vendor tracking tool.