Interconnection Security Agreement

Vanderbilt University Medical Center - All of Us Research Program Data and Research Center

and

University of Southern California - All of Us Research Program Health Provider Organization

All of Us Research Program
Interconnection Security Agreement

Vanderbilt University Medical Center - All of Us Research Program Data and Research Center (DRC)
and
University of Southern California - All of Us Research Program Health Provider Organization ("HPO")

This Interconnection Security Agreement ("Agreement") is made and entered into as of the date of the last signature affixed hereto (the "Effective Date") by and between Vanderbilt University Medical Center ("VUMC"), a Tennessee not-for-profit corporation, and University of Southern California ("USC"), a California not-for-profit corporation. Hereinafter VUMC and University of Southern California shall collectively be referred to as "Parties."

For the sake of clarity, all provisions of this agreement are binding provisions, including sections labeled "Background" and other sections that provide background and context to the Agreement.

All of Us Research Program

The purpose of this Agreement is to establish terms governing USC and VUMC regarding the development, management, operation, and security of a connection between systems owned by USC and the All Of Us Research Program Data and Research Center ("DRC") owned by Vanderbilt Institute of Clinical and Translational Research at VUMC.

VUMC is the recipient of that certain National Institutes of Health ("NIH") grant number 1U2COD023196-01 (as may further be revised or amended), entitled "Data and Research Support Center" (the "DRC Grant"), pursuant to which VUMC has established the All of Us Research Program Data and Research Center ("DRC"), an information security system that meets FISMA moderate standards under the Federal Information Security Management Act of 2002 ("FISMA").

USC is the recipient of that certain NIH grant number 1OT2OD024611-01 (as may further be revised or amended), entitled "Precision Medicine Initiative Cohort Program Healthcare Provider Organization Enrollment Centers" (the "HPO Grant"). In addition to USC, other Healthcare Provider Organizations (collectively, "HPOs") received this grant in other geographical regions.

In connection with the DRC Grant, VUMC, among other things: manages coordination and communication among all organizations participating in the All of Us Research Program ("Program") for the purpose of aggregating participant data; performs data integration across a wide variety of data types, including acquiring, integrating, and curating data; creates and hosts data access and analysis tools in a secure computing environment; and coordinates the collection of participant data, including health records, physical measurements, and other information from USC.

In connection with the HPO Grant, USC, as a member of the California Precision Medicine Consortium ("CaPMC"), facilitates recruitment and enrollment of volunteer participants and the collection of physical measurements and other data from such participants. To that end, USC may contract with enrollment sites that are separate legal entities from USC ("USC Enrollment Sites"). USC must assure that all applicable requirements of this Agreement apply contractually to USC Enrollment Sites, including requirements related to access, use, disclosure, and transfer of Data;

Interconnection Security Requirements; Security Considerations; and Communication (at those terms are defined herein).

The DRC, as a condition of the DRC Grant, must use Interconnection Security Agreements for data transferred between and among the DRC and the Program's participating organizations, including USC ("Data"), and shall require all participating organizations to execute Interconnection Security Agreements (or comparable agreements) before allowing access to Data (including data obtained from USC). The Data that will be transferred between and among USC, the DRC, and the Program's participating organizations may contain Personally Identifiable Information ("PII") and Research Health Information ("RHI"), collected with informed consent from participants. For purposes of this Agreement, PII and RHI are defined as follows:

- PII is information relating to an identified or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to such person's physical, physiological, mental, economic, cultural, or social identity.
- RHI is health data associated with a consented Program participant that relates to such participant's health, including the provision of healthcare to such participant or the payment of health care for such participant, and is acquired or collected specifically for the purposes of conducting research.

DRC shall use or disclose Data provided by USC as outlined in the DRC Grant, the HPO Grant, and All of Us Research Program protocols, in a manner that is consistent with applicable state and federal laws and regulations, including any informed consent requirements and the terms of the NIH funding.

SECTION 1 – BACKGROUND

The requirements for interconnection between USC and the DRC, owned by Vanderbilt Institute for Clinical and Translational Research at VUMC, are dictated by the Program. Pursuant to Program agreements, both HIPAA (the Health Insurance Portability and Accountability Act of 1996, as codified at 42 U.S.C. § 1320d, as amended, including all current and future regulations) and FISMA systems are acceptable and fall under the NIST Cyber Security Framework. Systems administrators and other appropriate staff (including authorized contractors) from both Parties will comply with appropriate security requirements to protect both Parties' data and information systems. The expected benefit of the interconnection is to expedite the processing of Program Data to meet prescribed timelines.

Entity 1: All of Us Research Program Data and Research Center (DRC)

The DRC system is a major application built to meet requirements of the Program. The DRC system will store Data associated with the Program gathered from multiple sources, as well as provide user applications to facilitate Data entry, provider operational work queue, and biobanking order workflow. Data stored in the DRC system will include information collected from multiple sources, including the Participant Technology Systems Center ("PTSC") website and apps, DRC applications, and direct Data transfer such as electronic health record ("EHR") Data shared by Program HPOs. Data may be collected from additional sources as appropriate to meet the needs of the Program.

The DRC system will provide two interfaces for USC staff as DRC system users, based on role:

Health Professional Portal ("HealthPro") is a DRC application that includes an interface for Program health professionals to perform participant lookup and Data entry during the physical evaluation and biobank process. HealthPro also facilitates health professional

operational work queue by providing to users a filterable list of their site's paired participants. This operational work queue may be either viewed within the HealthPro web application or downloaded as a .csv file. Dashboards also are available through the HealthPro application to select user roles. These Dashboards allow views of aggregate operational Data.

The DRC also provides for secure Data upload to and storage in the DRC's Raw Data Repository ("RDR"). Using an authenticated account associated with a specific site, Data files can be uploaded to an RDR storage bucket through the Google Cloud Software Development Kit ("SDK"). The upload mechanism is intended to facilitate transfer of Data from the HPO's EHR to the DRC.

Entity 2: University of Southern California
USC, as an HPO member of the CaPMC, is responsible for managing engagement, enrollment, and retention of participants into the Program, performing physical measurement collection, collecting biospecimens, and providing EHR Data. In these activities, USC key personnel and research staff funded by the Program will be users of the DRC system. These named personnel will access DRC applications or environment for data entry and retrieval for patients enrolled by USC. For patients that consent to release of EHR data from the USC Research Data Warehouse ("RDW") to the Program, data extracts derived from the USC RDW will be delivered to DRC in a format specified by the Program. Information systems management, support, and security for USC, including clinical, administrative, and research entities that include Keck School of Medicine, Keck Hospital, Norris Hospital, and Verdugo Hills Hospital, is provided by Keck Medicine Information Services.

SECTION 2 – INTERCONNECTION STATEMENT OF REQUIREMENTS
The requirement for interconnection between USC and VUMC is to facilitate the exchange of Data between USC and the DRC. USC requires the use of the DRC system at VUMC and VUMC requires the use of USC RDW data matched to Program participants to expedite the processing of participant Data associated with the Program and to meet timelines.

SECTION 3 – SECURITY CONSIDERATIONS

The DRC system is hosted in Google Cloud Platform, which provides highly available and redundant systems for the DRC environment. The Google App Engine component is leveraged for hosting the HealthPro application and has been assessed by a third party to meet FedRAMP compliance (see Google Services FedRAMP authorization information at https://marketplace.fedramp.gov/#/product/google-services?sort=productName). The DRC system enforces two-factor authentication and the encryption of sensitive data at rest and in transit. The API interfaces will leverage Google Service Accounts for authorizing access for services and applications. The DRC system has undergone a formal security assessment process to meet NIST 800-53 Rev 4 security controls at the FISMA Moderate level, and performs regular vulnerability testing and application penetration testing. Further documentation of the security measures is included in the DRC System Security Plan (SSP).

Keck Medicine of USC secures its network perimeter through firewalls and other detection and protection tools that monitor external network traffic and block potential threats. Examples of these tools include endpoint protections (anti-virus), web security gateway (proxy & filtering), email scrubbing, and intrusion prevention. Data from these tools, as well as the tools described in subsequent sections of this Agreement, are sent to Keck Medicine of USC's outsourced security

information and event management system and security operations center, which provides 24/7 monitoring and analysis of potential threats and alerts the Keck IT team in real-time.

Since 2013, Keck Medicine of USC has engaged a third party Managed Security Services Provider (MSSP), Proficio, that receives audit logs from firewalls, critical systems, servers and other sources and monitors 24/7 for potential security incidents. Proficio follows a "Runbook" that prescribes the appropriate response to various events. Keck IT and Proficio representatives meet every other week to review the status of these items.

a. General Information

HealthPro:
The DRC system will provide authorized USC users of the DRC system access to HealthPro. Authorized USC staff will utilize HealthPro to facilitate the physical measurement collection process, which includes viewing sufficient PII to verify participant identity, performing data entry from participant's physical measurement collection, and completing the biospecimen ordering workflow. Additionally, authorized USC staff will be able to utilize HealthPro's Participant Work Queue, a filterable list of its paired participants containing operationally relevant data to inform local recruitment and enrollment processes. Data from the Participant Work Queue, which contains limited PII, may be either viewed within the HealthPro application or downloaded as a .csv file. Data downloaded from the HealthPro application must be treated according to the USC's process for handling PII and RHI pursuant to applicable state and federal law, including HIPAA and the Common Rule. Further, in accordance with the Rules of Behavior and Acceptable Use Policy, data downloaded from HealthPro must not be stored on portable media or personal devices.

Captured Biobank process data includes information about the types and time of biospecimen collected, in addition to the types and times of subsequent biospecimen processing and finalization for shipment to the Biobank, operated by the Mayo Clinic. HealthPro will create Biobank orders in the Mayo Clinic system and fetch appropriate files for biospecimen tubes and shipping manifests. Biospecimen order labels and manifests are intended for printing, specimen labeling, and specimen shipment, and do not contain PII.

Dashboards:
The DRC system also will support a Dashboard for operational and administrative use by authorized personnel. The user pool for this feature may be different from the user pool accessing HealthPro to collect physical measurements and track participants. Dashboards are a tool for site leadership, so not every person who has access to the HealthPro interface will have access to the Dashboards. Dashboard users will be able to view aggregated Data, including participant count in various stages of the research pipeline. Counts can also be shown as separate totals of individuals in various categories, including: race and ethnicity, gender, age, location (state, census region) and possibly other demographic variables.

EHR:
The DRC will support the collection of consented RHI, including EHR Data supplied directly from the USC RDW. USC will share with the DRC EHR Data for participants recruited at the CaPMC HPO member sites. The Data will consist of RHI and PII, and may include demographics, visits, clinical observations, measurements (e.g., laboratory), medications, various ancillary reports (e.g., cardiology, radiology), physician notes, and other clinical data.

RDW Data that is uploaded to the DRC will be stored in the RDR in its originally transmitted form. As with all Data held within the DRC, RDW Data also will be processed, curated, and exposed in a

Curated Data Repository that will be made available to qualified researchers and citizen scientists according to All of Us Research Program policy and participant consent. Some Data derived from transferred RDW data will be made available to the participant to whom the Data refers via the PTSC app and website to provide transparency and value to participants.

b. Services Offered

The DRC has created the HealthPro portal that will be used by authorized, authenticated users in the Program to enter Data collected during the physical measurements, create Biobank orders for biospecimen, and access operationally relevant participant Data. Additionally, authorized, authenticated users may access operational Dashboards through the HealthPro portal. These Dashboards are view-only and contain aggregate Data.

The DRC also supports the collection of consented RHI, including but not limited to RDW Data supplied directly from HPOs. The Data transfer will occur through secure Data upload to the DRC's RDR. The secure upload will require an authorized account associated with a specific HPO, with Data file upload facilitated by the Google Cloud SDK.

Each member of the CaPMC, including USC, will prepare research data (including EHR data), which it will send to DRC. All exchange of Data with the DRC will use secure transfer methods specific to the DRC.

c. Data Sensitivity

Data points and interactions between the DRC and authorized USC staff contain PII and RHI and should be treated as highly confidential information. PII and RHI Data within DRC systems will be accessible only to authorized and authenticated user accounts. Data download from HealthPro is restricted to operationally relevant Data associated with a HPO's paired participants. Any Data downloaded from the HealthPro application must be treated according to the HPO's process for handling sensitive information. Biobank order information, which does not include PII, is the only Data shared with the Mayo Clinic Biobank.

Data received by the DRC via direct upload from participants, Data transfer from HPOs (e.g., USC RDW), or Data transfer from other authorized systems will contain PII and RHI. These Data are transferred through secure Data upload to the DRC system for storage.

d. Access Control

DRC:
The DRC system access control and authorization is centrally managed through Google Access and Identity Solution provided by Google App Engine. Authorization to specific functionality within the DRC is managed through roles. All actors calling HPO-DRC APIs use user-managed service accounts.

The DRC system enforces strong access control, separation of duties, credential management and account review/access revoke to offer a secure and stable operational environment. Implementation details for Access ("AC") and Identification & Authorization ("IA") controls are documented in the SSP.

USC:
The USC will authorize access on the basis of role-based All of Us personnel status. All accounts and access are managed in a way that is consistent with USC IS Policy ISPOL-2004 and ISPOL-3010. Keck Portal is a Citrix virtualization gateway which is hosted and integrated with the entire

security framework using AD for authorization while following policy driven provisioning of users; without properly provisioned user access, navigation in and throughout the USC network is blocked.

ISPOL-3010 - Access controls minimize exposure to Keck Medicine of USC resulting from unauthorized use of resources and to preserve and protect the confidentiality, integrity, and availability of the networks, systems, applications, and data. Authorization of access is provided through provisioning practices requiring senior level and direct management review of documented authorization. Access control is safe if no permission can be leaked to an unauthorized or uninvited principal with levels of control applied; levels of control are

- Zero Access –no access by default,
- Unique Access – Access requires the use of a unique user identifier in conjunction with an associated authenticator,
- Least Privilege - Only minimum access necessary to perform an operation,
- Separation of Duties – Functions and capabilities are separate and provide as much granularity as possible,
- Role-Based Access– "separation of duties" is the principle of role-based access defined to allow the subject (i.e. user) access to an object (i.e. data) where roles are created for job functions of specific roles, and
- Authorized Access.

Access is revoked based on removal criteria ranging from management request to breach of policy and variations of both.

e. User Community

DRC personnel are authorized for access based on the least privilege for their role. Personnel are subject to background checks, undergo mandatory security training, and must agree to Rules of Behavior for the DRC environment, for privileged users, or Acceptable Use Policy, for non-privileged users, prior to access. See DRC Rules of Behavior for Privileged Users, available at: https://docs.google.com/document/d/1E6bRJ4I7AclEkaFS4Tg2zt9u3WyFMOpu4-omMjhITRM/edit?usp=sharing,
and DRC Acceptable Use Policy for Non-Privileged Users, available at https://docs.google.com/document/d/1p136gslEMcf9A8mFZ3ALtgDXltybYVtJvGahW-JJyew/edit?usp=sharing.

VUMC personnel with access to DRC applications or environment shall be required to complete background screening consistent with VUMC policy, local laws and standards, and human subject/ethics in research and privacy training prior to accessing DRC applications or environment.

The information recipients from the DRC include DRC System Administrators, Developers, Operational Administrators, Project Managers, and other authorized staff. Security Analysts and Auditors will access information contained within audit logs. Select Data will be shared with the PTSC and with participants themselves through the PTSC's website and apps. Aggregate Data views will be available to DRC, HPO, and Program leadership. To support the research purpose of the Program, curated Data will be available to approved researchers as appropriate for their authorization.

USC is responsible for identifying personnel to fill the "Site Admin" role. This role is responsible for authorizing USC personnel access to the DRC environment. This includes identifying the required level of access for each individual, ensuring background checks are performed to appropriate level according to system access, submitting and managing signed Rules of Behavior (for privileged

users) or Acceptable Use Policy (for non-privileged users) forms, and ensuring that all necessary security training is completed. More than one individual can be identified as "Site Admin" to provide backup coverage.

Per USC Policy ISPOL-3010, access controls minimize exposure to Keck Medicine of USC by establishing common community of users solely bound by their authorization credentials and provisioning as defined by policy based approvals.

The information recipients from USC include research coordinators, operational and systems administrators, USC leadership, and other authorized staff. All USC personnel associated with the Program with access to DRC applications or environment shall be required to complete background screening consistent with USC policy, local laws and standards, and human subject/ethics in research and privacy training prior to accessing DRC applications or environment. USC personnel are authorized for Data based on the least privilege for their role.

f. Information Exchange Security

To secure the information exchange from USC to the DRC back-end components, DRC encrypts all Data during transport using HTTPS (port 443). The DRC leverages encryption from service providers, including the Web Application Firewall (WAF) provider, which enforces encryption for all inbound (public) traffic, and Google App Engine; which also encrypts traffic between the WAF and Google App Engine services.

USC secures its endpoints by using an automated patch management system for all workstations, laptops, and servers. The patch management lifecycle is done on a monthly basis after new updates are released. A test group of workstations is employed in order to validate interoperability with other applications.

g. Federal Security Policy and Standards

The DRC adheres to the VUMC Security Policies and Standards as are reflected in the VUMC Information Security Policy and VUMC IT Standards. All relevant personnel, operational and technical artifacts are governed through the aforementioned. This interconnection must comply with these policies and standards. The policies encompass the FISMA guidelines provided in NIST 800-53 Rev 4 and other relevant publications.

CaPMC members, including USC, adhere to their institution-specific policies and standards for information security. These policies are derived from HIPAA Privacy and Security regulations and cover all handling and transmission of ePHI data.

Both the DRC and USC shall adhere to: (a) the White House's *Data Security Policy Principles*, which include the four principles of authentication, authorization, audit, and encryption; (b) the *PMI Privacy and Trust Principles*; (c) the Common Rule and the relevant privacy and security standards under HIPAA, as applicable. Moreover, both the DRC and USC shall obtain NIH Certificates of Confidentiality to protect Program Participants from having their information disclosed in response to legal proceedings and demands.

h. Incident Reporting

USC or VUMC, upon discovering a security incident involving the interconnection, shall report such incident in accordance with agency-specific incident reporting procedures and shall expeditiously notify USC's Incident Response Team at (323) 442-4444 or by email at loor@med.usc.edu and the

VUMC Incident Response Team ("IRT") at security@pmi-ops.org. VUMC will notify the NIH within one (1) hour of detection of an incident by contacting the NIH IRT at 301.881.9726 or by email at NIHInfoSec@nih.gov.

USC technical staff shall immediately notify the designated VUMC counterpart by telephone or e-mail when a security incident(s) is detected, so that the counterpart may take steps to determine whether the VUMC system has been compromised and to take appropriate action. The VUMC technical staff shall promptly notify its Computer Security Incident Response Center (CSIRC), the VUMC IRT, of the incident.

VUMC incident response policy is reflected in the *VUMC All of Us Research Program Incident Response Plan.*

USC incident response policy is reflected in *ISPOL-2017 - Incident Response Team.*

i. Audit Trail Responsibilities

As documented in the DRC SSP, VUMC uses Stackdriver and BigQuery to capture and correlate all audit logs from components within the DRC system, including this connection. Events from all components in the boundary captured by the log server include:

- Successful and unsuccessful account logon events
- Account management events
- Object access
- Policy change
- Privilege functions
- Process tracking
- System events

Since 2013, Keck Medicine of USC has engaged a third party Managed Security Services Provider (MSSP) that receives audit logs from Active Directory, firewalls, critical systems, servers and other sources and monitors 24/7 for potential security incidents. These audits minimally include basic authentication activity (e.g., user logon, logoff, failed authentication attempts), account management events, and system events. Proficio follows a "Runbook" that prescribes the appropriate response to various events. Keck IT and Proficio representatives meet every other week to review the status of these items.

j. Training and Awareness

Security awareness training is provided to VUMC personnel as a part of initial training for new users. This training must be completed prior to gaining access to the system or performing assigned duties, which include administering the system. Personnel are required to undergo annual refresher training to ensure that they are aware of security responsibilities and current threats. Additionally, for DRC, VUMC leverages role-based training for executives, management, and IT Administrators.

Security awareness training is provided to USC personnel as a part of initial training for new users. This training must be completed prior to gaining access to the system or performing assigned duties, which include administering the system. Personnel are required to undergo a Systems Security Awareness annual refresher training to ensure that they are aware of security responsibilities and current threats.

All USC staff are trained according to roles described in ISPOL-3010; all USC All of Us personnel are also certified in HIPAA and Human Subjects Research.

k. Breach Notification

Privacy Breach

A breach is any successful compromise at any level of protective controls to, or unauthorized access to or use of, systems or Data. An attempt, successful or unsuccessful, is an incident, making a breach a subset of incidents.

USC Notification Obligations

USC agrees to notify the VUMC IRT within one (1) hour of any use or disclosure of PII or RHI by USC not permitted by this Agreement, any security incident, and any breach of unsecured PII or RHI of which USC becomes aware.

USC shall provide the following information to VUMC within ten (10) business days of discovery of a breach of unsecured PII or RHI except when, despite all reasonable efforts by USC to obtain the information required, circumstances beyond the control of the USC necessitate additional time. Under such circumstances the USC shall provide to VUMC the following information as soon as possible and without unreasonable delay, but in no event later than thirty (30) calendar days from the date of discovery of a breach:

a. The date of the breach.

b. The date of the discovery of the breach;

c. A description of the types of unsecured PII or RHI that were involved;

d. Identification of each individual whose unsecured RHI has been, or is reasonably believed to have been, accessed, acquired, or disclosed; and

e. Any other details necessary to complete a risk assessment in accordance with the Program requirements.

The DRC Security Team or VUMC-IRT will notify key members of VUMC DRC development, ISSO, data owners, support, operations, Security Operations Center ("SOC") and other departments as needed to investigate, contain, and resolve the incident. Once the occurrence of an incident is verified, the DRC Security Team or VUMC-IRT will simultaneously notify NIH-IRT within one (1) hour of verification at IRT@nih.gov or 301-881-9726 (24 x 7).

VUMC Notification Obligations

To the extent Data maintained within the DRC is breached, the Program's Breach Notification requirements, which currently are being developed by the NIH in partnership with Program leadership and VUMC on behalf of the DRC, will dictate the process for breach notification to the affected HPOs and Program Participants.

l. Security Documentation

The following information technology security documents set forth the procedures and requirements for the protection of Data transmitted pursuant to this Agreement:

VUMC/All of Us Research Program DRC

- All of Us RP DRC User Policy and Procedures
- All of Us DRC IT Rules of Behavior for Privileged Use

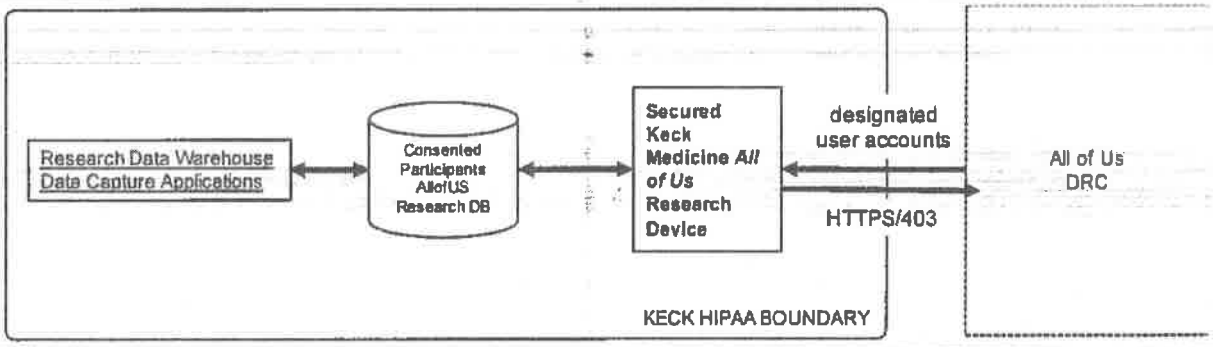
- All of Us DRC IT Acceptable Use Policy – Non Privileged User
- All of Us DRC SSP 800-53 Rev4
- VUMC All of Us DRC SDLC
- DRC-Configuration Management Plan

USC Information Security Policies

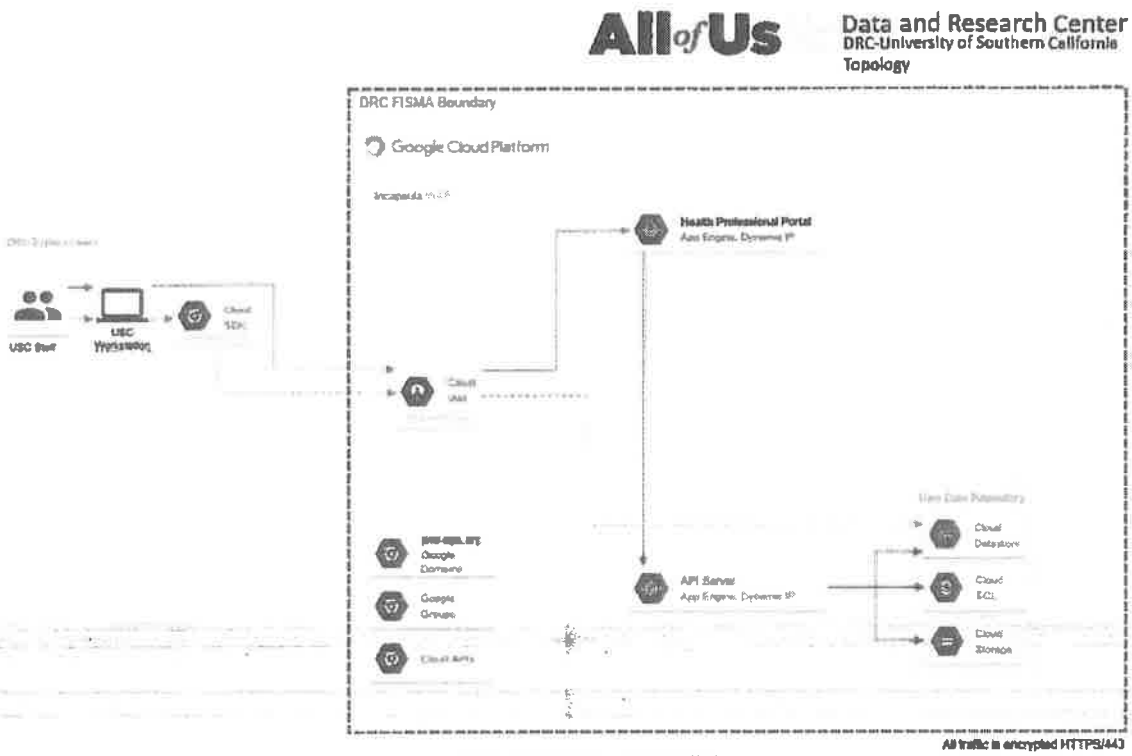
- ISPOL-3010 Access Control Policy
- ISPOL-1002 – Backup and Recovery Standards
- ISPOL-2004 – Password Security
- ISPOL-2017 - Incident Response Team
- RES-301 - Uses and Disclosures of Protected Health Information for Research Purposes
- HIPAA Privacy Rule Clin-206: Minimum Security Standards for Electronic Protected Health Information for Keck Medicine

SECTION 4 - TOPOLOGICAL DRAWING

The following diagrams illustrate all communication paths, circuits, and other components used for the interconnection.



FOR OFFICIAL USE ONLY



FOR OFFICIAL USE ONLY

SECTION 5 – COMMUNICATION

Frequent formal communications are essential to ensure the successful management and operation of the interconnection. The Parties agree to maintain open lines of communication between designated staff at both the managerial and technical levels. All communications described herein must be conducted in writing unless otherwise noted.

USC and the DRC agree to designate and provide contact information for technical leads for their respective system and to facilitate direct contacts between technical leads to support the management and operation of the interconnection. See Exhibit B-1 (VUMC POCs) and Exhibit B-2. (USC POCs). To safeguard the confidentiality, integrity, and availability of the connected systems and the Data they store, process, and transmit, the Parties agree to provide notice of specific events within the time frames indicated below:

Security Incidents: The technical staffs will immediately notify their designated counterpart by telephone or e-mail when a security incident(s) is detected, in order to determine whether their system has been compromised and take appropriate security precautions. In addition, the technical staffs will notify their respective Incident Response Centers or points of contact to ensure that appropriate actions and reporting takes place. The VUMC-IRT should be notified by email to security@pmi-ops.org. The Incident Reporting section defines additional detail and reporting requirements.

Disasters and Other Contingencies: The technical staff will immediately notify their designated counterpart by telephone or e-mail in the event of a disaster or other contingency that disrupts the normal operation of one or both of the connected systems.

Material Changes to System Configuration: Planned technical changes to the system architecture will be reported to technical staff within a week before such changes are implemented. The initiating party agrees to conduct a risk assessment based on the new system architecture and to modify and re-sign the ISA within one (1) month of implementation.

New Interconnections: USC will notify VUMC at least one (1) month *before* it connects the system that is related to this interconnection with any system that is not directly related to this interconnection, including systems that are owned and operated by third parties.

SECTION 6 – TIMELINE AND SIGNATORY AUTHORITY

The provisions of this Agreement shall be effective as of the Effective Date and shall terminate (a) upon the end of Program operations, or (b) if either Party should cease operations, or (c) when all of the Data is destroyed or returned to DRC. The Parties agree to review the security controls described in this Agreement at least annually or whenever a significant change occurs. To the extent the technology described in this Agreement materially changes, the Parties agree to amend this Agreement accordingly.

SECTION 7- MISCELLANEOUS

This Agreement grants no copyright, trademark, trade secret or patent rights or licenses, express or implied.

This Agreement may be executed in any number of counterparts, each of which shall be an original and all of which together shall be one document binding on all the parties even though each of the parties may have signed different counterparts.

This Agreement together with all attachments and exhibits represents the entire understanding of the parties with respect to the subject matter hereof. In the event of any inconsistency between this Agreement and the parties' understandings, the terms of this Agreement shall govern.

[Signature page follows]

IN WITNESS WHEREOF, the parties have executed this Agreement effective upon the date of the last signature affixed hereto.

APPROVED BY:

Vanderbilt University Medical Center

Print Name: ~~Libby D. Salberg~~
Title: Director
Office of Contracts Management
Date: 7/14/17

University of Southern California

Print Name: Mark K. Todd
~~Vice Provost for~~
Academic Operations
Title:
Date: June 22, 2017

READ AND ACKNOWLEDGED BY:

ALL OF US RESEARCH PROGRAM DATA RESEARCH CENTER PRINCIPAL INVESTIGATOR

Print Name: Joshua Denny, MD, MS
Professor, Biomedical Informatics and Medicine
Title: Dir. Center for Predision Medicine
Date: 7/12/2017

UNIVERSITY OF SOUTHERN CALIFORNIA

PRINCIPAL INVESTIGATOR

Print Name: Daniella Meeker
Title: Assistant Professor
Date: 5/10/21017

Exhibit B-1. VUMC Points of Contact

Vanderbilt University Medical Center Points of Contact:

System Owner Josh Denny, MD, MS Professor of Biomedical Informatics and Medicine, Director, Center for Precision Medicine Vice President for Personalized Medicine Vanderbilt University Medical Center 2525 West End Ave, Nashville, TN 37203 Josh.denny@vanderbilt.edu	**Senior Technical Advisor** Paul Harris, PhD Professor of Biomedical Informatics Research Professor of Biomedical Engineering 2525 West End Ave, Nashville, TN 37203 Paul.a.harris@vanderbilt.edu
IT Security Program Bill Schultz Principal Security Architect 3401 West End Ave. 530, Nashville, TN 37203 (615) 936-3401 Bill.schultz@vanderbilt.edu	**Technical POC** Sarah Tahiri Senior IT Project Manager 2525 West End Ave. 1430, Nashville, TN 37203 (615) 936-6246 sarah.w.tahiri@vanderbilt.edu
Contingency Planning Ross Davis Application Developer Manager 2525 West End Ave. 1430, Nashville, TN 37203 Ross.davis@vanderbilt.edu	**Incident Response** VUIT Incident Response All of Us Research Program DRC Security Team security@pmi-ops.org

Exhibit B-2. USC Points of Contact

USC Points of Contact:

IT Security Program David Loor Data Security Officer (IT Director – Security) 2011 N. Soto, Los Angeles, CA 90032 (323) 442-2455 Loor@med.usc.edu	**Technical POC** Sean Updegrove Chief Technology Officer 2011 N. Soto, Los Angeles, CA 90032 (323) 865-7737 Sean.Updegrove@med.usc.edu
Contingency Planning David Loor Data Security Officer (IT Director – Security) 2011 N. Soto, Los Angeles, CA 90032 (323) 442-2455 Loor@med.usc.edu	**Incident Response** David Loor Data Security Officer (IT Director – Security) 2011 N. Soto, Los Angeles, CA 90032 (323) 442-2455 Loor@med.usc.edu