ARKANSAS HEALTHCARE TRANSPARENCY INITIATIVE
DATA MANAGEMENT PLAN

CONTACT INFORMATION

Project Title: An Evaluation of Value-Based Payment Reform in Arkansas

Date: January 17, 2017

Organization: Department of Health Care Policy, Harvard Medical School

Phone Number: 617-432-3333

Mailing Address: 180 Longwood Ave.

City: Boston State: MA ZIP Code: 02115

Person responsible for privacy and/or security: Caroline Wood

Email: wood@hcp.med.harvard.edu

Phone Number: 617-432-1294

INSTRUCTIONS

Use the following sections to develop your Data Management Plan. You may include attachments where necessary. Cleary identify the attachment in the corresponding section.

I. DATA MANAGEMENT POLICIES AND PROCEDURES

Attach copies of any data privacy and security policies and procedures for the requesting organization and collaborating organizations who will have access to Initiative data.

II. PHYSICAL POSSESSION AND STORAGE OF DATA FILES

- Who will have the main responsibility for organizing, storing, and archiving the data? Please provide name(s) and job title(s).
- Describe how your organization will maintain an inventory of Initiative data files and manage physical access to them for the duration of the project.
- Describe how your organization binds all members (i.e., organizations, individual staff) to specific privacy and security rules in using Initiative data files. This includes confidentiality agreements and non-disclosure agreements.
- Provide details about how your organization will notify the Arkansas Center for Health Improvement (ACHI) of any project staffing changes.
- Describe your organization's training programs that are used to educate staff on how to protect Initiative data files.

- Explain the infrastructure (facilities, hardware, software, and other) that will access the Initiative data files.
- Describe the policies and procedures regarding access to Initiative data files.

- Explain your organization's system or process to track the status and roles of the project team.

- Describe your organization's physical and technical safeguards used to protect Initiative data files, including actions taken to physically secure data files and safeguards to limit access to Initiative data and analytical extracts among the project team.

III. DATA SHARING, ELECTRONIC TRANSMISSION, DISTRIBUTION

- Describe your organization's policies and procedures regarding the sharing, transmission, and distribution of Initiative data files.

- If your organization employs a data tracking system, please describe.

- Describe the policies and procedures your organization has developed for the physical removal, transport, and transmission of Initiative data files.

- Explain how your organization will tailor and restrict data access privileges based on an individual's role on the project team.

- Explain the use of technical safeguards for data access (which may include password protocols, log-on/log-off protocols, session time out protocols, and encryption for data in motion and data at rest).

- Are additional organizations involved in analyzing the data files provided by ACHI?

  If so, please indicate how these organizations' analysts will access the data files:
  __ VPN connection
  __ Travel to physical location of data files at requesting organization
  __ Request that a copy of the data files be housed at second location
  __ Other:

- If an additional copy of the data will be housed in a separate location, please describe how the data will be transferred to this location.

IV. DATA REPORTING AND PUBLICATION

- Who will have the main responsibility for notifying ACHI of any suspected incidents wherein the security and privacy of the Initiative Data may have been compromised?

ARKANSAS HEALTHCARE TRANSPARENCY INITIATIVE
DATA MANAGEMENT PLAN

- Please describe and identify your organization's policies and procedures for responding to potential breaches in the security and privacy of the Initiative Data.
- Explain how your organization's data management plans are reviewed and approved.
- Explain whether and how your organization's data management plans are updated during the Data Use Agreement (DUA) period.
- Please attest to the ACHI cell suppression policy of not publishing or presenting tables with cell sizes with less than 11 observations to anyone who is not an authorized user of the Data.

CEW I agree. (Initial)

V. COMPLETION OF RESEARCH TASKS AND DATA DESTRUCTION

- Your organization must ensure that it has policies and procedures in place to destroy Initiative Data upon completion of the project and that you have safeguards to ensure the data are protected when members terminate their participation in the project. Describe the policies and procedures in place to destroy the Data Files upon completion of the project.

VI. ASSURANCES

Data Recipients must notify ACHI, as soon as practicable, of any unauthorized use or disclosure of Initiative data.

The undersigned agrees that the Requestor and any collaborating organizations will adhere to the Data Management Plan described herein and will notify ACHI of any material changes in data management pertaining to the approved project.

Signature of Duly Authorized Representative: Caroline E. Wood

Printed Name: Caroline Wood

Title: Manager of Data Security and Compliance

Original Data Management Plan Submission Date: January 18, 2017

Revision Data Management Plan Submission Date _____

Edited: 1/18/17

Arkansas APCD Data Management Plan
Department of Health Care Policy, Harvard Medical School

I. DATA MANAGEMENT POLICIES AND PROCEDURES

Please see the below-outlined data management plan for all relevant data privacy and security policies and procedures for the Department of Health Care Policy, Harvard Medical School.

II. PHYSICAL POSSESSION AND STORAGE OF DATA FILES

- Who will have the main responsibility for organizing, storing, and archiving the data? Please provide name(s) and job title(s).

When physical media are received by the Data Custodian (Dr. Chen), they are immediately turned over to the Systems Operation Manager (Young Sul). The Systems Operation Manager will load the data onto the Department of Health Care Policy's server unless otherwise required by the terms of the data use agreement. After data are transferred to HCP systems, physical media containing raw data are labeled by PI, project and ADAMS record number and secured in the Data Center safe which is located in a locked office in a locked suite (Data Center IT Suite) with restricted, key-card access. The Data Custodian will be allowed access to data on the secure server and he will be responsible for organizing the files. Arkansas APCD data will not be archived. HCP data recipient will return or destroy APCD data pursuant to terms of the Arkansas APCD Data Use Agreement.

- Describe how your organization will maintain an inventory of Initiative data files and manage physical access to them for the duration of the project.

The Department of Health Care Policy uses the Acquired Data Accountability and Management System (ADAMS) database to maintain an inventory of all acquired datasets and their associated terms of use. ADAMS houses an electronic record of each DUA held by researchers at HCP and links it with the associated research protocol (IRB). ADAMS is a fully searchable database that captures critical project and data use information including the file location of all data stored on HCP's servers and computers. All records in ADAMS are vetted by the Department of Health Care Policy's Compliance Office, specifically by HCP Data Compliance Officer Ayan Elmi and Caroline Wood. HCP Data Custodians use best practices of a Pragmatic Data Security Cycle (define –discover –secure –monitor –protect –discover –destroy) to ensure that all project data are well inventoried on a project level and no source data are kept at the expiration of the agreement.

- Describe how your organization binds all members (i.e., organizations, individual staff) to specific privacy and security rules in using Initiative data files. This includes confidentiality agreements and non-disclosure agreements.

All members of HCP are educated in data security, privacy and confidentiality upon initial entrance into the department, and again multiple times each year. Members sign an acknowledgement form upon completion of this training. Access to data is controlled by Unix file permissions which are set by IT. These permissions are allowed by IT only when the Department Compliance Officer has confirmed an individual has completed department-required training and any other specific training required by the data vendor. This information, including additional training requirements and associated documentation such as individual confidentiality or non-disclosure agreements, are captured in the ADAMS database. All data use must comply with IRB human subjects regulations and adhere to Harvard security and privacy requirements and policies (http://security.harvard.edu). Further, Harvard University requires all staff to sign a blanket confidentiality agreement that is renewed on an annual basis.

- Provide details about how your organization will notify the Arkansas Center for Health Improvement (ACHI) of any project staffing changes.

The Project PI (Dr. Chernew) will notify ACHI via email of any project staffing changes (additions or removals). The PI will also notify the HCP Compliance Office and Harvard Institutional Review Board of these changes. Staff added to a project will not be provided access to data until all Departments and ACHI requirements have been met and approval secured. Staff removed from a project will have their access to data terminated.

- Describe your organization's training programs that are used to educate staff on how to protect Initiative data files.

Staff involved in human subjects research are required by Harvard Medical School's Institutional Review Board to complete human subjects training, specifically offered by the Collaborative Institutional Training Initiative (CITI), available: https://www.citiprogram.org. This training must be renewed every 3 years. At a department level, the Department of Health Care Policy requires new employees, regardless of whether or not they will have direct involvement in human subjects research, to complete the CITI human subjects training. Department personnel are also required to complete a Department-specific data security training which includes department-specific information and an overview of privacy and confidentiality. At the completion of the training, staff members sign an acknowledgement of completion. HCP also offers refresher training at various points throughout the year.

- Explain the infrastructure (facilities, hardware, software, and other) that will access the Initiative data files.

Restricted Access Facility: APCD data files will be stored in the Department of Health Care Policy Data Center, located in the HCP IT Suite at 180 Longwood Avenue, Boston, MA 02115. 180 Longwood Avenue is a secure building accessible only to those with a Harvard University ID card. Visitors obtain access via an intercom system from any of the exterior doors. Visitors are verified through the intercom by the security control center or the HCP receptionist. The Harvard Medical School (HMS) Security Department, including its 24/7 Security Command Center is headquartered on the lower level of 180

Longwood, as is the HMS Facilities Group Call Center: the group's central monitoring station for HVAC and other critical systems. Therefore the organizations most directly responsible for physical protection, support, and incident response are situated in close proximity to the HCP Data Center and are well-positioned to respond should critical situations arise. Entrance to the building is captured by video cameras which are monitored by the HMS Security Command Center. In addition, there is a fixed-position closed-circuit television camera located in the "horse tunnel" driveway/ walkway that connects Longwood Avenue with the 180 Building's courtyard area. Security footage is maintained for a minimum of 20 days. All restricted access areas are clearly marked. All third party visitors, including but not limited to vendors, contractors, service delivery personnel, etc., are notified of these restricted access areas. The HCP IT suite (001) and the IT server room (031) are restricted to key-card access only. IT personnel are the only personnel allowed access without escort. This access is logged electronically and can be reviewed by HMS Security or HUPD. Logs are maintained for a minimum of 6 months. HCP Management may request access to the logs for special review. In the case of building emergencies, Security and Facilities have access to all areas of the building. Any access of restricted areas must be accompanied by an HMS Security Officer and captured in an incident report. The HCP Facilities Coordinator is notified of the access and the purpose of the access. The HCP Facilities Coordinator will notify the appropriate team that the access occurred.

Computing Resources: The department's shared computing resources consist of a mix Unix, Linux, and Windows servers that support approximately 30 networked printers and 150 Windows and Macintosh desktop workstations. Desktop systems connect to departmental and university computing facilities and the Internet via switched Ethernet cable and fiber networks. An additional firewall filters access to and from the Medical School network and the Internet.

Wireless access (WiFi) connects to the Medical School network, but not to HCP's departmental network or files. Through the Medical School network, there is access to e-Commons, the Medical School's link to PubMed and other national databases, and the Internet.

Data Storage: The department's Unix data storage employs either disk mirroring or RAID 5 configurations for fault tolerance and data security. This is implemented in hardware where the equipment provides the capability, or in software. Off-line tape storage is used mainly for backup/recovery and for archival purposes. A networked backup system (Symantec NetBackup) manages an incremental daily backup of the data stored on Unix servers, and periodic full backups. Windows Network Drives, which are implemented on Unix systems using Samba file services, are included. Tapes that hold project data are encrypted. Regularly scheduled backups are solely for data recovery and disaster backup purposes, not archival purposes. Most backup tapes are recycled after four months, in compliance with our most stringent DUAs. Backup tapes for some specific projects are retained for 12 months before recycling. Archive tapes for specific projects can be created on request of the project leader, as data use agreements allow.

Data transfer capabilities: Data can be submitted to HCP on physical media such as tape or disk, or via secure electronic file transfer. Formats for physical media include tape SDLT II cartridges, optical disk (CD, DVD), and USB storage devices. A secure SSL enabled web transfer application from Accellion Inc. is available, as well as email or email attachments (10 MB limit), and SFTP (secure FTP). If necessary, data can be further secured with file encryption such as PGP.

End-User Software: Statistical software in the Unix environment includes SAS with Interactive Matrix Language and Graphics Modules, Matlab, Stata, Sudaan, BMDP, SPSS-X, S-Plus, R, and Systat. The department has some Windows licenses for SAS, SPSS, STATA and S-Plus, but the majority of researchers use the Unix versions.

Compilers for general purpose programming languages include FORTRAN, C (plus IMSL numerical library for C), C++, and Java. Both Sun and GNU versions of C and C++ are available. All Windows users have the Microsoft Office desktop productivity suite and Adobe Reader. Endnote, Adobe Acrobat and Photoshop are available for those who need it. Other Windows software is available, but not in widespread use. Most people use Microsoft Outlook for email, connecting to a Microsoft Exchange server managed by the Medical School IT department. Some users choose to access mail with a Unix mail utility such as Pine or DTMail. Windows workstations connect to Unix systems with Hummingbird Exceed or VNC for graphical X-Windows sessions, and SSH (Secure Shell) for text sessions.

Network access and network security: Unix and Windows servers are connected with a 100/1000MB switched router. The departmental network is a local 10/100MB-switched Ethernet network with wired connections only. There is no WiFi access to the departmental network. The departmental network is isolated from the rest of the Medical School and the Internet by its own router and firewall and is located on its own VLAN. Unencrypted inbound telnet sessions, (not using SSH) are blocked at the firewall. Remote access over the Internet (including access from the Medical School wireless network) is only available with encrypted communications methods like SSH and VPN (Virtual Private Network) software.

- Describe the policies and procedures regarding access to Initiative data files.

Department recipients of physical media are required to surrender media to the Data Center Systems Operation Manager(s), Young Sul or Kenny Lau. The Systems Operation Manager will load data to the Department server unless required otherwise by the data use agreement. After data are transferred to HCP systems, physical media containing raw data are labeled by PI, Project and ADAMS record number. Physical media are secured in the Data Center safe which is located in a locked office in the Data Center IT Suite, which is restricted by key-card access. Access to this Suite is always logged by security.

- Explain your organization's system or process to track the status and roles of the project team.

Prior to the commencement of any research activities, Harvard Medical School's Institutional Review Board will review a study protocol to determine whether human subjects are involved in the research and the extent to which they will require review of a study throughout its duration. Staff directly involved with human subjects or sensitive research data are listed on the IRB protocol. Under the direction of the PI, the project coordinator (Emily Corcoran) is responsible for maintaining the IRB protocol. When research data are acquired under a data use agreement, the project coordinator will create and maintain an ADAMS record for each acquired dataset. ADAMS houses an electronic record for each DUA held by researchers at HCP and links it with the associated IRB research protocol and list of

authorized study personnel, specifically those who are authorized to access data. The Compliance Office may verify at any time the members of a research team with access to a specific dataset via ADAMS.

The HCP Compliance Office will confirm if/when a person is authorized to access specific research data. Once confirmed, IT will set UNIX file permissions to allow that individual access to a specific directory on the server (where electronic data files have been loaded). Data files are not transferred electronically or distributed to an authorized user, rather, the authorized user is granted permission to access the location on the server where electronic files have been loaded, further partitioned by study or research role as needed. The PI will notify both the HCP Compliance Office and IRB of any project staffing changes (additions or removals). Staff added to a project will not be provided access to data until requirements at all levels (IRB, Department and ACHI) have been met and approval secured. Staff removed from a project will have their access to data terminated (IT will remove Unix file permissions).

- Describe your organization's physical and technical safeguards used to protect Initiative data files, including actions taken to physically secure data files and safeguards to limit access to Initiative data and analytical extracts among the project team.

All physical media are turned over to IT. Media are labeled and secured in the departmental safe which is located in a locked office in a locked suite with restricted key-card access. All data backup tapes are written in an encrypted form before being stored offsite in a secured facility. The building, Machine Room, and IT Office are secured via keycard locks. Access is always logged by security. Antivirus software runs on all client PCs used to access APCD data. No antivirus software is run on the Unix servers containing APCD data due to the overall poor performance of this software for Unix systems. We do not run full disk encryption on our fileservers, although we do have PGP level encryption available for file-based encryption if needed. Encryption on our fileservers is not required for certification as a "Level 4" Data Facility as we are (outlined in Section III) per Harvard Security Policy.

HCP employees are required to complete the HCP data security training when they first enter the Department. This training includes an overview of privacy, confidentiality and department-specific best practices specifically for the storage of electronic and physical data. Physical media governed by a data use agreement must be stored in the department safe. Electronic media must be stored on the secure server which is governed by Unix permissions granted by IT only when the Compliance Office verifies approved access.

III. DATA SHARING, ELECTRONIC TRANSMISSION, DISTRIBUTION

- Describe your organization's policies and procedures regarding the sharing, transmission, and distribution of Initiative data files.

Harvard University's Information Security Policy (http://vpr.harvard.edu/pages/harvard-research-data-security-policy) provides specific guidance for managing research data. This Policy applies to researchers and research team members who obtain, access or generate research data, in particular confidential

information. This policy applies to all research data regardless of the storage medium (e.g., disk drive, electronic tape, cartridge, disk, CD, DVD, external drive, paper, fiche, etc.) and regardless of form (e.g., text, graphic, video, audio, etc.), physically housed at Harvard or stored remotely under the management of Harvard researchers.

The Department of Health Care Policy at Harvard Medical School adheres to these policies and is further certified by Harvard University Information Technology (HUIT) as a Level 4 Data Facility. The Department is reviewed annually for meeting the additional controls required for a Level 4 Data Facility. APCD data stored at this site will be treated at a minimum as Level 4 data. Required protection in a Level 4 data facility is detailed here: http://policy.security.harvard.edu/view-data-security-level. These controls strengthen the security of sharing, transmission and distribution of data files (if these actions have been approved by ACHI).

APCD data are stored on the HCP secure server as described previously. The secure server is designated for data storage and is restricted by Unix permissions set by IT. Access may be allowed by IT only after an individual is verified as an authorized user by the Compliance Office. Specifically for APCD data use, authorized users are required to sign an Arkansas APCD Confidentiality Agreement. Data are not loaded onto remote devices or individual desktops unless specified by a data vendor (e.g. HRS restricted data). Users are educated on these practices and are made aware of the penalties noted in the data use agreement for non-compliance. Data are not shared between projects and/or institutions unless specifically approved by a data vendor.

- If your organization employs a data tracking system, please describe.

The Acquired Data Accountability and Management System (ADAMS) is a Drupal database used to track agreements governing use of acquired data for research. An ADAMS record is created for each acquired dataset and captures the following information: type of data (third party or prospectively collected), PI (Dr. Chernew), Data Custodian (Dr. Chen), Study Coordinator (Emily Corcoran), funding, IRB approval and ID number, data security (confidentiality) level as determined by the IRB, data storage information (physical and/or electronic), data file contents, authorized users, location(s) data may be accessed from and what type of security the access will have, whether or not data will be forwarded outside of Harvard systems, and if yes, what form the transfer will occur in, project goals, data vendor, provider number (if applicable), agreement effective dates, terms of data destruction. A copy of the fully-executed data agreement and any other supporting documentation is uploaded to the ADAMS record. ADAMS is a working, informational database designed to promote compliance with governing data use agreements through informed decision-making. ADAMS captures various types of information, but is not designed to detect events such as the transfer of data outside of our organization. If a transfer of data outside of Harvard has been approved under an agreement, it will be captured in the record.

- Describe the policies and procedures your organization has developed for the physical removal, transport, and transmission of Initiative data files.

Harvard University's Information Security Policy (http://vpr.harvard.edu/pages/harvard-research-data-security-policy) provides specific guidance for managing research data. This Policy applies to researchers and research team members who obtain, access or generate research data, in particular confidential information. This policy applies to all research data regardless of the storage medium (e.g., disk drive, electronic tape, cartridge, disk, CD, DVD, external drive, paper, fiche, etc.) and regardless of form (e.g., text, graphic, video, audio, etc.), physically housed at Harvard or stored remotely under the management of Harvard researchers.

Physical removal of APCD files: HCP will destroy APCD data files upon expiration of the data use agreement or at the end of the study, whichever occurs first. Paper files (if applicable) will be shredded onsite. Physical media (CD ROM, other non-paper media) will be collected onsite by Data Shredder, a fully licensed, bonded and insured data destruction vendor. Data Shredder will provide the HCP Compliance Office with a signed certificate of destruction (COD) upon removal of the physical media. The COD will be uploaded to ADAMS and shared with APCD in tandem with a signed Exhibit D (Certification of Project Completion and Destruction or Retention of Data). Electronic files will be deleted by the Data Custodian. The deletion process will be witnessed by a Department IT representative and documented in a separate, internal certificate of destruction form.

Transport of data: HCP data recipient will not transport APCD data physically in any medium. Data will only be transported physically if required by the data vendor. Harvard will comply with the data vendor's preferred method of transport (currier, third party carriers). Personal transport of physical media in prohibited.

Transmission of data: HCP data recipient will not transmit APCD data files to any third party unless specifically authorized by the data vendor to do so. A secure SSL enabled web transfer application from Accellion Inc. is available, as well as email or email attachments (10 MB limit), and SFTP (secure FTP). If necessary, data can be further secured with file encryption such as PGP.

- Explain how your organization will tailor and restrict data access privileges based on an individual's role on the project team.

The ADAMS database houses a record for each project-specific dataset housed or accessed via the Department of Health Care Policy. Each record includes project-specific information as well as a separate list of authorized users for that specific study dataset. Both the Compliance Office and the HCP IT Department share access to this database to verify authorized data users for a study's dataset(s) as well as refer to the DUA to ensure users have complied with any vendor-specific requirements (i.e. notifying the vendor of personnel addition). This database is maintained to accurately reflect department personnel changes including new and departing individuals, as well as changes to the IRB personnel roster (removing or adding a person from a study protocol).

If several types of APCD data are acquired for a research study and either (a) must be housed separately, and/or (b) cannot be accessed by all research team members, separate file partitions within the project-specific directory will be created to house the different data types. These file partitions will not be accessible to individuals until authorization is confirmed by the HCP Compliance Office and UNIX file

permissions are granted by IT. In either scenario above, housing requirements and role-specific access will be captured in ADAMS.

- Explain the use of technical safeguards for data access (which may include password protocols, log-on/log-off protocols, session time out protocols, and encryption for data in motion and data at rest).

- 5-minute screen lock on all office computers.
- Building ingress is key-carded and under video surveillance.
- All sensitive IT areas are key-carded.
- 30-minute default logout on Unix servers.
- VPN accounts lock.
- Restricted use on specific servers - login privileges are limited to specific project teams.
- Password protocols conform to University policy.
- All network communication between client and server is encrypted.
- Remote access to PC desktops is only available via the HMS encrypted VPN.

Antivirus software runs on all client PCs used to access APCD data. No antivirus software is run on the Unix servers containing APCD data due to the overall poor performance of this software for Unix systems. We do not run full disk encryption on our fileservers, although we do have PGP level encryption available for server file-based encryption if needed and on client desktop PCs used to access the APCD data. Encryption on our fileservers is not required for certification as a "Level 4" Data Facility as we are per Harvard Security Policy.

- Are additional organizations involved in analyzing the data files provided by ACHI?

No. Only HCP authorized users will analyze the data provided by ACHI. Only when ACHI has granted specific approval for other organizations or their staff to access data provided to Harvard will this be allowed.

- If an additional copy of the data will be housed in a separate location, please describe how the data will be transferred to this location.

There will not be an additional copy of the data to be housed in a separate location.

IV. DATA REPORTING AND PUBLICATION

- Who will have the main responsibility for notifying ACHI of any suspected incidents wherein the security and privacy of the Initiative Data may have been compromised?

The Data Custodian (Dr. Chen) will have the main responsibility for notifying ACHI of any suspected incidents wherein the security and privacy of the APCD data may have been compromised.

HCP Policy: Any possibility or concern of non-compliance with the data security policy or breach of data security should be reported immediately to the HCP Data Compliance Office at hcpcomplianceoffice@hcp.med.harvard.edu. The Department Administrator, Cynthia Hobbs, should be contacted next hobbs@hcp.med.harvard.edu or 617-432-0182. If Ms. Hobbs is not available, contact the HCP Systems Operations Manager, Young Sul, at sul@hcp.med.arvard.edu or 617-432-0186.

- Please describe and identify your organization's policies and procedures for responding to potential breaches in the security and privacy of the Initiative Data.

The concern of non-compliance will be documented by the HCP Compliance Office and the PI (Dr. Chernew) of the project consulted. If the concern is determined by HCP Compliance Committee to NOT be a breach of data security, the resolution will be documented for internal files, audit and training purposes. If the incident IS determined to be a breach of data security, the HCP Compliance Managing Committee and the HMS Committee on Human Studies (CHS) will be notified and Harvard guidelines for reporting incidents will be followed (http://www.security.harvard.edu/reporting-issues). The Harvard University Office of General Counsel will contact ACHI, and State and Federal incident reporting guidelines will be followed. HCP follows State, Federal, and Harvard University Whistleblower laws and policy http://security.harvard.edu/files/resources/Whistleblowing_Policy.pdf.

- Explain how your organization's data management plans are reviewed and approved.

Institutional Data Management policies remain subject to Harvard University Data Security requirements, government policy, regulations, and industry standards. Security innovations are applied according to all relevant federal and institutional guidelines. Study-specific data management plans are reviewed by the Institutional Review Board, in addition to the HCP Compliance Office to ensure protection of human subjects and ability to comply.

- Explain whether and how your organization's data management plans are updated during the Data Use Agreement (DUA) period.

Harvard University does not currently have a policy to conduct periodic updates to the Data Management plans. Data Management policies do remain open to changes based on Harvard University Data Security requirements, government policy, regulations, and industry standards. Security innovations are applied accordingly.

V. COMPLETION OF RESEARCH TASKS AND DATA DESTRUCTION

- Your organization must ensure that it has policies and procedures in place to destroy Initiative Data upon completion of the project and that you have safeguards to ensure the data are protected when members terminate their participation in the project. Describe the policies and procedures in place to destroy the Data Files upon completion of the project.

APCD data will be destroyed at the end of the project or at the time of DUA expiration, whichever occurs first. Upon expiration of the DUA, the Study Coordinator (Ms. Corcoran) will inform the IT Director that the media are to be given to the HCP Compliance Office where they are stored in a locked safe in a locked office until they are picked up by Data Shredder, a fully licensed, bonded and insured data destruction vendor. A detailed internal certificate of destruction is filled out by the Data Custodian (Dr. Chen) or the PI (Dr. Chernew) for the electronic data files and witnessed by IT as having been removed from the servers. The APCD data destruction form will be filled out and sent to ACHI with the supporting documentation.