DATA SHARING AGREEMENT

Between

STATE OF WASHINGTON OFFICE OF FINANCIAL MANAGEMENT (hereinafter referred to as OFM)

AND

CENTER FOR EDUCATION DATA & RESEARCH AT THE UNIVERSITY OF WASHINGTON (hereinafter referred to as UW-CEDR or Recipient)

This Data Sharing Agreement (DSA or Agreement) is by and between State of Washington entities OFM and UW-CEDR (collectively the "Parties"), is entered into pursuant to the authority granted by chapter 39.34 RCW, relevant federal statutes, and related regulations.

1. PURPOSE OF THE DSA, CONTEXT FOR DATA SHARING

   This DSA shall govern the access, use, storage, copying, creation, resulting derived data, and distribution of data by the Recipient. Pursuant to State of Washington, Office of the CIO policy 141.10 the parties acknowledge that the subject of this Agreement may involve the sharing of data and information considered highly confidential. Further, the Recipient acknowledges its responsibility to secure access to such data in compliance with this OCIO policy.

   The context for data sharing arises from the request from the Recipient to use OFM DATA to answer research questions identified in *APPENDIX E: METHODOLOGY* of this DSA. This project meets the requirements of the Audit or Evaluation Exception as outlined in the Family Education Rights and Privacy Act (FERPA) because the data are being used to evaluate the Careers Pathway program, therefore, Recipient is an authorized representative for the purpose of this project.

2. DEFINITIONS.

   "**AGREEMENT**" means this Data Sharing Agreement, including Appendices A, B, C, D, E and F, which are incorporated by this reference in this Agreement.
   "APPENDIX A" means the document attached to this Agreement titled *Statement of Confidentiality And Non-Disclosure*
   "APPENDIX B" means the document attached to this Agreement titled *Certification of Data Disposition*
   "APPENDIX C" means the document attached to this Agreement titled *Data Recipient Data Security Plan*
   "APPENDIX D" means the document attached to this Agreement titled *Data Recipient Disciplinary Policies For Employees Who Violate Education and/or Unemployment Insurance Wage Privacy Laws*
   "APPENDIX E" means the document attached to this Agreement titled *Methodology*
   "APPENDIX F" means the document attached to this Agreement titled *Cohort Description And Data Elements*

   "**CONFIDENTIAL INFORMATION**" means any data and information provided under this DSA. Including, without limitation, data and information that is specifically protected from disclosure by law:
   a. Personal information about individuals, regardless of how that information is obtained.
   b. Information concerning employee personnel records.
   c. Information regarding IT infrastructure and security of computer and telecommunications

systems.

"**DATA ACCESS**" means rights specifically granted under this DSA to Recipient systems and personnel to leverage the capabilities for connection to, reading, modification, deletion, and/ or otherwise method of interface with OFM systems, networks, other information technology infrastructure, OFM DATA, and/or any other non-OFM DATA information necessary for implementing DATA ACCESS capabilities.

"DATA BREACH" means any event in an information system or network that results in the exposure of data or capabilities to compromise or create a threat of material harm to the interests of individuals identifiable by the data therein. Additionally, events that meet the definition of "breach of the security of the system" as defined under RCW 42.56.590(4), are included in this definition. This definition is to be applied in the broadest sense applicable.

"**DATA STORAGE**" refers to the state of data at rest, which may include:, server-based storage on-site at a state entity or third party contractor storing data on behalf of a state entity, local device storage (including on workstations, and state personnel's PCs, and private mobile devices), and/or any other form of electronic storage media (including CDs, flash drives, portable hard drives, etc.).Under this Agreement storage of data is limited to server and local device storage.

"MALICIOUS CODE" means software (such as a Trojan horse) that appears to perform a useful or desirable function, but actually gains unauthorized access to system resources or tricks a user into executing other malicious logic.

"**OFM DATA**" means all data, records and information created, received, maintained, or transmitted by OFM which is accessed, used, created (including Recipient data derived from OFM DATA), stored, copied, or distributed by Recipient, in connection with the purpose of this DSA. OFM DATA shall be presumed to be confidential information, unless a less sensitive data classification can be substantiated with sufficient evidence.

"**PRIVACY ADMINISTRATOR**" is the individual designated in this Agreement who is responsible for overseeing the privacy and security of the data provided hereunder.

1. PERIOD OF AGREEMENT.

   This DSA shall commence on **October 15, 2018** and remain in force through **June 30, 2020** unless terminated sooner or extended as provided herein. This Agreement may be amended by mutual written agreement of the Parties. Further, this Agreement may be extended in up to one-year terms as mutually agreed by the parties. Any such extension will be effected in writing and attached to this Agreement. If specified by this Agreement or as required by law, certain provisions of this DSA will survive the termination of this Agreement.

2. STANDARD OF CARE

   a. The Recipient acknowledges and agrees that the fundamental privacy rights are vested in individuals associated with the OFM DATA that is provided to the Recipient under this DSA. Recipient will exercise due care and take all reasonable efforts to protect such individual privacy rights.

   b. Recipient represents and warrants that, with regard to confidentiality, availability, and integrity of OFM DATA, safeguarding the privacy rights of individuals and employers identified within OFM DATA, DATA ACCESS, DATA STORAGE, and handling of OFM DATA provided in connection with the purpose of this DSA shall be undertaken in compliance with current OCIO standards, policy and best practices. Such standards, policies and best practices can be found at: https://ocio.wa.gov/policy/securing-information-technology-assets.

3. DESCRIPTION OF DATA TO BE SHARED.

SEE APPENDIX F

4. PRIVACY AND CONSTRAINTS ON USE

a. Recipient may not make any ad hoc analyses or other uses of OFM DATA not specified within this DSA, are not permitted without obtaining prior written agreement from OFM. For avoidance of doubt, the following specific reporting capabilities are deemed either within the scope of this DSA or expressly permissible:

   i. Do Career Pathways generate successful outcomes for different populations of disadvantaged students?

b. Except as allowed under this DSA, Recipient is not permitted to share OFM DATA with another entity.

c. Recipient shall restrict access to OFM DATA to individuals who have signed and returned to OFM the Statement of Confidentiality and Non-Disclosure (Appendix A).

d. Recipient is not authorized to update or change any OFM DATA, and any updates or changes may be cause for immediate termination of this Agreement.

e. Neither Washington State nor OFM guarantee the accuracy or fitness for purpose of the data provided. Recipient acknowledges and accepts all risk and liability its use or misuse of information provided pursuant to this Agreement.

f. Data provided by OFM under this DSA shall not be linked with other data or data sets in any way that may disclose the identity of individuals or employers; the data in any data set shall be used for statistical purposes only. Using OFM DATA to identify students or employers may be cause for immediate termination of this Agreement. Further, at OFM's sole discretion, other data sharing agreements with Recipient may also be subject to termination and OFM may decline requests for data sharing agreements with the Recipient in the future. If the identity of any student or employer is discovered inadvertently, Recipient will not use this information and will immediately inform OFM in writing of any such discovery.

g. Recipient will follow applicable federal and state laws protecting student and employment data, and the guidelines specified in the Institute of Education Sciences SLDS Technical Brief, Statistical Methods for Protecting Personally Identifiable Information in Aggregate Reporting (NCES 2011-603 https://nces.ed.gov/pubsearch/pubsinfo.asp?pubid=2011603) when displaying student information in public reports. Publicly-reported aggregated results will not contain any group of fewer than 10 individuals.

h. When displaying employment data, Recipient must ensure that cell sizes are ample enough so that one record does not contain 80% of the wages or hours of a particular reporting cell. Other considerations when using employment data can be found in ERDC Technical Report 2012-01, Employment Data Handbook located at https://erdc.wa.gov/technical-resources.

i. Recipient must provide draft report(s) to OFM and data contributors at least ten (10) working days prior to any public release of reports to verify proper disclosure avoidance techniques have been used and communicate with OFM or data contributors when questions arise regarding data provided.

j. If Recipient becomes legally compelled to disclose any data (whether by judicial or administrative order, applicable law, rule or regulation, or otherwise), Recipient must use all reasonable efforts to provide OFM with prior notice.

k. Recipient is required to provide to OFM a writing (or writings) current within the last 12 months that describes the present state of Recipient's information privacy practices, including (but not by way of limitation) a summary of: how the use of OFM DATA by Recipient in connection with the purpose of this DSA may impact individual privacy rights, privacy rights safeguards presently implemented by OFM, and what privacy control capabilities are available to individuals and others.

l. Recipient shall plan to retain no copies of OFM DATA beyond the expiration of the DSA. Towards this end, Recipient shall certify when OFM DATA in Recipient's possession is deleted by providing OFM APPENDIX B. Disposal of media and data must follow the Washington Office of the Chief Information Officer (OCIO) guidance in Media Handling and Data Disposal Best Practices set forth at:

https://ocio.wa.gov/policy/media-handling-and-data-disposal-best-practices

m. In accordance with federal employment data law and education data best practices, OFM, in its sole discretion, may require an on-site inspection of Recipient to assure that the requirements of the state's law and data sharing agreement are being met. A list of Washington State approved auditing services companies are provided through the Department of Enterprise Services website: https://fortress.wa.gov/es/apps/ContractSearch/ContractSummary.aspx?c=05913. You may choose one from the list or send a letter requesting a specific company that may only be used with the approval from OFM. Audits must be accomplished within the first year that the data was transferred, and every three years until termination of the Agreement, and carrying through to the destruction of data.

n. The requirements of this Section 6. PRIVACY AND CONSTRAINTS ON USE shall survive the termination or expiration of this Agreement or any subsequent agreement intended to supersede this Agreement.

5. CONFIDENTIALITY AND ENCRYPTION OF DATA

a. Unless and until required, for the purposes of litigation, public disclosure law, or other legal right regulating the disclosure of state records, OFM DATA shall be assumed by Recipient to be confidential and treated as such. Except as specifically contemplated in writing under this Agreement, Recipient shall not publish, copy, or disclose OFM DATA connected with the purpose of this DSA to other parties.

b. If Recipient is served with any subpoena, discovery request, court order, or other legal request or order that calls for disclosure of any OFM DATA, then Recipient will promptly notify OFM

unless specifically prohibited by law from doing so. Notification is not prompt if, due to Recipient's delay, OFM lacks sufficient time to raise objections to the disclosure, obtain a protective order, or otherwise protect OFM DATA by limiting disclosure. Recipient shall at Recipient's expense, provide prompt and full assistance to OFM or its designated agent(s) in efforts to protect OFM DATA.

c. Recipient shall, in connection with DATA STORAGE of OFM DATA select and apply encryption, using industry-tested means, methods, algorithms or cryptographic modules validated that are effective. Compliance with National Institute of Standards and Technology (NIST) guidance on encryption shall be rebuttably presumed effective.

d. Recipient acknowledges that its breach or threatened breach of any its obligations under this Section 7 *CONFIDENTIALITY AND ENCRYPTION OF DATA* would not be susceptible to adequate relief by way of monetary damages only. Accordingly, OFM may, in that case, apply to court for any applicable equitable remedies (including injunctive relief), without the need to post any security, notwithstanding Section 11 *DISPUTE RESOLUTION* of this DSA.

6. INFORMATION SECURITY SAFEGUARDS

a. The DATA ACCESS and DATA STORAGE of OFM DATA by Recipient shall be protected by rigorous safeguards, against unauthorized disclosure and/or alteration. Such safeguards must meet or exceed those specifically set forth in this Agreement

b. Such safeguards must:

i. Meet or exceed the applicable standards for securing information technology assets as promulgated by the State of Washington Office of the CIO, including but not limited to Office of the CIO policy 141.10 §§ 5-11.
ii. Demonstrate the current or developing ability to meet or exceed the policies and guidelines for information security and privacy risk management commensurate with leading industry practices.

c. Such safeguards must, in particular, and at least:

i. Be informed by the principle of defense-depth; controls at multiple layers designed to protect the confidentiality, integrity and availability of data.
ii. Include appropriate personnel vetting/background checks, have appropriate separation of duties, and undertake other such workflow controls over personnel activities as necessary to safeguard OFM DATA.
iii. Follow change management procedures designed to keep Recipient's systems current on security patches, and prevent unintended or unauthorized system configuration changes that could expose system vulnerability or lead to a data breach.
iv. Involve a software development life cycle (SDLC) process that includes security and quality assurance roles and control process intended to eliminate existing and potential security vulnerabilities.
v. Have appropriate technical perimeter hardening, wherein Recipient monitors its system and perimeter configurations, and network traffic for vulnerabilities, indicators of activities by threat actors, and/or the presence of Malicious Code.

vi. Have access, authorization, and authentication technology appropriate for protecting confidential information.
vii. Maintain a process for backup and restoration of data.
viii. Protect facilities with adequate physical protections.

d. Recipient will coordinate with OFM to facilitate efficient and effective change management procedures compatible with the security and privacy requirements of this DSA.

e. OFM and Recipient each shall act with all due care and provide appropriate informational notification to the other when there is a data breach fully within the information systems of that party and the nature of the data breach directly impacts the confidentiality or integrity of the OFM DATA that has been submitted, transmitted, exchanged, or shared under this DSA.

f. Recipient will comply with the requirements of the Washington State Auditor's Office and State of Washington Office of the CIO with respect to IT Security Auditing. Recipient shall promptly inform OFM in writing when (i) Recipient has submitted the required audit attestations to the appropriate state authorities, and (ii) if there are outcomes from the auditing process, germane to the purpose of this DSA, such as findings of non-compliance, variance from State standards, or formal acceptance of risk, or documentation of residual risk and/or compensating controls.

7. ALLOCATION OF LIABILITY

As between OFM and Recipient, on behalf themselves and their personnel, each agrees to defend, indemnify, and hold the other harmless from and against all claims, demands, suit, proceedings, judgment, award, direct damages, costs, expenses, fees, fines of a penal nature, civil penalties, and other liabilities (including the obligation to indemnify others) arising from or connected to a data breach, to the extent caused by the indemnitor party's negligence. The indemnitee's right to indemnification under this DSA will not be construed as excluding other rights and remedies available to the indemnitee.

8. TERMINATION

a. **For Convenience**. Either party may terminate this Agreement for any reason upon 60 business days' notice to the other party.
b. For Cause. OFM may terminate this Agreement at any time prior to the date of completion if and when it is determined that Recipient has failed to comply with the conditions of this Agreement. OFM shall promptly notify Recipient in writing of the termination and the reasons for termination, together with the effective date of termination. In case of termination, the data provided by OFM must be returned to OFM or destroyed on or before the date of termination. Written notification of destruction to OFM is required.

9. DISPUTE RESOLUTION – DISPUTE RESOLUTION PANEL

Both parties agree to exercise good faith in dispute resolution and to settle disputes prior to using a Dispute Resolution Panel whenever possible. Unless irreparable harm will result, neither party will commence litigation against the other before the Dispute Resolution Panel has issued its decision on the matter in dispute.

In the event a dispute arises under this DSA and cannot be resolved between the parties it will be handled by a Dispute Resolution Panel (the Panel) in the following manner:

Each party to this DSA will appoint one member to the Panel. These two appointed members will jointly appoint an additional member. The Panel will review the facts, DSA terms and conditions as well as applicable statutes and rules. The Panel will make a determination of the dispute as quickly as reasonably possible. The determination of the Panel will be final and binding on the parties hereto.

Notwithstanding any dispute, the parties agree to carry out all their respective responsibilities to protect the data provided under this DSA.

10. SEVERABILITY AND GOVERNING LAW
    a. The provisions of the DSA are severable. If any provisions of this DSA are held invalid by any court, then that invalidation shall not affect the other provisions of this DSA, and the invalid provision shall be considered modified to conform to the existing law.

    b. This Agreement shall be construed under the laws of the State of Washington. In the event of a lawsuit involving this DSA, venue shall be proper only in Thurston County, Washington.

11. CONTACTS

DATA RECIPIENT: CENTER FOR EDUCATION DATA & RESEARCH

Contact Role	Agreement Administrator	Privacy Administrator
Name:	Dan Goldhaber	Nate Brown
Title:	Director	Research Manager
Department:	Center for Education Data and Research, University of Washington	Center for Education Data and Research, University of Washington
Email:	dgoldhab@uw.edu	nrb9@uw.edu
Telephone:	206-547-5585	206-547-5585

DATA PROVIDER: OFM

Contact Role	Agreement Administrator	Privacy Administrator
Name:	Jim Schmidt	Lynn Cole
Title:	Sr. Forecasting Coordinator	Data Analyst
Department:	Forecasting	Forecasting
Email:	Jim.schmidt@ofm.wa.gov	Lynn.cole@ofm.wa.gov
Telephone:	360-902-0595	360-902-0952

12. AUTHORITY TO BIND

The signatories to this Contract represent that they have the authority to bind their respective organizations to this DSA.

13. COUNTERPARTS

This DSA may be executed in counterparts or in duplicate originals. Each counterpart or each duplicate will be considered an original copy of this DSA as if signed by each party, for all purposes.

14. SIGNATURES

In Witness Whereof, the parties hereto, having read this DSA in its entirety, including all attachments, by their signatures below signify that they understand and agree to it in full.

OFM

Roselyn Marcus
Signature

~~Rebecca R. Riley~~ Roselyn Marcus
Printed Name

~~IT Contracts Administrator~~ Assistant Director Legal & Legislative Affairs
Title

10/18/2018
Date

RECIPIENT

Richard S. Sewell
Signature

Carol Rhodes (Richard S. Sewell signing for Carol Rhodes)
Printed Name

Director, Office of Sponsored Programs (Grant and Contract Administrator)
Title

10/16/2018
Date

APPENDIX A

STATEMENT OF CONFIDENTIALITY AND NON-DISCLOSURE
between
STATE OF WASHINGTON OFFICE OF FINANCIAL MANAGEMENT
and the
CENTER FOR EDUCATION DATA & RESEARCH AT THE UNIVERSITY OF WASHINGTON (UW-CEDR)

As an employee of the UW-CEDR, I have access to information provided by the State of Washington, Office of Financial Management (OFM). This information is confidential, and I understand that I am responsible for maintaining this confidentiality. I understand that the information may be used solely for the purposes of work under DSA No. K2405.

Employee
Initials

_____ I have been informed and understand that all information related to this DSA is confidential and may not be disclosed to unauthorized persons. I agree not to divulge, transfer, sell, or otherwise make known to unauthorized persons any data or information provided to me, regardless of form.

_____ I also understand that I cannot access or use this information for my own personal use or benefit. I understand that my use is limited to the extent necessary and for the purpose of performing my assigned duties as an employee of the UW-CEDR under this Agreement. I understand that a breach of this confidentiality will be grounds for disciplinary action, which may include termination of my employment and other legal action.

_____ I have been informed of and agree to abide by all federal and state laws and regulations regarding confidentiality and disclosure of the information related to this DSA.

_____ I have read, understand and agree to be bound by the data sharing agreement related to this Statement of Confidentiality and Non-Disclosure.

	Employee	Supervisor By my signature below, I certify that the employee signing this document has been informed of Recipient obligations including any limitation on the use or publishing of confidential data.
Signature	_____	_____
Printed Name	_____	_____
Organization	_____	_____
Job Title	_____	_____
E-mail address	_____	_____
Date	_____	_____

Please return signed forms to the OFM Agreement Administrator, PO Box 43124, Olympia, WA 98504-3124

APPENDIX B

Certification of Data Disposition

Recipient Name: CENTER FOR EDUCATION DATA & RESEARCH AT THE UNIVERSITY OF WASHINGTON

OFM Data Sharing Agreement (DSA) Number: K2405

Date of Disposition _____

Media (type, serial number, other unique identifiers) _____

Date the media was sanitized: _____

The person performing the activity was: _____

The method used to render all data unusable (e.g. software tool used and/or physical destruction of the media) was: _____

All copies of any data sets related to this DSA that have not been disposed of in a manner described above, have been returned to OFM's Agreement Administrator named below:

Name/Title _____

Media to be disposed must stay within the control of the agency from the time it is collected until the time it is sanitized. Storage media to be disposed should be collected by, and in the constant possession of dedicated, trusted personnel. Media must be maintained in a secure, locked area until it can be sanitized.

By the authorized signature below, the data Recipient hereby certifies that the data provided by OFM has been handled and rendered unusable as indicated above and as required in the Agreement designated above.

Signature of Recipient Agreement Administrator _____ Date: _____

Name/Title _____

Return original to OFM Agreement Administrator indicated on page 1 of the referenced DSA. Retain a copy for your records.

APPENDIX C: DATA RECIPIENT DATA SECURITY PLAN

Data will be stored at the Center for Education Data and Research (UW-CEDR). Access to restricted data will be limited to the project directors and research staff who require access for evaluation/analysis purposes and who have agreed, in writing, to maintain the individual confidentiality of all data. UW-CEDR has the following security features:

Physical Security Measures

Network concentration equipment and data server are to be housed in a locked and fenced cage accessible only by authorized personnel.

Receipt/Labeling & Storage of Confidential Storage Media

All storage media (diskettes, tape cartridges, CDs, internal and external hard drives) that hold confidential data are added to UW-CEDR's restricted data inventory and labeled with the following information:

- The word CONFIDENTIAL or RESTRICTED
- Inventory tracking number
- Stored in a data safe located in the secured data server room

Logging

The following information about what happens to the storage media while in UW-CEDR's care is recorded:

- Receipt of item from external source
- Creation of item at UW-CEDR
- Destruction of item
- Transfer of item to someone else's responsibility (even within the institution)
- Any breach in data security

And includes:

- Date
- Name of responsible individual
- Description (what happened, to whom transferred, etc.)

Any breach in data security or release of confidential information must be reported to UW-CEDR's Principal Investigator and to the University of Washington's Internal Review Board.

Printing

Confidential printouts must be stored safely at all times. The following protocols are to be used for any and all printouts of confidential data:

- Do not send confidential data that includes identifiers to any "public" printers (where any passerby can see or take the printouts).
- Use printers for confidential, non-identified data only if you can be with the printer while it's printing. You do not need to log what happens to printouts that never leave the UW- CEDR premises.
- Dispose of confidential printouts in a shredder, unless externally imposed requirements dictate a different method.

Backups

Backups of confidential data are themselves confidential, and also require logging.

- Backups should be encrypted if they contain confidential data.
- Backup tapes, diskettes or CDs containing confidential data must be locked up.
- Backup tapes, diskettes, or CDs containing confidential data must be sanitized before they are discarded or disposed of according to the guidelines in the section on disposal of confidential storage media.

Disposal or Scrubbing of Confidential Storage Media

Acceptable methods for the disposal or "scrubbing" of confidential storage media are:

- Returning the media to the source
- Physical destruction by an approved method
- Erasure using a recommended "secure erasure" product (e.g. PGP Secure Erase)

Computer Data Network Security Measures

Neither the secure data server nor the workstation machines will be connected to the internet or any other external network. The secure server will be coded/locked so that only specified PCs will be able to access it. Computer access to the secure server will be restricted to a specific list of machines, based on each machine's unique MAC address. This measure ensures that access to the server cannot be achieved by simply removing the secure network cable from a researcher's machine and plugging it into an unauthorized machine.

More specifically, we have:

- No external connectivity. This includes no connectivity to any wide-area network or the internet.
- Direct connections from computers to network to concentration device. Extending hubs or switches will not be permitted, in order to maintain access control.
- MAC address-based filtering placed on network concentration device for each and every authorized computer connecting to the network.
- IP address-based filtering for management of network concentration device only allowed from server, which resides in locked cage.
- No DHCP servers or automatic network connectivity protocols will be allowed.

Data Server Security Measures

- Located in a physically secure, locked and fenced cage.
- Data server to be kept logged off when not in active use.
- Password protected screensaver to activate after 5 minutes of non-activity.
- Anonymous connections to data server not permitted – valid account required for logging into server.

Workstation Server Security Measures

- Desktop computers to be kept logged off when not in active use.
- Password protected screensavers to activate after 5 minutes of non-activity.

Research Personnel Security Measures

- Secure network access will be restricted (through the use of passwords) to just those researchers who are currently approved by NCES or other authorizing institution to access the secure data. Currently, all UW-CEDR quantitative researchers and research assistants have submitted notarized affidavits of non-disclosure and received NCES approval to work with restricted data.

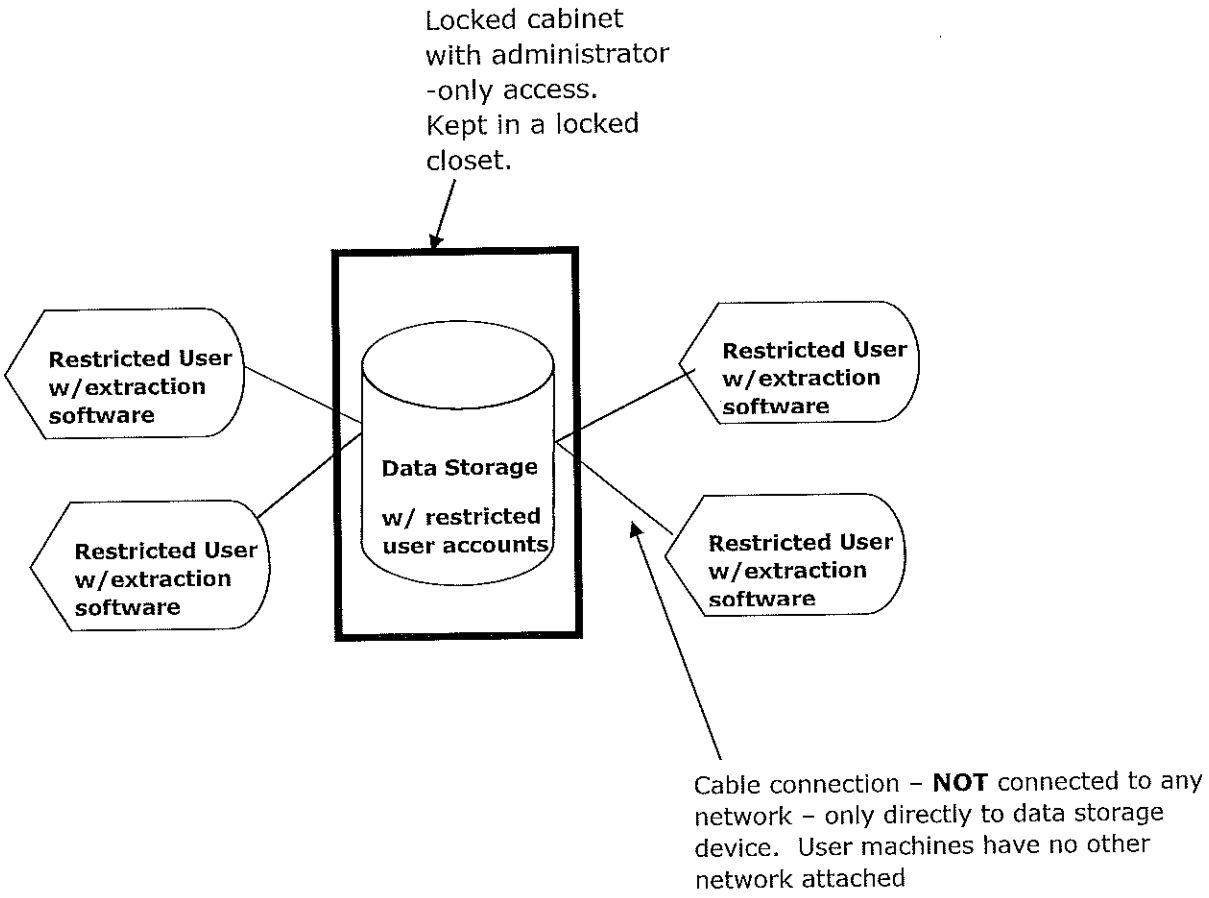
The following additional measures will be implemented to ensure that the confidentiality of restricted data is protected and maintained:

- Data analysis files will be stripped of individually identifiable information, will be password-protected, and accessible only to members of the research team who have signed confidentiality agreements.

- Linkage files containing individually identifiable information will be stored at UW-CEDR in locked data safes. The linkage files will be stored separately from data analysis files.
- All data provided by ERDC to UW-CEDR will be transmitted via Secure File Transfer Protocol (SFTP).Adequate precautions will be taken to ensure the physical and administrative security of individually identifiable data. Hard copy data and diskettes containing individually identifiable data will be kept in a safe or locked file cabinet at UW-CEDR.
- Computer Services will be notified of the location of all data analysis files in this project. Diskette/tape backups will be stored in locked file cabinets in a secure room at UW-CEDR.
- All hard copy files with individually identifiable information will be destroyed at the end of the project.
- All files that link unique I.D. numbers with individual names will be destroyed at the end of the project.
- Project findings and reports prepared for dissemination will not contain information that could be used to identify any individual.

Although geographic identifiers may be used in analysis, they will never be reported in the results. In addition, results from these surveys will not be reported unless the cell size is above a threshold of three observations to maintain a majority of respondents.

DIAGRAM OF UW-CEDR SECURE NETWORK



APPENDIX D: DATA RECIPIENT DISCIPLINARY POLICIES FOR EMPLOYEES WHO VIOLATE EDUCATION AND/OR UNEMPLOYMENT INSURANCE WAGE PRIVACY LAWS

Failure by an individual to comply with the University of Washington policies on information security and privacy may result in disciplinary action up to and including termination for University employees, contract termination in the case of contractors or consultants, dismissal for interns and volunteers, or suspension or expulsion in the case of a student.

The University reserves the right to pursue appropriate legal actions to recover any financial losses suffered as the result of a violation of the University policies on information security and privacy.

APPENDIX E: METHODOLOGY

Research Questions:

1. How many students embark on formally defined career or college readiness pathway programs in Washington State Community Colleges? Is participation in these programs associated with good postsecondary and employment outcomes?
2. What are the effects of the introduction of career pathway programs on students' educational attainment and earnings?

Methodology:

Research question 1 is a descriptive study of students' progression through well-defined career and college-readiness pathways in Washington's two-year colleges. To address this research question, we will classify students into various college pathways using enrollment data from the State Board for Community and Technical Colleges. We will then use this data to compute various milestones (e.g., accumulation of a certain number of credits, completion of certificate programs, associate degrees, and transfer to four-year institutions). Using data on these milestones, we will estimate regressions describing the academic progress of students participating in these programs. A typical regression would take the form

$$Y = X\beta + Pathway\delta + \epsilon \quad (1)$$

where Y is an academic milestone, X is a vector of student academic and demographic characteristics and *Pathway* is a vector indicating several different program pathways available to community college students. The pathway indicators describe the subject area (and in some cases degree level) of the student's program.

To answer research question 2, we will estimate difference-in-differences models that compare outcomes for students who are eligible for certain career and college-readiness pathways before and after the implementation of these programs. For instance, certain kinds of "stackable credential" programs are available for students who have previously earned a certificate and would like to continue to an associate degree. These changes in pathway designs inform our research. A typical regression is

$$Y = X\beta + Pathway\delta_1 + Eligible\delta_2 + Eligible{\times}Pathway\delta_3 + \epsilon \quad (2)$$

where *Eligible* indicates that the student is eligible for the pathway (this will vary by pathway and may indicate enrollment in a prerequisite program, remedial status, etc.) and *Eligible×Pathway* indicates enrollment in a program after the introduction of the specific pathway component.

APPENDIX F: COHORT DESCRIPTION AND DATA ELEMENTS

Cohort: Students who attended WA public community and technical colleges between 2005 and 2017

Higher Education Student Characteristics

ResearchID
SourceSystemTypeCD
DataCollectionTTL
TermSystemTTL
OrganizationYear
TermTTL
TermStartDT
TermEndDT
EnrolledOrganizationID
EnrolledOrganizationTTL
IPEDSOrganizationID
IPEDSOrganizationTTL
MajorProgramFieldOfStudyCIP
MajorProgramFieldOfStudyCIPTTL
MajorConcentrationCIP
MajorConcentrationCIPTTL
GenderTTL
DateOfBirth_YearMonth
CountyID
CountyDesc
StateOfOriginID
StateOfOriginDesc
NationOfCitizenshipID
NationOfCitizenshipDesc
ResidentStatusTTL
RaceID1
RaceTTL1
RaceGroupID1
RaceGroupTTL1
RaceID2
RaceTTL2
RaceGroupID2
RaceGroupTTL2
RaceID3
RaceTTL3
RaceGroupID3
RaceGroupTTL3
RaceID4
RaceTTL4

RaceGroupID4
RaceGroupTTL4
RaceID5
RaceTTL5
RaceGroupID5
RaceGroupTTL5
EthnicityID1
EthnicityTTL1
HispanicLatinoGroupTTL1
EthnicityID2
EthnicityTTL2
HispanicLatinoGroupTTL2
EthnicityID3
EthnicityTTL3
HispanicLatinoGroupTTL3
PELLGrantStatus
PriorPELLGrantStatus
StateNeedGrantStatus
PriorStateNeedGrantStatus
StudentTypeID
StudentTypeTTL
BaccalaureateClassStandingTTL
RunningStartID
RunningStartTTL
RunningStartIndicator
PriorRunningStartIndicator
SBCTCDualEnrollmentIndicator
PriorSBCTCDualEnrollmentIndicator
PriorTransferOrganizationID
PriorTransferOrganizationTTL
VeteranStatusTTL
VeteranBenefitID
VeteranBenefitTTL
AdmitYear
AdmitTermTTL
AdmitCampusID
AdmitCampusTTL
SBCTCSourceID
SBCTCSourceTTL
SBCTCPriorEducationID
SBCTCPriorEducationTTL
EconomicDisadvantageID
EconomicDisadvantageTTL
FamilyStatusID
FamilyStatusTTL

FirstYearEnrolledEverSBCTC
FirstTermEnrolledEverSBCTCTTL
FirstYearEnrolledEverPCHEES
FirstTermEnrolledEverPCHEESTTL
PreviousInstitutionDegreeLevelID
PreviousInstitutionDegreeLevelTTL
PreviousCreditsTransferredTotal
PreviousCreditsTransferredAP
PreviousCreditsTransferredIB
RecentHighSchoolCompletion
HighSchoolCompletionYear
PurposeForAttendingID
PurposeForAttendingTTL

Higher Education Completions

ResearchID
SourceSystemTypeCD
AchievementOrganizationID
AchievementOrganizationTTL
IPEDSOrganizationID
IPEDSOrganizationTTL
AchievementOrganizationYear
AchievementTermTTL
AchievementDT
AchievementTypeCD
AchievementTypeTTL
DegreeAcronym
DegreeName
AchievementCIP
GenderTTL
DateOfBirth_YearMonth
CountyID
CountyDesc
StateOfOriginID
StateOfOriginDesc
NationOfCitizenshipID
NationOfCitizenshipDesc
ResidentStatus
RaceID1
RaceTTL1
RaceGroupID1
RaceGroupTTL1
RaceID2

RaceTTL2
RaceGroupID2
RaceGroupTTL2
RaceID3
RaceTTL3
RaceGroupID3
RaceGroupTTL3
RaceID4
RaceTTL4
RaceGroupID4
RaceGroupTTL4
RaceID5
RaceTTL5
RaceGroupID5
RaceGroupTTL5
EthnicityID1
EthnicityTTL1
HispanicLatinoGroupTTL1
EthnicityID2
EthnicityTTL2
HispanicLatinoGroupTTL2
EthnicityID3
EthnicityTTL3
HispanicLatinoGroupTTL3
PriorPELLGrantStatus
PriorStateNeedGrantStatus
MostRecentPriorStudentTypeID
MostRecentPriorStudentTypeDesc
PriorRunningStartIndicator
MostRecentPriorTransferOrganizationID
MostRecentPriorTransferOrganizationDesc
CreditsTransferred
OccupationID
OccupationName
SOC

High School Completions

ResearchID
SourceSystemTypeCD
AchievementOrganizationID
AchievementOrganizationTTL
AchievementDT
AchievementTypeCD
AchievementTypeTTL

HighSchoolGPA
K12PrimarySchool
RecordNote

Higher Education Enrollment

ResearchID
SourceSystemTypeCD
EnrollmentOrganizationID
EnrollmentOrganizationTTL
IPEDSOrganizationID
IPEDSOrganizationTTL
DataCollectionTTL
TermSystemTTL
OrganizationYear
TermTTL
TermStartDT
TermEndDT
CumulativeInstitutionGPA
CreditsAttempted
CreditsEarned
LNIApprenticeship

Higher Education Enrollment Detail

TermEndDT
CourseSectionID
CourseSectionTTL
CourseNumber
CourseSubjectCIP
CollegeLevelCourseEnrollmentFlag
CollegeLevelMathCourseEnrollmentFlag
CollegeLevelEnglishCourseEnrollmentFlag
PreCollegeCourseFlag
PreCollegeMathCourseFlag
PreCollegeEnglishCourseFlag
CourseStartDT
CourseEndDT
VariableDatesFlag
CreditsAttempted
CreditsEarned
GradeID
GradeTTL
GradeNumber

SBCTCFeePayStatusID
SBCTCFeePayStatusTTL
SBCTCDeptDivTTL

UI Wage

ResearchID
SourceSystemTypeCD
EmployerResearchID
IndustryNAICS2Digit
Wage Year
WageTermTypeTTL
TotalHours
TotalWages
Cnt_ResearchIDs