The Cross-National Equivalent Files at the Center for Human Resources Research (CHRR)

This document describes the Cross-National Equivalent File (CNEF) data stored at CHRR at The Ohio State University. The document briefly describes the CNEF data and the Investigator platform at CHRR that serves as the interface between the data and users. It then describes the different ways users interact with the data and the level of security associated with each level.

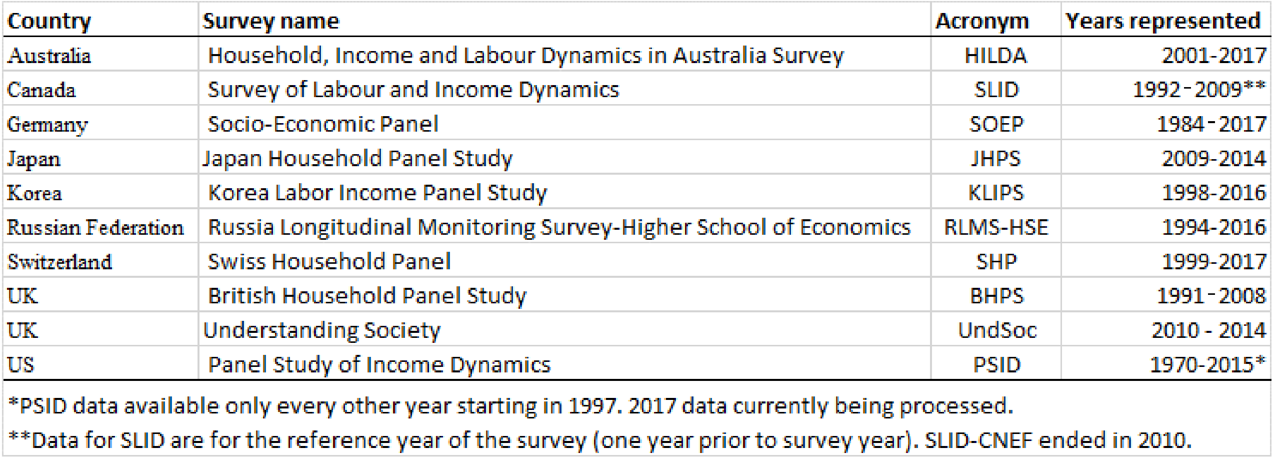
To protect the CNEF data (and a multitude of other public use and restricted data sets), CHRR employs stringent security standards. We summarize important features of those standards below. An Appendix presents CHRR documents that describe details of the data security protocols and procedures.

Overview of the CNEF project

Scholars and colleagues at partner institutions in nine countries collaborate to prepare CNEF files. The CNEF files consist of data drawn from household-based panel surveys administered in each country. Researchers use data from those surveys and a well-established harmonization criterion to create a set of variables that are comparable across countries and over time. The CNEF variables represent a subset of data available in each of the original parent surveys for which it is possible to harmonize data across at least two of the nine countries. Researchers have not yet harmonized all data that meet this criterion.

All harmonized CNEF variables share a common conceptual basis and common response categories. Researchers create CNEF variables if data exist on parent surveys in at least two of the nine countries and if those data can be harmonized. As of May 2019, CNEF includes data from surveys administered in Australia, Canada, Germany, Japan, Korea, Russian Federation, Switzerland, United Kingdom, and the United States. All of the parent surveys follow individuals over time. Table 1 lists the surveys administered in each country and the most recent wave of the data available to researchers.

Table 1. CNEF countries, parent survey names, and years for which data are available



Country	Survey name	Acronym	Years represented
Australia	Household, Income and Labour Dynamics in Australia Survey	HILDA	2001-2017
Canada	Survey of Labour and Income Dynamics	SLID	1992-2009**
Germany	Socio-Economic Panel	SOEP	1984-2017
Japan	Japan Household Panel Study	JHPS	2009-2014
Korea	Korea Labor Income Panel Study	KLIPS	1998-2016
Russian Federation	Russia Longitudinal Monitoring Survey-Higher School of Economics	RLMS-HSE	1994-2016
Switzerland	Swiss Household Panel	SHP	1999-2017
UK	British Household Panel Study	BHPS	1991-2008
UK	Understanding Society	UndSoc	2010 - 2014
US	Panel Study of Income Dynamics	PSID	1970-2015*

*PSID data available only every other year starting in 1997. 2017 data currently being processed.

**Data for SLID are for the reference year of the survey (one year prior to survey year). SLID-CNEF ended in 2010.

Researchers worldwide use these data to study social and economic behaviors and outcomes. Although CNEF data have been available for more than twenty-five years, it is only now that researchers have the opportunity to browse and download CNEF data via a web-based data platform, called "***CNEF Investigator***."

CNEF Investigator

With funding from the National Institute for Child Health and Development (NICHD) the CNEF project has created a web-based platform for the CNEF data. The platform is the Investigator data interface that CHRR researchers developed. Together with colleagues at CHRR, we reconfigured CNEF data and mounted it on the Investigator platform. One can access and browse the data at https://www.chrr.ohio-state.edu/investigator

Security & encryption

Randy Olsen and a team of programmers at CHRR developed the Investigator platform to provide an interface for researchers to browse, explore, and download data from the National Longitudinal Surveys. Since then, CHRR adapted the Investigator platform so it can host other data sets. CHRR worked with the CNEF team to adapt Investigator to offer existing and potential researchers access to CNEF data. It does so through its matured and user-friendly platform. Before we describe the levels of access we propose that researchers have, we will briefly describe the data security and encryption environment CHRR provides. That environment includes a safe storage and distribution environment that makes Investigator an ideal platform to modernize how CNEF users browse and access the data.

CHRR follows the National Institute of Standards and Technology (NIST) 800-53 revision 4 moderate baseline security framework. CHRR implements its NIST 800-53 revision 4 security policy on all components of its information systems. This includes systems that may be covered by another information security policy at CHRR. The NIST 800-53 rev 4 covers all aspects of security, including (but not limited to): Access Control; Audit and Accountability; Identification and Authentication; Physical and Environmental Protection; Risk Assessment; Security Assessment and Authorization; System and Communication Protection; and System and Information Integrity.

CHRR trains all new staff to be conversant in these security protocols. Every year CHRR personnel refresh their security training. Several CHRR Information Technology staff members hold IT security certifications. In addition to these activities, CHRR dedicates substantial funds each year toward security. Finally, third party auditors regularly audit all of CHRR's activities to ensure they comply with the NIST 800-53 framework.

CHRR employs various enterprise-level tools to maintain the IT infrastructure. Juniper SRX firewall appliances, with context-aware firewall capabilities, comprehensive real-time threat defense, and highly secure communication mechanisms is utilized as CHRR's firewall appliance. For external data services (the "Investigator"), CHRR uses Oracle Enterprise as its database management system. CHRR maintains two secure data processing sites and mirrors crucial backups between the sites to ensure full safety of data at all times.

A Tier 3 State of Ohio data center, with strictly controlled security access and redundant power distribution hosts CHRR’s external services. CHRR scans all application, database, servers, and systems on its network regularly with Nessus vulnerability scanning software to detect the presence of flaws in the system. CHRR employs Data Loss Prevention software and Intrusion Detection Systems on both the network (IDS) and server (HIDS). CHRR sends all security audit logs to its Splunk Security information and event management (SIEM) system. That system correlates log information, monitors in real-time and alerts CHRR of any issues.

The CHRR systems also comply with protocols laid out in the Federal Information Processing Standard (FIPS) Publication 140-2 (FIPS 140-2). Specifically, CHRR ensures compliance with FIPS 140-2 for all cryptographic operations that run inside its information systems. Further, CHRR requires the use of encrypted protocols and FIPS 140-2 approved algorithms and ciphers for all communications that include sensitive data. CHRR requires the use of those protection protocols and algorithms for communications across both internal and external networks. Finally, CHRR forbids the use of all plain text network protocols that transmit authentication or sensitive data.

HIPAA Security Policy

CHRR complies with the Health Insurance Portability and Accountability Act (HIPAA). This Act mandates that organizations comply with HIPAA Security Rule safeguards for all Electronic Protected Health Information (EPHI) in its information systems. Therefore, CHRR has implemented the security safeguards that HIPAA requires.

Interested readers may request the “CHRR Security Manual.” It fully documents CHRR’s policies and procedures. Additional references appear below.

Proposed levels of data access

We propose to offer three ways that CNEF researchers and potential CNEF researchers can interact with CNEF data using the Investigator platform. Two of the three require or may require that a person establish an Investigator User Account.

The overarching aim is to increase the use of CNEF data and of the data from the parent surveys for each CNEF partner. We propose three levels of access because we recognize that each CNEF partner faces different constraints on data access, wants to retain control over their data, or their government may not authorize some expressions of the data.

In recognition of these issues, we propose a “Browse mode” to fully protect the data but still let potential CNEF users see and explore the data. Whether users may access data beyond browsing is completely determined by each CNEF partner. We envision three ways CNEF users might actually get the data.

1. Encrypted files burned onto a DVD and delivered by mail to the authorized user;
2. Complete data files delivered by secure ftp technology;
3. User chosen subsets of variables delivered by secure ftp technology.

The first option is the one we currently use. We use it partly because some CNEF partners require it. However, we expect most partners will eventually switch from this method because online delivery is actually more secure, costs less, and users prefer it. Below we describe the second two types of access and the procedure users will have to follow.

Investigator User Accounts

Anyone may establish a CHRR Investigator account at no cost. Establishing an account does not automatically give users access to data. The establishment of an Investigator User Account provides the first (of several) methods by which we track who is using the data.

To establish an Investigator account, users simply email CNEF_account_request@chrr.osu.edu with the following information: First name, last name, and email address.

Once an Investigator account is established, the user requests access to specific data.

The CNEF Project Manager assigns users access to one or more of the CNEF Investigator studies on a country-by-country basis. We offer three levels of access to CNEF data. In the meantime, CHRR maintains a full audit trail of all account logins, permission assignments, data accesses through Investigator, and administrative accesses.

Default access – Browse mode

The default level of access allows users to browse all CNEF files. Note that the CHRR system allows us to track the number of times each scholar logs onto the CNEF Investigator as well as information on the country file and variables the user downloaded.

In the Browse mode, scholars who have an Investigator account may view basic information about each CNEF file including the list of variables, years for which the data are available, variable definitions, response categories, and how each variable is distributed. Under this level of access users can only view aggregate descriptions of the data (numerical and graphical frequency distributions), meta-data that describes the variable, and construction of those data. We are in the process of creating pages that show the code that CNEF partners use to construct the data. We also want to explore the possibility of providing links to the parent survey platforms that let users get information and access documentation for each underlying variable and increase the use of the full parent survey for each country.

Data access

We propose to create two additional access levels. One allows users to download the complete (encrypted) CNEF data file for each country. The second level allows users to employ Investigator's “shopping basket” technology to select a subset of available variables (for any combination of countries) and download that basket of variables.

Complete country file access

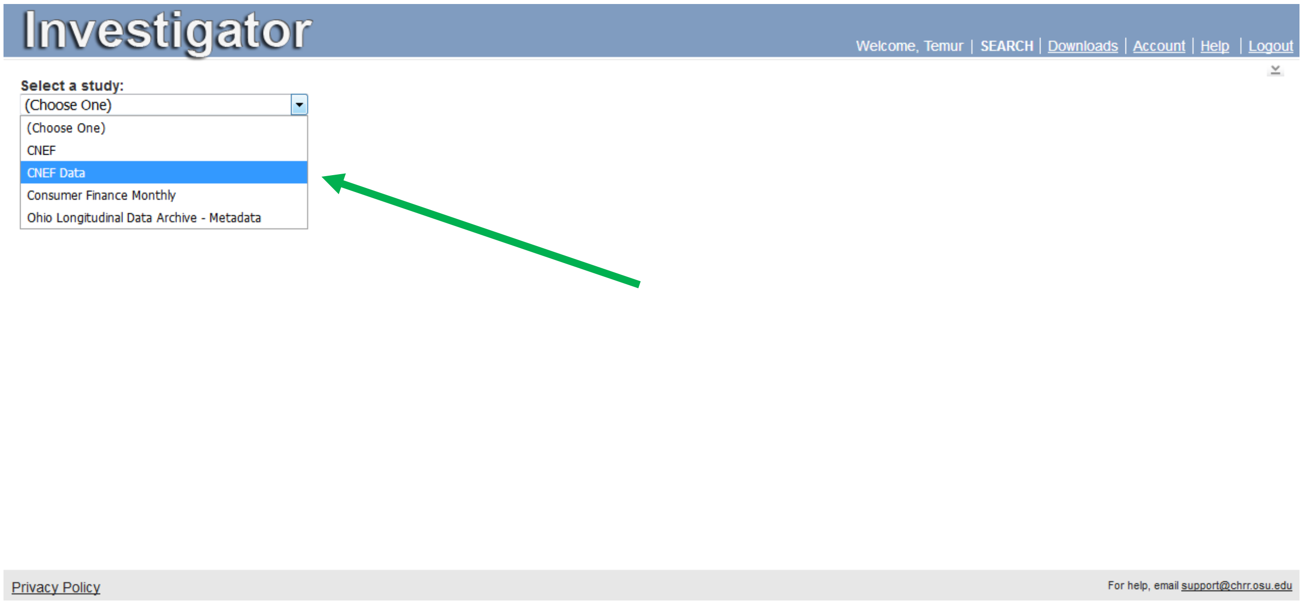
Under the complete country file access, authorized users may download data but only the complete set of data for a particular country. To use this option, users must send us the access authorization they get from the CNEF partner. To get that authorization they need to follow the procedure outlined at https://cnef.ehe.osu.edu/data/access-procedures/. The CNEF Project Manager will not authorize a user to download the data unless and until they has confirmed the authorization with the appropriate country authority.

Individual variable access

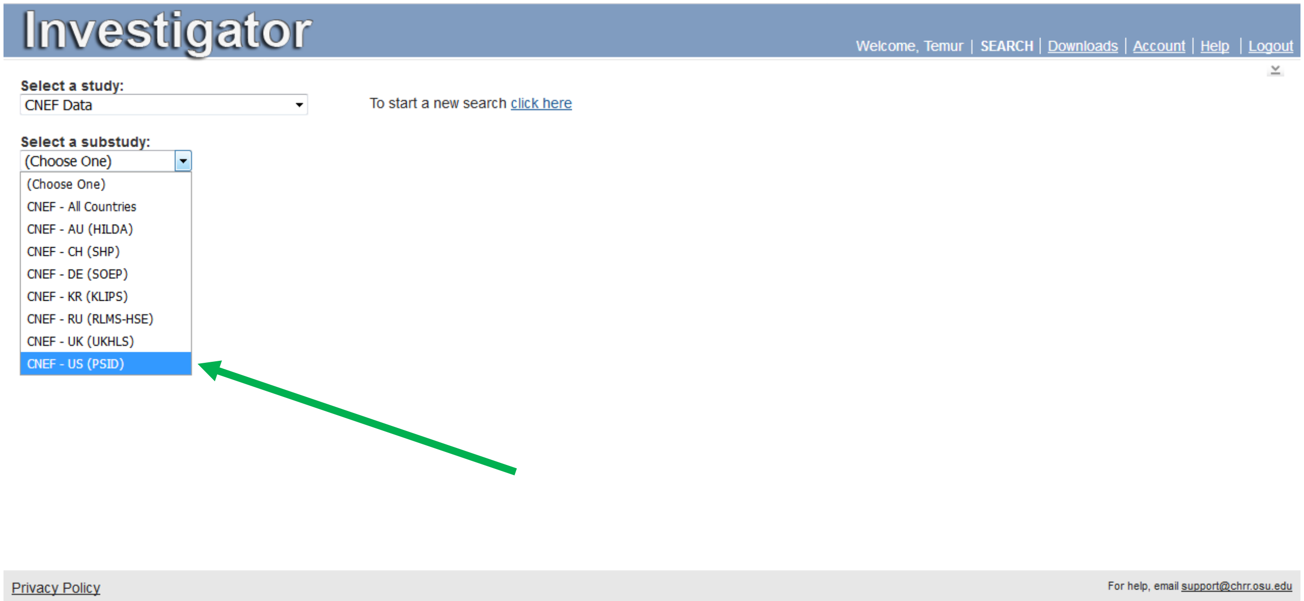
Under the individual variable data access, users may employ Investigator's "shopping basket" technology to select a set of variables for each CNEF country. This option has the advantage that users select only variables they actually need. The individual variable access also provides users with more flexibility and therefore increases the probability they will use the data.

The remainder of this document presents images of the Investigator interface. The difference between "Browse" and "Data Access" is in the access of the data, and will not affect the overall experience for the user. "Browse" level of access lets users explore and see the richness of the CNEF data, while not giving them access to the underlying individual data.

In the image below, you can see how the administrator of CNEF-Investigator may see both browse-only "CNEF" and data access "CNEF data" parts of Investigator.


Investigator
Welcome, Temur | SEARCH | Downloads | Account | Help | Logout
Select a study:
(Choose One)
(Choose One)
CNEF
CNEF Data
Consumer Finance Monthly
Ohio Longitudinal Data Archive - Metadata
Privacy Policy
For help, email support@chrr.osu.edu

After signing into Investigator, a user selects the country file they will browse;



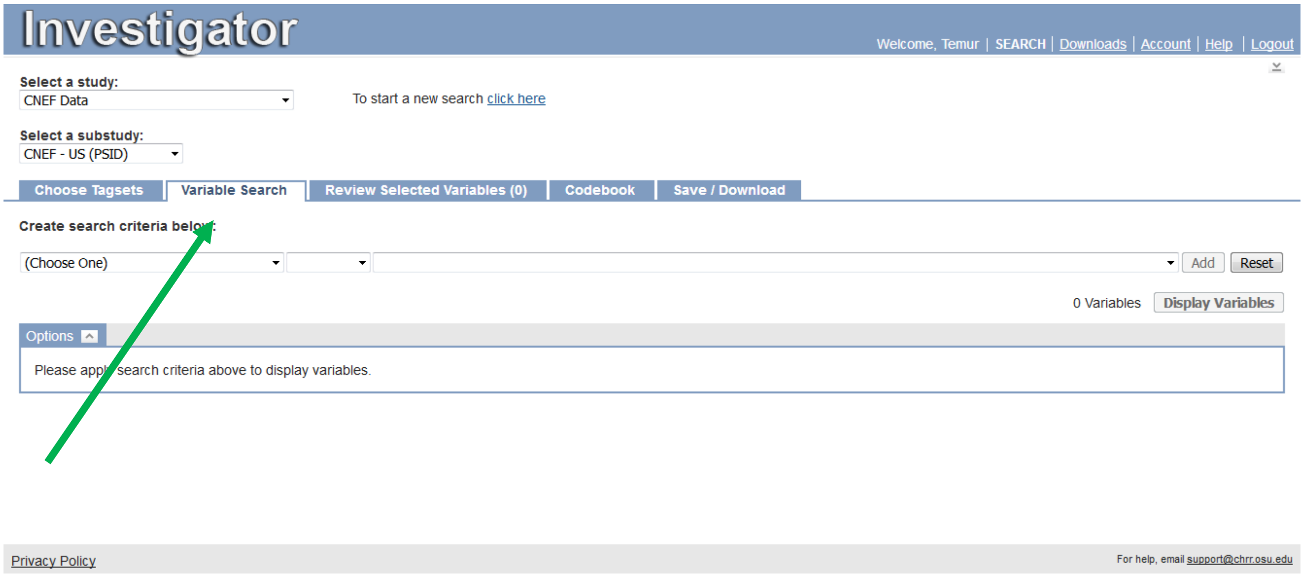
Select a study: CNEF Data

To start a new search click here

Select a substudy: (Choose One)

For help, email support@chrr.osu.edu

chooses the action; in Browse mode, users may only search the data and Codebook;



Select a study: CNEF Data

To start a new search click here

Select a substudy: CNEF - US (PSID)

Create search criteria below:

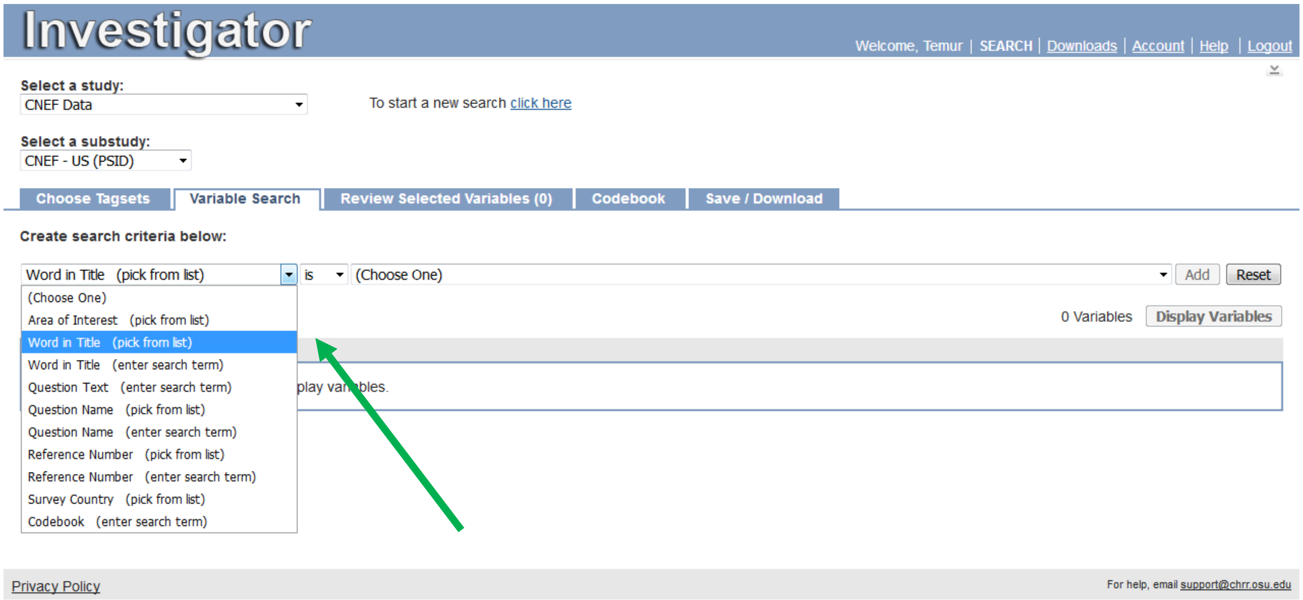
(Choose One)

0 Variables

Please apply search criteria above to display variables.

For help, email support@chrr.osu.edu

how to search for data of interest;


Investigator
Welcome, Temur | SEARCH | Downloads | Account | Help | Logout
Choose Tagsets
Variable Search
Review Selected Variables (0)
Codebook
Save / Download
Word in Title (pick from list)
is
(Choose One)
Add
Reset
(Choose One)
Area of Interest (pick from list)
Word in Title (pick from list)
Word in Title (enter search term)
Question Text (enter search term)
Question Name (pick from list)
Question Name (enter search term)
Reference Number (pick from list)
Reference Number (enter search term)
Survey Country (pick from list)
Codebook (enter search term)
0 Variables
Display Variables
Privacy Policy

Select a study: CNEF Data

To start a new search click here

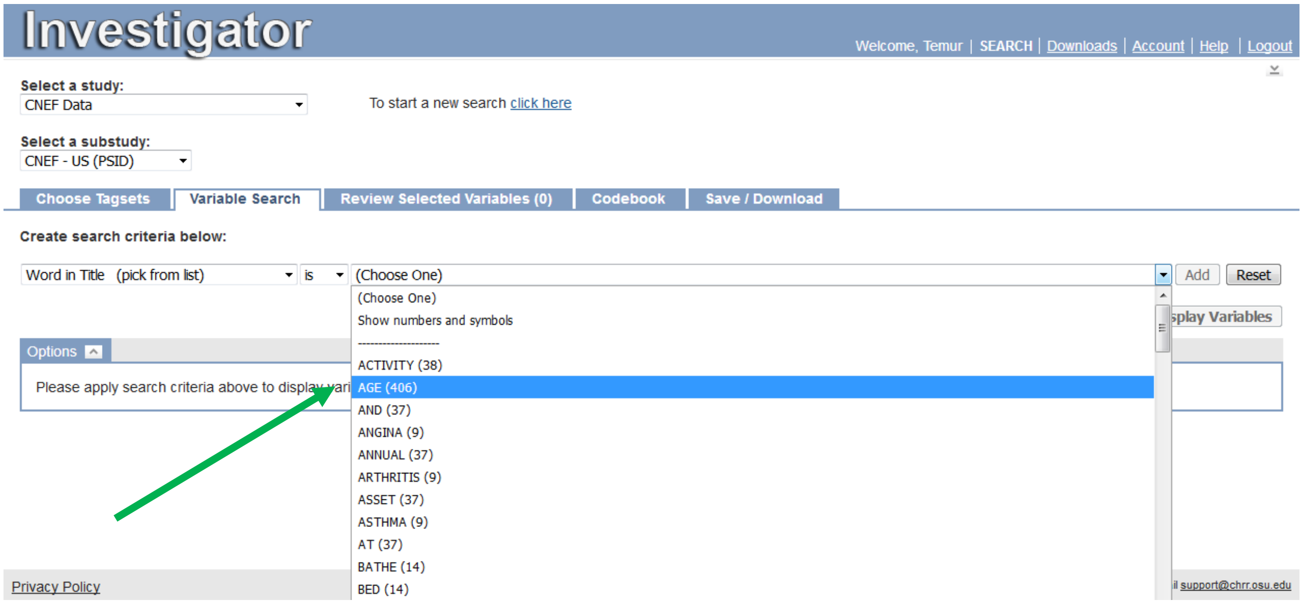
Select a substudy: CNEF - US (PSID)

Create search criteria below:

play variables.

For help, email support@chrr.osu.edu

Example: using a keyword that identifies the data of interest;



Select a study: CNEF Data

To start a new search click here

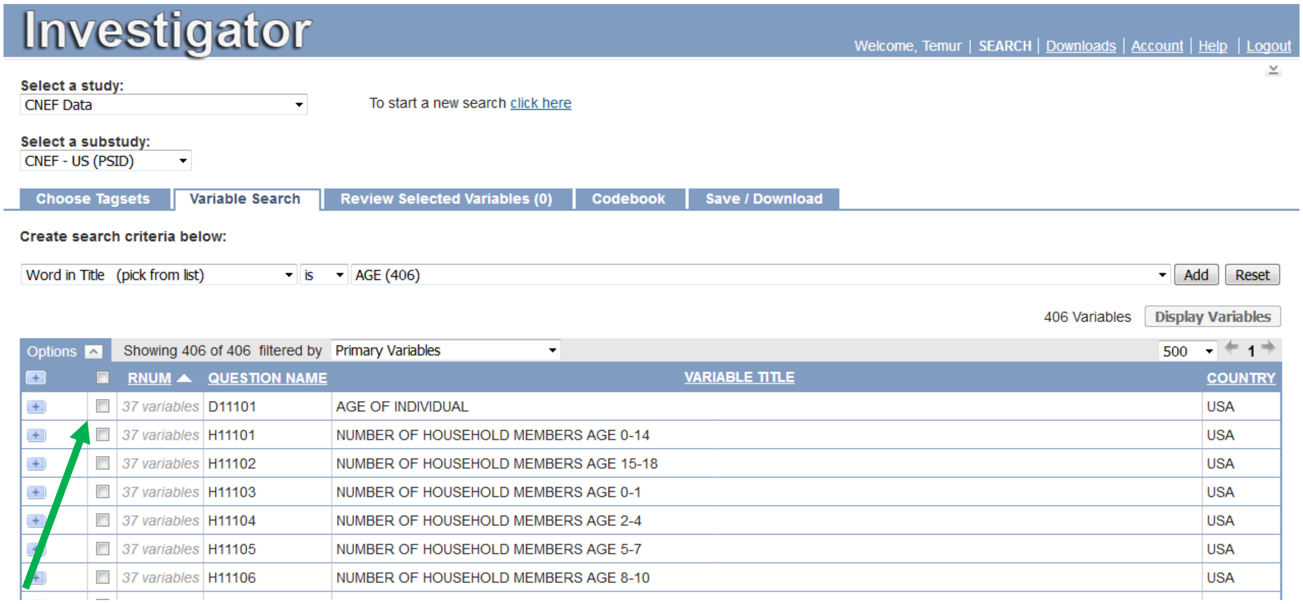
Select a substudy: CNEF - US (PSID)

Create search criteria below:

Please apply search criteria above to display vari

il support@chrr.osu.edu

within that set, the user picks the specific variable;



Select a study: CNEF Data

To start a new search click here

Select a substudy: CNEF - US (PSID)

Create search criteria below:

Word in Title (pick from list) is AGE (406)

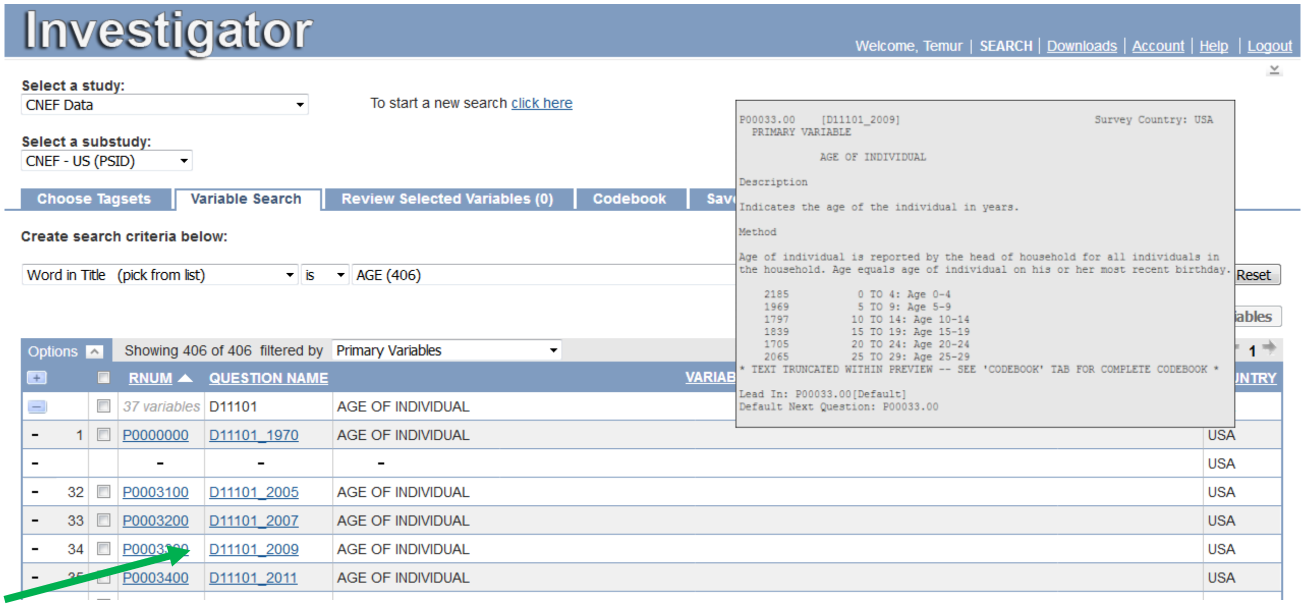
406 Variables

Showing 406 of 406 filtered by Primary Variables   500   1

	□	RNUM ▲	QUESTION NAME	VARIABLE TITLE	COUNTRY
+	□	37 variables	D11101	AGE OF INDIVIDUAL	USA
+	□	37 variables	H11101	NUMBER OF HOUSEHOLD MEMBERS AGE 0-14	USA
+	□	37 variables	H11102	NUMBER OF HOUSEHOLD MEMBERS AGE 15-18	USA
+	□	37 variables	H11103	NUMBER OF HOUSEHOLD MEMBERS AGE 0-1	USA
+	□	37 variables	H11104	NUMBER OF HOUSEHOLD MEMBERS AGE 2-4	USA
+	□	37 variables	H11105	NUMBER OF HOUSEHOLD MEMBERS AGE 5-7	USA
+	□	37 variables	H11106	NUMBER OF HOUSEHOLD MEMBERS AGE 8-10	USA

For each variable, users can choose to view the data described in three ways:

Numerical frequencies (single country, given year);


Investigator
Welcome, Temur | SEARCH | Downloads | Account | Help | Logout
Choose Tagsets
Variable Search
Review Selected Variables (0)
Codebook
Save
Reset
Options

Select a study: CNEF Data

To start a new search click here

Select a substudy: CNEF - US (PSID)

Create search criteria below:

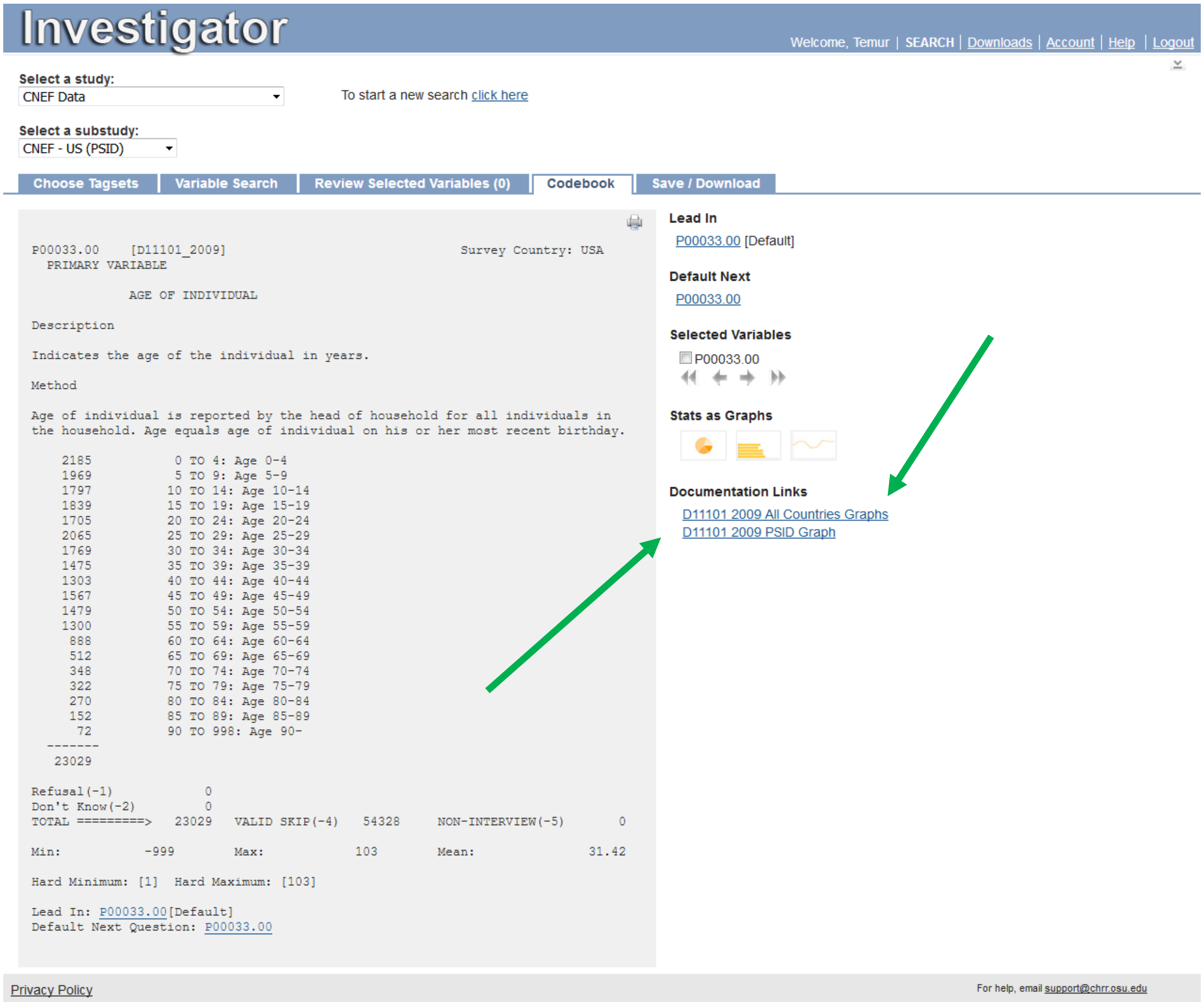
Word in Title (pick from list) is AGE (406)

Showing 406 of 406 filtered by Primary Variables   1

```
P00033.00     [D11101_2009]                              Survey Country: USA
  PRIMARY VARIABLE

             AGE OF INDIVIDUAL

Description

Indicates the age of the individual in years.

Method

Age of individual is reported by the head of household for all individuals in
the household. Age equals age of individual on his or her most recent birthday.

    2185           0 TO 4: Age 0-4
    1969           5 TO 9: Age 5-9
    1797          10 TO 14: Age 10-14
    1839          15 TO 19: Age 15-19
    1705          20 TO 24: Age 20-24
    2065          25 TO 29: Age 25-29
* TEXT TRUNCATED WITHIN PREVIEW -- SEE 'CODEBOOK' TAB FOR COMPLETE CODEBOOK *

Lead In: P00033.00[Default]
Default Next Question: P00033.00
```

		□	RNUM ▲	QUESTION NAME	VARIAB	NTRY
−		□	37 variables	D11101	AGE OF INDIVIDUAL	
-	1	□	P0000000	D11101_1970	AGE OF INDIVIDUAL	USA
-			-	-	-	USA
-	32	□	P0003100	D11101_2005	AGE OF INDIVIDUAL	USA
-	33	□	P0003200	D11101_2007	AGE OF INDIVIDUAL	USA
-	34	□	P0003300	D11101_2009	AGE OF INDIVIDUAL	USA
-	35	□	P0003400	D11101_2011	AGE OF INDIVIDUAL	USA

Graph of distribution – single country and all CNEF countries


Investigator
Welcome, Temur | SEARCH | Downloads | Account | Help | Logout
Choose Tagsets
Variable Search
Review Selected Variables (0)
Codebook
Save / Download

Select a study: CNEF Data

To start a new search click here

Select a substudy: CNEF - US (PSID)

```
P00033.00    [D11101_2009]                                  Survey Country: USA
  PRIMARY VARIABLE

             AGE OF INDIVIDUAL

Description

Indicates the age of the individual in years.

Method

Age of individual is reported by the head of household for all individuals in
the household. Age equals age of individual on his or her most recent birthday.

    2185          0 TO 4: Age 0-4
    1969          5 TO 9: Age 5-9
    1797         10 TO 14: Age 10-14
    1839         15 TO 19: Age 15-19
    1705         20 TO 24: Age 20-24
    2065         25 TO 29: Age 25-29
    1769         30 TO 34: Age 30-34
    1475         35 TO 39: Age 35-39
    1303         40 TO 44: Age 40-44
    1567         45 TO 49: Age 45-49
    1479         50 TO 54: Age 50-54
    1300         55 TO 59: Age 55-59
     888         60 TO 64: Age 60-64
     512         65 TO 69: Age 65-69
     348         70 TO 74: Age 70-74
     322         75 TO 79: Age 75-79
     270         80 TO 84: Age 80-84
     152         85 TO 89: Age 85-89
      72         90 TO 998: Age 90-
  -------
   23029

Refusal(-1)             0
Don't Know(-2)          0
TOTAL =========>    23029   VALID SKIP(-4)    54328     NON-INTERVIEW(-5)       0

Min:            -999        Max:             103        Mean:               31.42

Hard Minimum: [1]  Hard Maximum: [103]

Lead In: P00033.00[Default]
Default Next Question: P00033.00
```

Lead In

P00033.00 [Default]

Default Next

P00033.00

Selected Variables

□ P00033.00

Stats as Graphs

Documentation Links

D11101 2009 All Countries Graphs

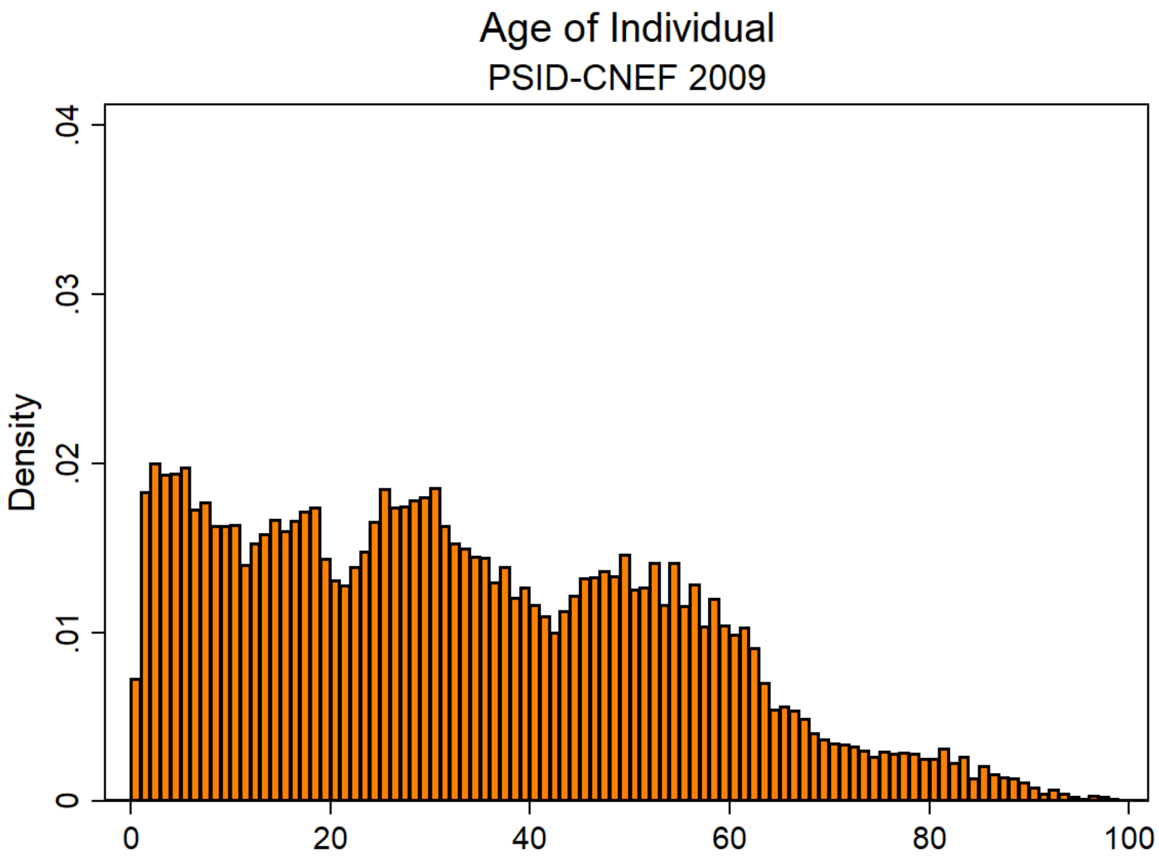
D11101 2009 PSID Graph

Privacy Policy

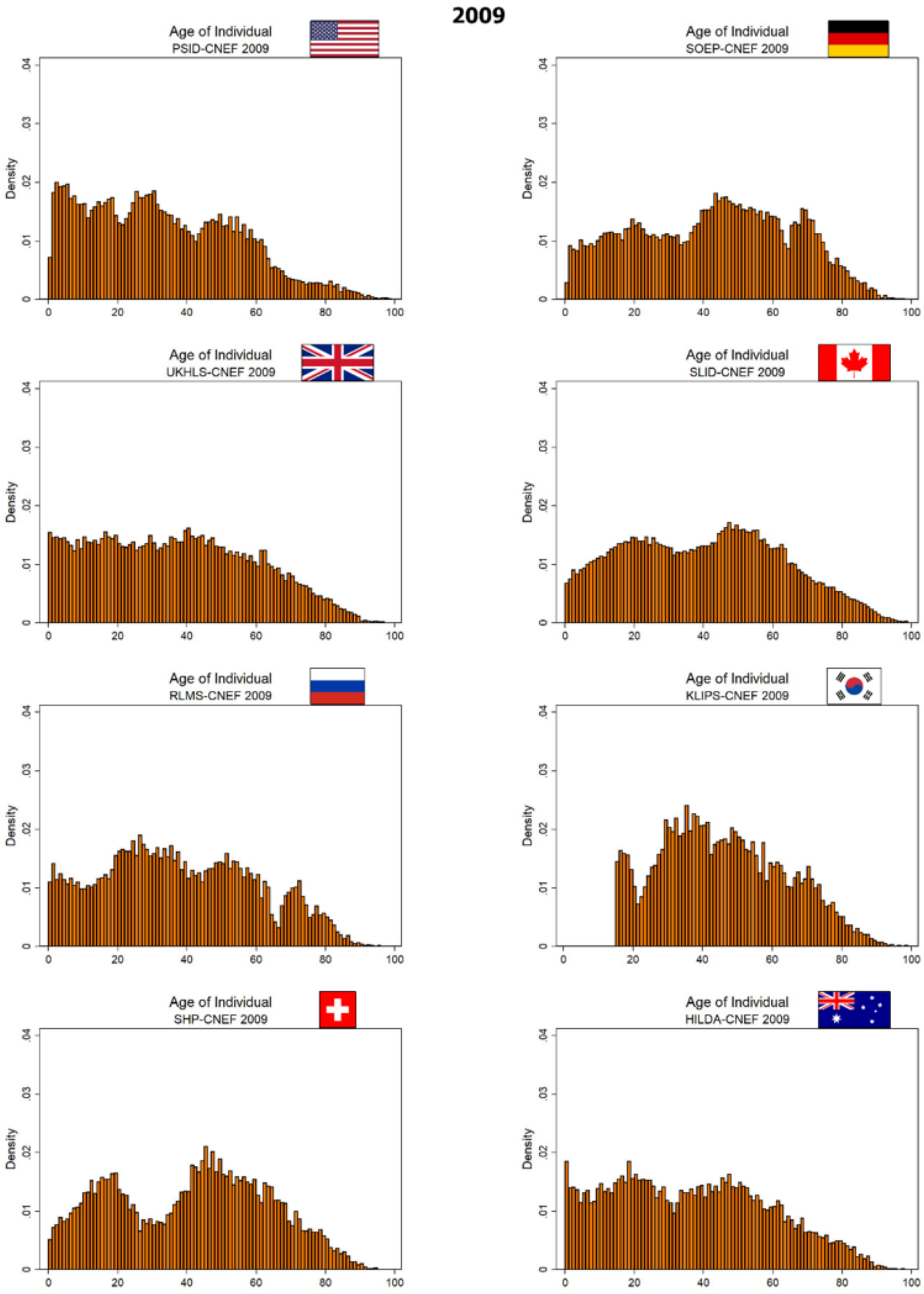
For help, email support@chrr.osu.edu

Note that we are currently adding the JHPS-CNEF data to the Investigator platform. Currently all of the “All Countries” figures plot distributions for only 8 countries.

Single country



All countries



Users can similarly browse the distributions of other variables, either for a single country, year-by-year, or for all 8 (soon 9) CNEF countries.

Users authorized to download data may select variables, create a shopping basket, and download the selected data. The system creates a raw data file plus command files in several formats (SPSS, SAS, Stata, R) that users can use to read the data.

As noted above – only the CNEF-parent institution decides whether to let users Download access. The CNEF parent institution sets the procedures by which they authorize users. As in the past, CNEF works closely with each CNEF partner to implement and monitor proper access to the data.

Appendix

Below we reproduce selected material from CHRR's security documentation. Interested readers may request more information regarding CHRR security policy and procedures by contacting nicki.stassen@chrr.osu.edu.

CHRR INFORMATION SECURITY POLICY

Title: CHRR Information Security Policy
Version: 1.2.0

1.0 Purpose

The purpose of this policy is to document the CHRR information security program and the security policies and procedures in place on CHRR information systems. CHRR is bound by laws and regulations which require that security to be applied information system wide at an enterprise level. The CHRR information security program's purpose is to maintain compliance with those laws and regulations and protect the availability, privacy, and confidentiality of all data in CHRR information systems.

2.0 CHRR Information Security Program

CHRR maintains an enterprise security program for all components of its information systems which is compliant with NIST 800-53, revision 4. CHRR's security program is based on a risk management framework which addresses security control selection based on a FIPS 199 worst-case impact analysis.

CHRR information systems are considered 'Moderate' under the NIST impact categorization system. Therefore CHRR has implemented the applicable security controls under the moderate baseline from the NIST Special Publication 800-53, revision 4. The security program covers the 18 operational, managerial, and technical NIST control families.

CHRR also ensures that all cryptographic operations within its information systems complies with Federal Information Processing Standard (FIPS) Publication 140-2.

CHRR also maintains a HIPAA Security Rule compliant environment for projects, contracts, or data sharing agreements which require CHRR to act as a health clearinghouse for Electronic Protected Health Information (EPHI).

3.1 CHRR Information Security Policy

CHRR maintains multiple security policies within its information systems. The policy which applies to a given information system component is depended upon which data resides on or is processed by the component. Each section in this policy will include a scope which discusses the policy application.

3.2 NIST 800-53 Security Policy

CHRR information systems are considered ‘Moderate’ under the NIST impact categorization system. Therefore CHRR has implemented the applicable security controls under the moderate baseline from the NIST Special Publication 800-53, revision 4. CHRR’s information security policies cover the following controls:

Control Family	Identifie	Clas
Access Control	AC	Technical
Awareness and Training	AT	Operational
Audit and Accountability	AU	Technical
Security Assessment and Authorization	CA	Management
Configuration Management	CM	Operational
Contingency Planning	CP	Operational
Identification and Authentication	IA	Technical
Incident Response	IR	Operational
Maintenance	MA	Operational
Media Protection	MP	Operational
Physical and Environmental Protection	PE	Operational
Planning	PL	Management
Personnel Security	PS	Operational
Risk Assessment	RA	Management
System and Services Acquisition	SA	Management
System and Communications Protection	SC	Technical
System and Information Integrity	SI	Operational
Program Management	PM	Management

CHRR maintains policy and procedure documents for each respective control family which discusses the implementation of the security controls in detail.

The combined documentation containing CHRR’s policies and procedures is known as the “*CHRR Security Manual*”.

3.1.1 Scope

CHRR implements its NIST 800-53 security policy on all components of its information systems. This includes systems that may be covered by another information security policy at CHRR.

3.2 HIPAA Security Policy

CHRR is required by law to comply with the Health Insurance Portability and Accountability Act (HIPAA) which includes the HIPAA Security Rule safeguards for all Electronic Protected Health Information (EPHI) in its information systems. Therefore CHRR has implemented the security safeguards required for compliance. CHRR's information security policies cover the security safeguards:

HIPAA Standard	Regulation
Administrative Safeguards	45 CFR § 164.308
Physical Safeguards	45 CFR § 164.310
Technical Safeguards	45 CFR § 164.312
Organizational Requirements	45 CFR § 164.314
Policies, Procedures and Documentation Requirements	45 CFR § 164.316

CHRR maintains a document titled "*CHRR HIPAA Compliance*" which discusses the implementation of the security controls in detail.

3.2.1 Scope

CHRR implements its HIPAA security policy on all components of its information systems which store or process EPHI.

4.1 References

a. NIST Special Publication 800-53 Revision 4 (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf)
b. FIPS 140-2 (http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf)
c. FIPS 199 (http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf)
d. HIPAA Security Rule (http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf)
e. HIPAA Privacy Rule (http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf)
f. CHRR Security Manual
g. CHRR HIPAA Compliance

5.0 Approval

Approved by:
Name: Nick Ramser
Position: CHRR Assistant Director of IT
Date: 6/2018
Name: Nicki Stassen
Position: CHRR Associate Director
Date: 6/2018

CHRR Security Overview

Security Framework

3 CHRR follows the NIST 800-53 rev 4 moderate baseline security framework. This framework is comprised of 18 control "families", and the moderate baseline contains 159 individual controls. The NIST 800-53 rev 4 covers all aspects of security, including:

- **3.1** Access Control
- **3.2** Audit and Accountability
- **3.3** Awareness and Training
- **3.4** Configuration Management
- **3.5** Contingency Planning
- **3.6** Identification and Authentication
- **3.7** Incident Response
- **3.8** Maintenance
- **3.9** Media Protection
- **3.10** Personnel Security
- **3.11** Physical and Environmental Protection
- **3.12** Planning
- **3.13** Program Management
- **3.14** Risk Assessment
- **3.15** Security Assessment and Authorization
- **3.16** System and Communication Protection
- **3.17** System and Information Integrity
- **3.18** System and Services Acquisition

4 CHRR personnel goes through yearly security training, and several IT staff hold IT security certifications.

5 CHRR is audited regularly by third party auditors against the NIST 800-53 framework.

6 CHRR dedicates substantial funds each year toward security.

IT Security Infrastructure

4 CHRR utilizes enterprise level firewall appliances, currently Juniper SRX firewall appliances, which provide context-aware firewall capabilities, comprehensive real-time threat defense, and highly secure communication mechanisms.

5 CHRR enforces multi-factor authentication for employees accessing the CHRR network.

6 CHRR maintains two secure data processing sites and mirrors crucial backups between the sites.

7 CHRR external services are hosted at a Tier 3 State of Ohio data center with strictly controlled security access and redundant power distribution.

8 CHRR uses Oracle enterprise as its database management system for external data services (the "Investigator").

- CHRR scans all application, database, servers, and systems on its network regularly with Nessus vulnerability scanning software to detect the presence of flaws in the system.
- CHRR employees Data Loss Prevention software and Intrusion Detection Systems on both the network (IDS) and server (HIDS).
- All security audit logs are sent to its Splunk Security information and event management (SIEM) system for log correlation, alerting, and real time monitoring.
- All endpoint devices are encrypted using FIPS 140-2 standard encryption.

Investigator Security Highlights

- Non-public Investigator accounts can only be created by designated CHRR personnel in the CHRR CSAM system.
- Non-public Investigator access is granted only by designated personnel and modifications to access is logged.
- Non-public Investigator access privileges are reviewed quarterly by CHRR staff.
- External web connections to the Investigator are available through https only.
- All connections between the Investigator and internal Oracle databases are encrypted.
- Investigator software development adheres to Configuration Management (CM), and includes peer review, Information Systems Security Officer and Change Control Board approval before production deployment.
- Investigator software is security scanned and unit tested as a part of the CM process, and development includes: SQL injection prevention, Cross-Site Request Forgery protection, Cross-Site Scripting prevention, and additional security measures.

CHRR IT Security Statement

CHRR maintains an enterprise security program for all components of its information systems which is compliant with NIST 800-53, revision 4. CHRR's security program is based on a risk management framework which addresses security control selection based on a FIPS 199 worst- case impact analysis.

CHRR information systems are considered ‘Moderate’ under the NIST impact categorization system. Therefore CHRR has implemented the applicable security controls under the moderate baseline from the NIST Special Publication 800-53, revision 4. The security program covers the 18 operational, managerial, and technical NIST control families. The included document “CHRR Information Security Policy” discusses the security program in more detail.

CHRR maintains comprehensive security procedures in its Security Manual, including, but not limited, to the following major topics.

Account Management

CHRR maintains Account Management procedures for both its internal users and external user account used in its software applications. CHRR follows the principal of Least Privilege in all parts of its information system, ensuring that access to data or systems is not granted without a proper purpose and approval. CHRR regularly reviews ACLs in its system to ensure they are correctly assigned. CHRR also maintains a full audit trail of all account logins, permission assignments, data accesses through Investigator, and administrative access. CHRR also ensures proper separation of duties and reviews all changes within the system.

Change Management

CHRR has an in depth Change Management program, in which it audits and approves all changes made within the system. CHRR maintains a Change Control Board which reviews and approves all changes prior to the change being implemented in the system. Depending on the nature of the change, security peer review, acceptance testing, and a security impact analysis may also be performed. As part of Change Management, all servers and applications in the system have a security baseline, which is enforced and reviewed for compliance during a change to ensure that security controls are not impacted by a change.

Vulnerability Scanning

CHRR scans all application, database, servers, and systems on its network regularly with vulnerability scanning software to detect the presence of flaws in the system. Any vulnerabilities found are fixed with defined timeframes based on their CVE severity. Scanning is conducted both internally and externally to ensure all systems are properly patched and secured from any known attack vectors.

Software Development

CHRR implements a waterfall software development methodology, heavily geared towards security. In preparation of production release, the Change Management process is followed, requiring peer review, security specific review and approvals from the Change Control Board as well as from the Information System Security Officer before a release is permitted.

CHRR’s Investigator software requires web security scanning and automated unit tests, with a focus towards security specific code. Additionally the software contains automated tests to ensure data integrity and quality control.

CHRR maintains a Developer Security Assessment Plan which uses the OWASP Top Ten as a guideline when testing for web application security risks. This includes, but is not limited to: Cross Site Request Forgery (CSRF) protection, SQL injection, Cross Site Scripting (XSS) and the use of NIST approved implementations of encryption algorithms.

Security specific flaws found in Investigator go through a Flaw Remediation process, requiring review of the flaw and a defined time frame of a fix based on the flaw’s severity.

Encryption and Cryptography

CHRR ensures that all cryptographic operations within its information systems complies with Federal Information Processing Standard (FIPS) Publication 140-2. All communications which send sensitive data across both internal and external networks must use encrypted protocols and use FIPS 140-2 approved algorithms and ciphers. Plain text network protocols which transmit authentication or sensitive data are forbidden by CHRR.