HCUP DATA SECURITY PLAN

The HCUP project team gives careful consideration toward achieving the balance between protection of data privacy and our nation's need for the use of data in healthcare research. The following document describes the privacy, confidentiality, and security protections in place to ensure adherence to Federal and State law as well as agreements made with Data Organizations participating in the project.

Changes to the HCUP Data Security Plan will be reported to HCUP Data Organizations.

Healthcare Cost and Utilization Project

Agency for Healthcare Research and Quality

HCUP DATA SECURITY PLAN

March 25, 2020

TABLE OF CONTENTS

I INTRODUCTION 1
II PRIVACY PROTECTION FOR DATA RECEIVED FROM HCUP PARTNERS 2
A. Statutory Data Protections 2
B. Privacy Protections for Use of HCUP Databases by AHRQ Staff and Contractors 3
III STRUCTURE OF FILES AND ACCESS TO DATA 4
A. Source Data 4
B. HCUP Intramural Databases 5
C. HCUP Data Development Files 5
D. HCUP Restricted-Access Public Release Databases 6
IV WORKING WITH CONTRACTORS 7
A. Primary Contractor 7
B. Secondary Contractors 8
C. Contractor Access to Data 8
V PROCEDURAL AND PHYSICAL PROTECTIONS 9
A. AHRQ Staff / Contractor Agreements 9
B. HCUP Data Use Agreements 9
C. Security of HCUP Data 10
D. Physical Access to Facilities 14
E. Secure Data Disposal 14

Healthcare Cost and Utilization Project

Agency for Healthcare Research and Quality

HCUP DATA SECURITY PLAN

I INTRODUCTION

The Agency for Healthcare Research and Quality's (AHRQ) mission is to produce evidence to make healthcare safer, higher quality, more accessible, equitable, and affordable, and to work within the U.S. Department of Health and Human Services and with other partners to make sure that the evidence is understood and used. AHRQ maintains the Healthcare Cost and Utilization Project (HCUP), a national resource of healthcare information that includes the largest collection of hospital discharge data in the United States. HCUP databases support health services research that will improve the quality of healthcare and promote evidence-based decision making. The information is used for research on a broad range of policy and health issues including cost and quality of health services, access to healthcare programs, medical practice patterns, and outcomes of treatments. The HCUP project team gives careful consideration toward achieving the balance between protection of data privacy and our nation's need for the use of data in healthcare research. To that end, this document describes the privacy, confidentiality, and security protections in place to ensure adherence to Federal and State law as well as agreements made with Data Organizations participating in the project. The terms "Data Organization" and / or "HCUP Partners" refer to the State government

agencies, hospital associations, and private data organizations that contribute administrative health data to the project, making the creation of HCUP databases possible.

Under the Healthcare Research and Quality Act of 1999, 42 U.S.C. §299 et seq., AHRQ is authorized to collect data for the purposes of enhancing the quality, appropriateness, and effectiveness of health services, and improving access to health services. AHRQ fulfills this mission in part by engaging in public health activities, such as promoting improvements in clinical and health system practices, including practices aimed at the prevention of disease and other health conditions.[1] For example, AHRQ is authorized to develop and disseminate information to consumers and professionals regarding healthcare quality, technology assessment, and the scientific evidence supporting health practices.[2] Congress has also authorized AHRQ to undertake initiatives that advance public and private efforts to improve healthcare quality nationwide.[3]

II PRIVACY PROTECTION FOR DATA RECEIVED FROM HCUP PARTNERS

A. Statutory Data Protections

AHRQ has used discharge data for research since the early 1980s, subject to its statutory privacy protections.[4] The release of information collected, assembled, or used by AHRQ and its contractors is restricted by the Agency's confidentiality statute that prohibits the use or release, without appropriate consent, of data that identify individuals who, or organizations that provided the data or are described in the data. Thus, AHRQ is obligated to protect data privacy for each data set that Data Organizations supply to HCUP. Specific requirements for use of data are stipulated in a detailed Memorandum of Agreement (MOA) that is established between AHRQ and each participating Data Organization. Among other things, each MOA includes

[1] 42 U.S.C. §299(b).
[2] 42 U.S.C. §299a(a).
[3] 42 U.S.C. §299b-1, 299b-2, 299b-3.
[4] Section 944(c) of the Public Health Service Act (42 U.S.C. 299c-3(c)).

requirements for protecting health data as mandated by State or other law. In some cases, these laws may be more protective of privacy than the HIPAA Privacy Rule.

AHRQ interprets its own confidentiality statute to apply to any person with access to data collected by AHRQ or in connection with a project that AHRQ has funded. By signing HCUP's data use agreement (DUA), a researcher is agreeing to comply with all of the conditions and restrictions contained in that agreement. The researcher is also acknowledging that violations of the HCUP DUA constitute violation of AHRQ's statutory confidentiality provisions and may result in civil, and possibly criminal, penalties.

The HIPAA Privacy Rule protects individually identifiable health information by establishing conditions for its use and disclosure by "covered entities." Disclosure of protected health information from covered entities for the purpose of research is allowed by the Privacy Rule under section 164.502 and 164.512(i). AHRQ and most Data Organizations participating in HCUP are not covered entities because they do not fit the definition of (1) a health plan, (2) a healthcare clearinghouse, or (3) a healthcare provider that electronically transmits health information in connection with standard financial or administrative transactions; however, AHRQ data policies are generally consistent with the requirements of the HIPAA Privacy Rule.

B. Privacy Protections for Use of HCUP Databases by AHRQ Staff and Contractors

AHRQ maintains a set of policies and procedures for protecting HCUP data privacy. Contractors working with AHRQ researchers are required to submit a security plan outlining the privacy protections they will use in handling HCUP data.

Each staff member, contractor, and guest researcher[5] given access to any HCUP data is required to review guidelines for protection of HCUP data and receive training in privacy, security, and confidentiality.[6] In addition, staff, contractors, and guest researchers must sign the AHRQ Staff / Contractor Agreement and an HCUP DUA specific for State and Nationwide databases (see section III for descriptions of the databases) before being given access to data.

III STRUCTURE OF FILES AND ACCESS TO DATA

AHRQ requests data from participating Data Organizations to develop files for a number of HCUP products and to facilitate internal AHRQ research and public health efforts. AHRQ's Primary Contractor is responsible for obtaining statewide discharge data and processing those data into the uniformly formatted HCUP databases.

A. Source Data

Source data refers to the files received from participating Data Organizations (HCUP Partners) in their original format. AHRQ's Primary Contractor is the sole holder of source data supplied by participating Data Organizations. Unformatted source data received by the Primary Contractor are not released to AHRQ or any of the other HCUP-related contractors. Source data may not be used by AHRQ or its Primary Contractor for purposes other than the development of HCUP databases as described in the HCUP Memorandum of Agreement (MOA) executed with each participating Data Organization.

HCUP requests that the Data Organization providing source data will encrypt, assign a unique code, or remove all direct patient identifiers, such as medical record numbers or Social Security Numbers, before supplying the data to HCUP. If the Data Organization is unable to

---

[5] "Guest researcher" is a term used by AHRQ to describe academic scientists, Federal employees, or graduate/Ph.D. level students who have been authorized to use Agency resources to further their research or training. For specific approved projects, guest researchers are sometimes given access to HCUP intramural data under supervision and guidance of a member of the HCUP team.

[6] The online HCUP Data Security and Confidentiality Course for AHRQ staff and contractors.

obscure personal identifiers, the Primary Contractor will immediately encrypt the identifiers and destroy all copies of the original file that contain the supplied identifiers.

B. HCUP Intramural Databases

Intramural databases are AHRQ versions of data used by AHRQ staff, their contractors, and guest researchers for activities related to research, public health, and the development of HCUP tools, products, and reports. These databases are also used in producing aggregate statistics for technical support to other Federal agencies, for the development of State- and community-level discharge statistics used in HCUPnet and Fast Stats (with permission from Data Organizations); for the maintenance and development of AHRQ Quality Indicators; and in the National Healthcare Quality and Disparities Report (QDR), and their derivative products. HCUP Intramural databases differ from the restricted-access public release databases (described below) because they may contain data elements that are not released outside of AHRQ.

Intramural databases are available only to authorized AHRQ staff, their contractors, and guest researchers, who must abide by statutory limits on disclosure[7] and the special restrictions imposed under AHRQ and HCUP data use agreements. Access to the HCUP Intramural databases must be approved by the HCUP Project Director or Manager and use of these files are reported to HCUP Partners in the *HCUP Annual Activities Report and HCUP Overview Binder.*

C. HCUP Data Development Files

AHRQ also maintains Data Development (DD) files containing person-level information that is not included in the HCUP Intramural databases, such as full dates (e.g., admission and discharge, date of birth), source-supplied encrypted identifiers, and other indirect patient and physician identifiers. Starting with data year 2012, the five-digit ZIP Codes are not separated into DD files unless required by HCUP Partners.

[7] Section 944(c) of the Public Health Service Act (42 U.S.C. 299c-3(c)).

DD files can be used only for specific, restricted purposes. DD files may be used to address problems discovered after construction of HCUP databases; and by AHRQ researchers and their contractors to develop analytic files for specific research projects. A proposed use of DD files must undergo an internal review and be given special permission by the HCUP Project Director or Manager.

D. HCUP Restricted-Access Public Release Databases

HCUP produces a number of databases for use by researchers outside of AHRQ. These "restricted-access public release" databases include the National (Nationwide) Inpatient Sample (NIS), the Kids' Inpatient Database (KID), the Nationwide Ambulatory Surgery Sample (NASS), the Nationwide Emergency Department Sample (NEDS), and the Nationwide Readmissions Database (NRD). Restricted-access public release versions of the State Inpatient Databases (SID), the State Ambulatory Surgery and Services Databases (SASD), and the State Emergency Department Databases (SEDD) are also available for some States. Release of the HCUP databases to researchers outside of AHRQ has always been governed by detailed HCUP data use agreements. HCUP data use agreements contain all the features that would be required for a covered entity to release a limited data set under the HIPAA Privacy Rule. Restricted-access public release databases are made available to both internal and external data users only after completion of required training[8] and submission of a signed HCUP DUA. In addition, before restricted-access public release State-level databases are released (SID, SASD, and SEDD), AHRQ reviews the statement of intended use provided by the applicant to ensure that the planned use of the data is consistent with HCUP policies and with Partner and HCUP data use requirements.

HCUP Partners that make available their State-level restricted-access public release files specify the data elements that AHRQ may include. Although HCUP Partners may permit the release of certain identifiers, it is AHRQ's policy that HCUP's restricted-access public release

[8] HCUP Data Use Agreement training at www.hcup-us.ahrq.gov.

files may not contain individual identifiers, full dates, or data elements that must be excluded from a limited data set as defined under HIPAA.[9] If the data organization concludes that confidentiality should also be provided for its institutions, (e.g., hospitals), institutional identifiers are encrypted or removed as well.

IV WORKING WITH CONTRACTORS

Much of the work to create and analyze HCUP databases, tools, products, and reports is accomplished through contract services. Contractors are engaged to conduct essential functions of the HCUP project. The "Primary Contractor" is responsible for core components of the HCUP project and tasks such as data acquisition, data processing, database creation, documentation, and special analyses. "Secondary Contractors" are engaged to perform other work that contributes to the HCUP project, such as research expertise, maintenance, development, validation of HCUP products and tools, and data programming for research projects conducted by AHRQ staff.

A. Primary Contractor

The HCUP Project Director or Manager oversees and directs all activities performed under contract by the Primary Contractor. This includes obtaining statewide discharge data and processing it into the uniformly formatted HCUP databases. Using the completed and delivered HCUP databases, the Primary Contractor provides additional support to AHRQ for other HCUP software tools, products, research, and reports developed for the project. This includes maintaining multiple HCUP tools (such as Clinical Classifications Software (CCS), Comorbidity Software, AHRQ's Cost-to-Charge Ratios, etc.), developing new tools, developing HCUP Statistical Briefs, Fast Stats, HCUPnet, and conducting data analysis for AHRQ reports to external audiences (such as the National Healthcare Quality and Disparities Report).

[9] As defined in 45 C.F.R. §164.514(e)(2).

IBM® Watson Health™ (Watson Health) is AHRQ's Primary Contractor responsible for the core work of developing, maintaining, and expanding the HCUP databases. Watson Health also works with the subcontractors, Social & Scientific Systems (SSS), M.L. Barrett, Inc., RAND Corporation, Ohio State University, and others to develop, maintain, distribute, and analyze the HCUP databases on behalf of AHRQ.

B. Secondary Contractors

AHRQ Project Managers are assigned to oversee and direct all activities performed under independent contract by Secondary Contractors that utilize HCUP data. These activities are directed within AHRQ and are limited to specific AHRQ project objectives. This type of work includes data programming for AHRQ staff research projects and producing aggregate statistics for other Federal agencies and other organizations at AHRQ's direction. It also includes activities such as the maintenance, refinement, expansion (i.e., development of new measures and tools), and validation of the AHRQ Quality Indicators. The creation of some HCUP tools have been accomplished by Secondary Contractors, which perform work on tasks such as the AHRQ Quality Indicators (QIs), the online HCUPnet statistical query system, and the online QR/DRnet query system.

C. Contractor Access to Data

Contractors have different levels of access to HCUP data, and all data access is limited to the level required to accomplish AHRQ-specified work. Contracts between the Federal government and HCUP-related contractors contain sections governing the authorized use of data under the contracts. These sections restrict the publication and dissemination of material derived from contracts, and they specify that the contractors have no rights to data collected or developed under the contracts. The contracts also contain provisions for penalty and debarment from Federal contracting should these restrictions be violated. All contractors maintain responsibility for assuring compliance with contractual requirements and protection of data. All contractors assure that their subcontractors are held to the same level of responsibility for compliance with contractual requirements and protection of data.

V PROCEDURAL AND PHYSICAL PROTECTIONS

A. AHRQ Staff / Contractor Agreements

AHRQ staff, their contractors, and guest researchers with access to HCUP data are required to sign the AHRQ Staff / Contractor Agreement that specifies privacy protections and restrictions placed on use of the data. They are also required to receive privacy, security, and confidentiality training on an annual basis that includes information on the appropriate (and inappropriate) use of HCUP data. The Staff / Contractor Agreements prohibit AHRQ, contractor staff, and guest researchers from giving access to HCUP files, providing confidential information derived from such files, or otherwise sharing such information with unauthorized individuals. The Agreement also prohibits use of the data for any purpose other than AHRQ-related work, and it prohibits access and use of data after employment has been terminated.

B. HCUP Data Use Agreements

All persons given access to HCUP databases are required to sign an HCUP Data Use Agreement and complete the online DUA training before being given access to data. These agreements place limitations on how HCUP data may be used. Criminal and civil penalties exist for violation of the Federal statute.[10]

Users must agree, among other things, to use the data for research and statistical purposes only and to make no attempt to identify individuals. In addition, users must agree not to identify establishments directly or by inference in published or disseminated material.

[10] Violation of the AHRQ Confidentiality Statute may be subject to a civil penalty of up to $14,140 under 42 U.S.C. 299c-3(d). Deliberately making a false statement about this or any matter within the jurisdiction of any department or agency of the Federal Government violates 18 U.S.C. § 1001 and is punishable by a fine, up to five years in prison, or both. Violators of the HCUP DUA may also be subject to penalties under state confidentiality statutes that apply to these data for particular states.

C. Security of HCUP Data

The HCUP Information Technology (IT) systems are in conformance with the standards set forth by the Federal Information Security Management Act (FISMA) and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy.* HCUP IT systems hosted by the Primary Contractor have received security authorizations to operate from the Federal Government and are compliant with all E-Government Act (P.L. 107-347), Office of Management and Budget (OMB) mandates, Federal Information Processing Standards (FIPS), and additional applicable NIST guidance. This guidance includes, but is not limited to FIPS 199, FIPS 200, NIST SP 800-18, NIST SP 800-30, NIST SP 800-37, NIST SP 800-53, NIST SP 800-53A, and NIST SP 800-60. All NIST and FIPS documentation can be found at the NIST website at www.csrc.nist.gov.

Data are protected by stringent security measures throughout the data life cycle, whether stored on media or electronically. In general, media (such as tapes, cartridges, disks, DVDs, and other storage devices), reports, listings, and any other material containing sensitive information are kept in locked files, locked offices, or controlled-access storage rooms. Data materials may be removed from storage by authorized project staff, but those materials must remain under the staff member's direct supervision. All materials are locked away at the end of each working day or whenever not in immediate use. Electronic files may only reside on secure authorized computer systems and be accessed through a secure network or encrypted Virtual Private Network (VPN). Critical backup files for disaster recovery are encrypted and housed at a secure, offsite location. Access to secure storage locations is controlled by the HCUP Project Director or Manager, contractor Project Directors, and/or a delegate, as appropriate to each site.

The following is a brief outline of HCUP data security protections:

Procedure	Source Data	Intramural Databases	Data Development Files	Restricted-Access Public Release Databases
General Measures				
Use	* Used by Primary Contractor for HCUP file creation and verification on dedicated secure servers * Restrictions on use per AHRQ HCUP policy, the AHRQ Staff-Contractor Agreement and HCUP DUAs	* Used by AHRQ researchers or their contractors for research, public health, and the development of HCUP tools, products, and reports * Restrictions on use per AHRQ HCUP policies, the AHRQ Staff-Contractor Agreement and HCUP DUAs	* Used by AHRQ researchers or their contractors for research, public health, and the development of HCUP tools, products, and reports * Restrictions on use per AHRQ HCUP policy, the AHRQ Staff-Contractor Agreement and HCUP DUAs	* Released through the HCUP Central Distributor for research, analysis and aggregate statistical reporting * Restrictions on use per HCUP DUAs
Data Access	* Data are held solely by the Primary Contractor * Access is granted only to authorized project staff	* Access for research use requires HCUP Project Director/Manager approval * Access is granted only to authorized project staff	* Access for research use requires HCUP Project Director/Manager approval * Access is granted only to authorized project staff	* Access is granted through the HCUP Central Distributor application process
Media				
Shipping	*Data may be shipped from HCUP Partner organizations to the HCUP Primary Contractor (Watson Health) according to Partner's policies and procedures. Most HCUP Partners submit data to the primary contractor via secure file	* Database files are encrypted * Data are sent via secure file transfer protocol and separately from documentation and passwords * All databases received are confirmed	* Database files are encrypted * Data are sent via secure file transfer protocol and separately from documentation and passwords * All databases received are confirmed	* Database files are encrypted * Data are delivered together with accompanying documentation to data users approved through an application process * Password is provided separately

Procedure	Source Data	Intramural Databases	Data Development Files	Restricted-Access Public Release Databases
	transfer protocol * Physical media (e.g., DVD) containing data is identified by a tracking number assigned by the originating party * Data are not shipped from the HCUP Primary Contractor unless being returned to the HCUP Partner organization * All shipments are confirmed			
Media Storage	* Media are kept in secure, limited-access rooms or locked cabinets at the Primary Contractor's work site *Media are never removed from the Primary Contractor's work site unless specifically requested by the HCUP Partner organization to return the media	* Media are kept in secure, limited-access rooms or locked cabinets * All sensitive data files must be encrypted before removal from a secure environment	* Media are kept in secure, limited-access rooms or locked cabinets * All sensitive data files must be encrypted before removal from a secure environment	* Media are kept in secure, limited-access rooms or locked cabinets
Electronic Files				
Electronic File Storage	* All HCUP computers storing source data are located in secure, limited-access rooms * Data are stored on encrypted drives	* All HCUP computers storing intramural data, are kept in secure, limited-access rooms * Data are stored on encrypted drives	* All HCUP computers storing DD data are kept in secure, limited-access rooms * Data are stored on encrypted drives	* All HCUP computers storing HCUP data are kept in secure, limited-access rooms or the data are stored on encrypted drives * Nationwide data available for download are

Procedure	Source Data	Intramural Databases	Data Development Files	Restricted-Access Public Release Databases
				stored on a secure FTP server
Access Method	* Access through dedicated secure servers or remotely via a secure (encrypted) VPN connection using identification verification, password and two-factor authentication	* Access through dedicated secure servers or remotely via a secure (encrypted) VPN connection using identification verification, password and two-factor authentication	* Access through dedicated secure servers or remotely via a secure (encrypted) VPN connection using identification verification, password and two-factor authentication	* Access is granted through the HCUP Central Distributor application process
Secure File Transfer Protocol (SFTP) Download	* HCUP Partner SFTP sites or encrypted secure mail servers are utilized to obtain data from most Data Organizations * Data are encrypted during transmission * Decryption key or password authentication is required to obtain data * Data are transferred directly to a server maintained by the Primary Contractor * Source data obtained directly through SFTP or secure mail are stored exclusively at the Primary Contractor's secure facility and never offsite	*Intramural data are obtained by AHRQ via its secure electronic file transfer site, sent by the Primary Contractor.	*Data Development files are obtained by AHRQ via its secure electronic file transfer site, sent by the Primary Contractor.	* SFTP download for dissemination of nationwide databases are purchased through the HCUP Central Distributor website * Data are encrypted during transmission and downloads require user log-in and verification process * Nationwide data available for download are stored on a SFTP server

D. Physical Access to Facilities

AHRQ and its contractors control physical access to facilities using electronic methods, security procedures, and/or personnel. Entering the AHRQ premises requires electronic screening and, for visitors, interaction with security personnel. Entrance to the Primary Contractor offices (Watson Health) requires that all visitors must first register at the reception desk, and thereafter must be escorted by a Watson Health employee.

AHRQ and contractor offices are equipped with locking storage cabinets and/or locking doors. Watson Health maintains an electronic key-card protected secure storage room for onsite archiving of data tapes, cartridges, disks, DVDs, or other storage devices and a separate key-card protected secure environment for its secure network and computer facilities. Removable disks or other storage devices with sensitive information are stored in locked cabinets or secured areas. Other contractors must employ similar procedures.

E. Secure Data Disposal

Data files will be destroyed once they are no longer required by the project. Destruction cycles vary by type of file.

At AHRQ's direction, the Primary Contractor destroys source data approximately two years after file development, and sends notification of destruction to the AHRQ Project Director or Manager. At the conclusion of the HCUP contract, all remaining source data held by the Primary Contractor will be destroyed or transferred to the next HCUP contractor (without regard to the time period said data have been in the possession of the incumbent Primary Contractor); final disposition of source data will only occur at the direction of the HCUP Project Director or Manager and with permission from the Data Organization(s).

After the Primary Contractor completes the processing of source data into the HCUP databases, and allowing sufficient time for quality control and problem investigation, the intermediate files are deleted during routine storage management. Files may remain on backup media in a secure location for a period of time until overwritten through normal backup media

rotation. The final HCUP databases are retained by the Primary Contractor for the duration of the project.

Printed output and documents containing confidential information are shredded when disposal is required. Electronic, optical, or magnetic records are securely erased or shredded to obliterate individual discharge data when disposal becomes necessary.

In the event of termination of the AHRQ contract with the Primary Contractor, AHRQ will retain the HCUP intramural, data development, and restricted-access public release databases to support longitudinal research.