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 health care 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 3, 2012

TABLE OF CONTENTS

Healthcare Cost and Utilization Project

Agency for Healthcare Research and Quality

HCUP DATA SECURITY PLAN

I INTRODUCTION

The Agency for Healthcare Research and Quality (AHRQ) is one of 12 agencies within the Department of Health and Human Services and is the lead Federal agency charged with improving the quality, safety, efficiency, and effectiveness of health care for all Americans. AHRQ maintains the Healthcare Cost and Utilization Project (HCUP), a national resource of health care 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 health care 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 health care 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 health care 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 health care 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 health care 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

[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)).

AHRQ and each participating Data Organization. Among other things, each MOA includes 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 health care clearinghouse, or (3) a health care 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

The Center for Delivery, Organization, and Markets (CDOM), HCUP's home center at 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 and contractor given access to any HCUP data is required to review guidelines for protection of HCUP data and to sign the AHRQ Staff-Contractor Agreement before access is granted. In addition to the AHRQ Staff-Contractor Agreement, staff and contractors are required to sign an HCUP DUA specific to each

restricted access public release database (see section III D. for descriptions of the NIS, SID, SASD, SEDD, KID, and NEDS databases).

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, re-identify, or remove all patient identifiers, such as medical record numbers or Social Security Numbers, before supplying the data to HCUP. If the Data Organization is unable to 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 include versions of HCUP data for use by researchers within AHRQ, and are used for activities such as 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, and (with permission from Data Organizations) for

the development of state discharge statistics used in HCUPnet http://hcup.ahrq.gov/HCUPnet.asp. HCUP Intramural databases differ from the restricted access public release databases (described below) because they are not available to researchers outside of AHRQ and may contain data elements that are not released outside of AHRQ in restricted access public release files.

Intramural databases are available only to authorized AHRQ staff, their contractors, and on-site guest workers,[5] who must abide by statutory limits on disclosure[6] 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 Officer and are reported to HCUP Partners in the *HCUP Annual Activities Report*, and accompanying project abstracts, tools, and publication lists maintained on the secure access section of the HCUP-US Website at http://www.hcup-us.ahrq.gov/partner/partner_MOA_ref.jsp. All users of HCUP Intramural Databases must receive training in privacy and security,[7] and must sign an AHRQ Staff-Contractor Agreement and HCUP DUA before being given access to data.

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 five-digit ZIP Code, full dates (e.g., admission and discharge, date of birth), source-supplied encrypted identifiers such as medical record number, and other patient and physician identifiers.

[5] "Guest workers" 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 facilities to further their research or training. For specific approved projects, guest workers are sometimes given access to HCUP intramural data under direct supervision and guidance of a member of the HCUP team, provided that the data files are used only on AHRQ premises.

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

[7] The on-line HCUP Data Security and Confidentiality Course for AHRQ staff and contractors.

DD files can be linked to the HCUP Intramural databases only for specific, restricted purposes: DD files may be used, should the need arise, to address problems discovered after construction of HCUP databases; and DD files are available, under specific, limited circumstances, to AHRQ researchers and their contractors to develop analytic files for specific research projects. A proposed use of DD files must be given special permission by the HCUP Project Officer. All users of DD files must receive training in privacy and security[8], and must sign an AHRQ Staff-Contractor Agreement and HCUP DUA before being given access to data.

D. HCUP Restricted Access Public Release Databases

HCUP produces a number of databases for use by researchers outside of AHRQ, including the Nationwide Inpatient Sample (NIS), the Kids' Inpatient Database (KID), the Nationwide Emergency Department Sample (NEDS), and versions of the State Inpatient Databases (SID), the State Ambulatory Surgery Databases (SASD), and the State Emergency Department Databases (SEDD). These databases are referred to as "restricted access public release files"; that is, they are publicly available, but only under restricted conditions. Release of the HCUP databases to researchers outside of AHRQ has always been governed by detailed HCUP data use agreements, and these data use agreements now 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 required training[9] and submission of a signed HCUP DUA. In addition, before restricted access public release state-level databases are released (SID, SASD, and SEDD), the user completes an application process to ensure that the planned use is consistent with HCUP policies and with Partner and HCUP data use requirements.

[8]The online HCUP Data Security and Confidentiality Course and the AHRQ Information Security and Privacy Awareness Training for AHRQ staff and contractors.
[9] HCUP Data Use Agreement training at http://www.hcup-us.ahrq.gov

HCUP Partners specify the data elements that AHRQ may include in their state-level restricted access public release files. Although HCUP Partners may permit the release of certain identifiers, it is AHRQ's policy that HCUP's restricted access public release files may not contain identifiers or other data elements that must be excluded from a limited data set.[10] If the data organization concludes that confidentiality should also be provided for its institutions, (e.g., hospitals), institutional identifiers are also encrypted or removed as well.

E. HCUP Software Tools and Supplemental Files

AHRQ develops and maintains various software tools and supplemental files available for use with HCUP and other administrative data to improve the ease of use and value of the databases. These resources are updated annually and are made available by download from the HCUP-US Website or by request. HCUP tools and supplemental files contain no patient-level data; however, HCUP supplemental files may contain hospital-level data designed to be used exclusively with the HCUP NIS, SID, KID, or NEDS. Use of these tools and supplemental files in association with the HCUP databases is governed by AHRQ and HCUP data use agreements.

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 such tasks 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 development and validation of HCUP products and tools, and data programming for research projects conducted by AHRQ staff.

[10] As defined in 45 C.F.R. §164.514(c)(2).

A. Primary Contractor

The HCUP Project Officer 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, 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 (such as refining CCS classifications), developing the data analysis and content for HCUP Statistical Briefs, and conducting data analysis for AHRQ reports to external audiences (such as the National Healthcare Quality Report and National Healthcare Disparities Report).

Thomson Reuters is AHRQ's Primary Contractor responsible for the core work of developing, maintaining, and expanding the HCUP databases. Thomson Reuters also works with the subcontractors, Social & Scientific Systems (SSS), M.L. Barrett, Inc., and others to develop, maintain, and distribute the HCUP databases on behalf of AHRQ.

B. Secondary Contractors

AHRQ Project Officers are assigned to oversee and direct all activities performed under independent contract by Secondary Contractors that utilize HCUP data. These activities may be directed by the Center for Delivery, Organization, and Markets (CDOM) or by other centers 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 (formerly titled "HCUP Quality Indicators"). The creation of most HCUP tools has been accomplished by Secondary Contractors, including, for example, the Clinical Classification Software (CCS) and the on-line HCUPnet statistical query

system at http://hcupnet.ahrq.gov.

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. Data Use Agreements

1. AHRQ Staff-Contractor Agreements

AHRQ and contractor staff 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 and security training on an annual basis that includes information on the appropriate (and inappropriate) use of HCUP data. Staff-Contractor Agreements prohibit AHRQ and contractor staff 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.

2. HCUP Data Use Agreements

All persons (including AHRQ staff and contractors) given access to HCUP restricted access public release databases are required to sign an HCUP Data Use Agreement and complete the on-line DUA training[11] 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.[12]

Users must agree, among other things, to use the data for research and statistical purposes only and to make no attempt to identify individuals. Identities of institutions may be available from some Data Organizations that already make that information public or agree to its release in the HCUP databases; however, in data use agreements with HCUP, users must agree not to identify establishments directly or by inference in published or disseminated material.

VI SECURITY OF HCUP DATA

The HCUP 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, *Guide for the Security Certification and Accreditation of Federal Information Systems*. HCUP IT system certification and accreditation is compliant with all Public Law (PL)-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

[11] HCUP Data Use Agreement training at http://www.hcup-us.ahrq.gov.

[12] Violation of the AHRQ confidentiality statute is subject to a civil penalty of up to $10,000 under 42 U.S.C. 299c-3(d). Signature on the HCUP DUA indicates agreement to comply with the DUA requirements. Deliberately making a false statement about complying with the DUA requirements 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 of up to $10,000 or up to five years in prison. Violators of the HCUP DUA may also be subject to penalties under state confidentiality statutes that apply to the data for particular states.

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 http://csrc.nist.gov.

In general, physical media such as tapes, cartridges, disks, CDs, or other storage devices, reports, lists, or any other material containing potentially identifying information are kept in locked files, locked offices, or controlled-access storage rooms at the end of each working day, whenever not in immediate use, and supervised by authorized project staff. Critical backup files for disaster recovery are housed at a secure, offsite location. Access to secure storage locations is controlled by the AHRQ Project Officer, contractor Project Directors, and/or a delegate, as appropriate to each site.

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

Procedure	Source Data	Intramural Databases	Data Development Files	Restricted Access Public Release Databases
Shipping	*Data are shipped separately from documentation * Shipped only to the Primary Contractor, Thomson Reuters * Media containing data is identified only 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	* Data are shipped separately from documentation * All shipments are confirmed	* Data are shipped separately from documentation * All shipments are confirmed	* Data are shipped together with accompanying documentation to data users approved through an application process
Storage	* All computers storing source data are located in secure, limited-access rooms * Media devices are kept in secure, limited-access rooms or locked cabinets at the Primary Contractor's work site	* All computers storing HCUP data, are kept in secure, limited-access rooms or locked offices * Media devices are kept in secure, limited-access rooms or locked cabinets	* All computers storing HCUP DD data are kept in secure, limited-access rooms or locked offices * Media devices are kept in secure, limited-access rooms or locked cabinets	* All computers storing HCUP data are kept in secure, limited-access rooms or locked offices * Media devices are kept in secure, limited-access rooms or locked cabinets

Procedure	Source Data	Intramural Databases	Data Development Files	Restricted Access Public Release Databases
Access	* Accessed only through identification verification and password authentication * Access is granted only to appropriate project staff * Computers accessing the data must either be stand-alone or connected by a secure network	* Password protected * Access for research use requires Project Officer approval * Computers accessing the data must either be stand-alone or connected by a secure network	* Password protected * Access is granted only to appropriate project staff * Access for research use requires Project Officer approval * Computers accessing the data must either be stand-alone or connected by a secure network	* Access for research use by AHRQ and contractor staff requires Project Officer approval
Use	* Use only for HCUP file creation and verification * Access through dedicated secure servers * Data may not be accessed over the Internet	* Use through dedicated AHRQ / HCUP secure servers * Data may not be accessed over the Internet	* Use only for specific requested data elements * Access through dedicated AHRQ / HCUP secure servers * Data may not be accessed over the Internet	* Organizational policies apply

A. Physical Access to Facilities

AHRQ and its contractors control physical access to facilities using electronic methods and 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 (Thomson Reuters) requires that all visitors must first register at the reception desk, and thereafter must be escorted by a Thomson Reuters employee.

AHRQ and contractor offices are equipped with locking storage cabinets and/or locking doors. Thomson Reuters maintains an electronic code-key protected secure storage room for on-site archiving of data tapes, cartridges, disks, CDs, or other storage devices and a separate code-key protected secure environment for its Local Area 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.

VII 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 certification of destruction to the supplying Data Organizations. 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 Officer and with permission from the Data Organization(s).

After contractors complete the processing of data into the HCUP databases, all non-deliverable and intermediate files are deleted from microcomputers and other platforms and/or are archived in a separate, secure location. Files may remain on backup media for a period of time until purged from the system. Final, deliverable HCUP project files are retained by the Primary Contractor for the duration of the project.

Printed output and documents containing confidential or identifying information are shredded when disposal is required. Electronic, optical, or magnetic records are 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 may, at its sole discretion, choose to retain the HCUP intramural, data development, and restricted access public release databases to support longitudinal research.