Data Holdings, Data Linkage Processes, and Security Provisions of the Maternal Child Health and Education Research and Data Center at the University of Florida

This document describes data holdings, data linkage processes, and security provisions at the University of Florida's Maternal Child Health and Education Research and Data Center (The Center). The Center uses an “honest broker” system that separates identified data from end-user analysis data. Honest brokers are separate personnel acting as disinterested parties to the data. Federal and local regulatory environments superimpose procedures, authorization requirements, and documentation requirements on this system.

Data Holdings
The Center’s data warehouse is composed of statewide maternal and child health records numbering 5 million individuals going back to 1985. The Center also operates two statewide live data entry systems with over 600 users for Children’s Medical Services Early Steps program and Regional Perinatal Intensive Care Centers program.

Data Linkage Processes
Personal identifiers are essential for the creation of linked datasets. Individually identified data most often include name, address, social security number, telephone number, date of birth, program participation, dates of service, and evaluation results. Databases are linked using industry standard software and techniques based on common data fields.

Security Provisions
Administrative Security
The Center follows federal, state, and University of Florida standards for privacy, confidentiality, and security compliance summarized in Figure 1. The Center documents its handling of protected health information (PHI), trains employees to handle these sensitive data appropriately, obtains appropriate permission from owners of the data, and limits access to authorized individuals.

Figure 1: The Center’s Security Provisions
The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. §1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. FERPA gives parents certain rights with respect to their children’s education records, which transfer to the student at age 18 or attendance of school beyond high school.

Similarly, the Center follows provisions of the Health Insurance Portability and Accounting Act (HIPAA) Privacy Rule, which protects the privacy of individually identifiable health information; the HIPAA Security Rule, which sets national standards for the security of electronic protected health information; and the confidentiality provisions of the Patient Safety Rule, which protect identifiable information being used to analyze patient safety events and improve patient safety.

The Security Program for the Information and Computing Environment (SPICE) at the University of Florida protects information that is owned, managed, and used by the University of Florida’s Health Science Center (HSC) in all its forms (e.g. electronic, paper), by training, systems analysis, and technical consultation and support. As part of the HSC, The Center follows SPICE guidelines.

**Physical Security**
The Center’s servers are located in the University of Florida’s Health Science Center. Physical security limits access to servers by IT personnel to authorized electronic access. Physical barriers include hardened doors and walls in a hurricane proof server room. Computer workstations are on a floor of a building with limited access controlled by electronic locks. Within the limited access building, workstations require multiple passwords before access to PHI is granted. At these workstations, only authorized personnel are allowed access to individually identified data. Access from specific workstations is limited by specifying specific private IP numbers and MAC addresses within a “Closed Zone” domain. Workstations in this Closed Zone do not have internet access.

**Electronic Security**
The Center uses an honest broker system to handle sensitive data. Identified data are on a server behind a firewall, accessible only to honest brokers which are authorized users with titles such as “data manager” or “data custodian.” Figure 2 illustrates the intake of data by a data custodian supplied by customers (lower right) who stand to benefit from having their organization’s data linked to the Center’s data warehouse. Data managers clean and link data as appropriate. Once ready for use, data managers de-identify data to the degree required for the project. These de-identified datasets are stored apart from the identified data and are handed off to researchers who in turn prepare web-based, public access summary information for end users such as government officials and community organizations.
The result of an honest broker system is that researchers do not have access to individually identified data through a combination of barriers: passwords, folder permissions, and physical separation. This separation protects identified data from access by researchers. Researchers have access only to de-identified, aggregate level data. Figure 3 summarizes access by individuals’ role.
Figure 3: Summary of Access to Data

Figure 4 summarizes the process of transforming personally identified data by Center data custodians and managers and making them available to researchers and ultimately end users. In the top panel, data managers select important data fields in different source databases and link them in preparation for achieving project objectives. In the middle panel, data managers strip off personal identifiers from these linked data files. In the bottom panel, researchers supply de-identified data in many formats to end users. End users have access to project data only in the forms indicated in the bottom panel, but can use the data in a variety of ways.
The Center possesses expertise to link administrative data with demographic and environmental data and display them in a variety of ways as described on the bottom panel of Figure 4. The role of data is to provide compelling evidence to support public health policy decisions and to support public health initiatives in the community. Sharing data securely is critical to achieve these goals.