

DATA SECURITY FOR THE INPATIENT COMPONENT OF THE NATIONAL HOSPITAL CARE SURVEY

The National Center for Health Statistics (NCHS) is launching a new survey called the National Hospital Care Survey, which has inpatient and ambulatory components. Beginning with the 2011 inpatient data collection, Uniform Bill (UB)-04 data will be transferred from participating institutions to the Centers for Disease Control and Prevention (CDC) network through a secure data network (SDN) connection. The SDN is a secure data transfer service offered by CDC, and provides a strong suite of security controls to host applications and exchange data between CDC programs and public health partners while providing a high level of data integrity, confidentiality, reliability, and security. This meets NCHS/CDC policies for data transmission via the Internet. Users, such as hospitals, accessing systems within the SDN environment are required to have digital certificates (x.509) installed on their machines to provide assurances of their identity when they log on. Each hospital will need at least one digital certificate. Only hospitals with a current digital certificate can log onto the SDN. The SDN provides system monitoring on a 24 x 7 basis, data redundancy features, and disaster recovery features for select information systems.

On receipt at NCHS, the data will be downloaded onto the specially designated and configured NCHS/Division Health Care Statistics (DHCS) server (FSP-727). The FSP-727 server is a Windows 2008 server (w/server operating system - Windows Server 2008 R2 Standard). The server is physically located at NCHS and protected under Windows firewall system security features and the CDC firewall.

Files will be loaded into a secure area on the FSP-727 server for verification and editing. Data containing personal identifiers (e.g. name, address, phone number, SSN, etc.) after verification and editing will be extracted and loaded onto separate files in separate secure sub-shares. If the transmitted information from an individual hospital fail the verification process, the failed data are destroyed, the specific hospital is notified, and a re-transmission of the original data will be requested. Access to these data is restricted by NCHS/CDC procedures. Access to these servers is controlled by NCHS administrators and limited to NCHS program staff (accessible only from internal DHCS subnet) that have been cleared to access confidential statistical data. Access to the data for this project will be further restricted to individuals authorized by the program and the NCHS server administrator.

No potentially identifiable data will be released in any form to the public. Reports produced by NCHS about the data or using the data will not identify an individual hospital or an individual discharge. Public use files will contain no information that can identify any individual or hospital.