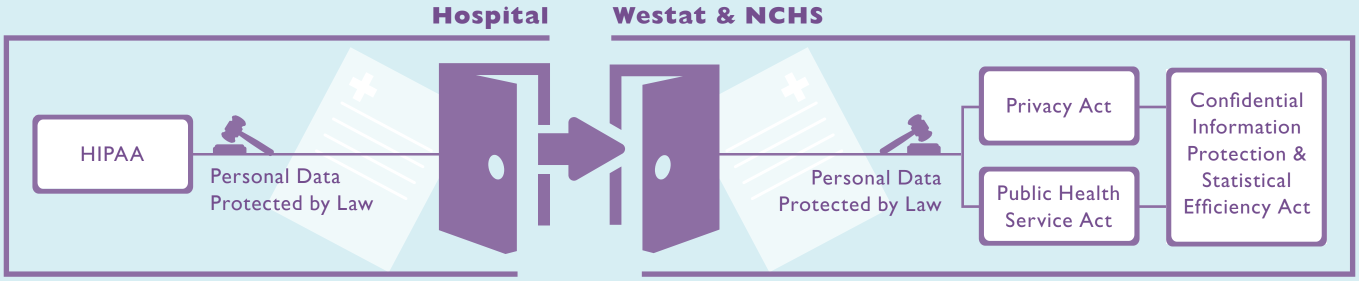
National Hospital Care Survey

Data Security


Hospital
Westat & NCHS
HIPAA
Personal Data Protected by Law
Personal Data Protected by Law
Privacy Act
Public Health Service Act
Confidential Information Protection & Statistical Efficiency Act

Our Legal Requirements

The National Center for Health Statistics (NCHS) legal requirements for safeguarding confidential information are governed by three laws. NCHS and its agents apply quality assurance standards and follow federally mandated laws, regulations, and guidelines from which federal agency system security requirements are derived. These laws are:

The Privacy Act (5 U.S.C. 552a); Public Health Service Act (42 U.S.C. 242 m(d) section 308(d); and, the Confidential Information Protection and Statistical Efficiency Act or CIPSEA (Public Law 107-347).

In addition, NCHS complies with the Federal Cybersecurity Enhancement Act of 2015. This law requires the federal government to protect federal computer networks by using computer security programs to identify cybersecurity risks like hacking, internet attacks, and other security weaknesses. If any cybersecurity risk is detected, the information system may be reviewed for specific threats by computer network experts working for the government (or contractors or agents who have governmental authority to do so).

- Each of these laws have been designed to protect the records of individuals; limit use; inform respondents; protect federal computer networks, and enable Westat as NCHS' contractor to act as its Designated Agent.

NCHS staff and its agents are required annually to complete training on confidentiality requirements and practices, including reporting any breach of confidentiality, and to sign annual non-disclosure agreements confirming intention to abide by all rules and regulations protecting confidential data. Contractor organizations are required to meet the same administrative, physical and technical safeguards as NCHS and to agree in writing to the same restrictions and obligations with respect to safeguarding confidential information collected in the National Hospital Care Survey (NHCS).

Westat's Data Security Plan

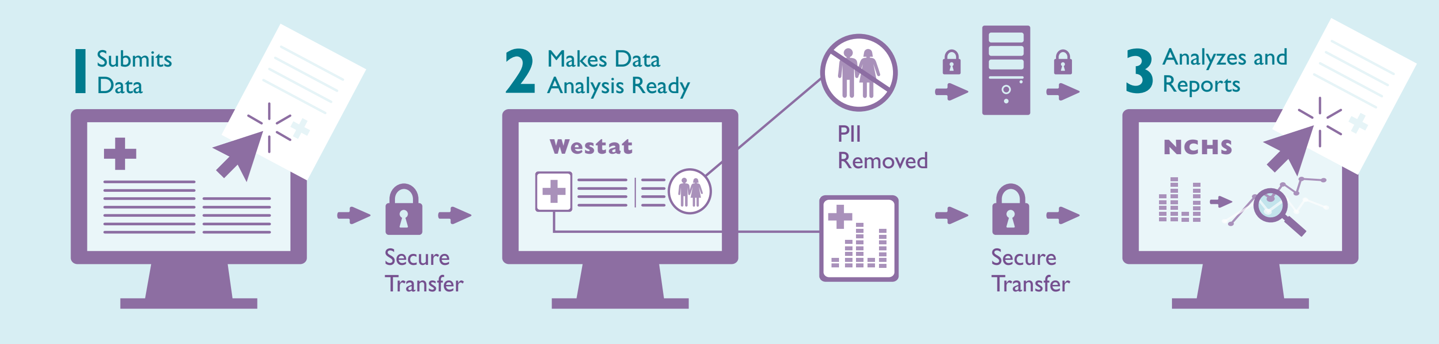
Westat, the data collection agent for the NHCS, has provided a comprehensive data security plan to NCHS to ensure safety and confidentiality of the NHCS data. The NHCS Data Security Plan (DSP) describes the survey procedures and data handling protocols that are being implemented to secure study data and protect confidentiality. The plan follows the structure and guidelines established by the National Institute of Standards and Technology (NIST; 800-series)[1] for meeting the requirements of the Federal Information Security Management Act (FISMA).[2] The DSP complies with all relevant laws, regulations, and policies governing the security of data and the protection of confidentiality, including the Privacy Act of 1974 (5 USC 552a), Section 308(d) of the Public Health Service Act (42 USC 242m) and the Confidential Information Protection and Statistical Efficiency Act (CIPSEA, PL 107-347) of 2002. The DSP considers all known data security and confidentiality protection risks and will be updated with improved data security practices, as needed.

Continued on back

From the Hospital to Westat – Secure Transfer

Data can be transmitted via Westat's Secure Transfer System (WSTS) or the use of a Hospital Information Service Provider (HISP).

- The WSTS provides the secure data network and transmission mechanism needed to receive and store data files from participating hospitals. All files sent via the WSTS are securely stored and transferred using Federal Information Processing Standard (FIPS) 140-2 validated Advanced Encryption Standard (AES) encryption. Data are encrypted both during transmission and when stored on the Westat server. Each hospital user receives an individual username, password, and access to a separate controlled area of the site.
- A HISP allows secure file transfer. Through Secure Exchange Solutions (SES) a secure, Direct Email Address is provided to allow our hospitals to send/receive secure communications, in a way that is both compliant with the Health Insurance Portability and Accountability Act (HIPAA) and complies with the federal standards.



From Westat to NCHS – Secure Transfer

After processing, these data will eventually be sent to NCHS via the Centers for Disease Control and Prevention's (CDC) Secure Access Management Services (SAMS). SAMS provides a secure data transfer service that meets NCHS/CDC policies for data transmission via the Internet. Upon receipt at NCHS, all of the personally identifiable information (PII) (direct and indirect) will be downloaded onto the specially designated and configured NCHS CIPSEA File Storage Server within the Consolidated Statistical Platform (CSP) environment. The dedicated NCHS CIPSEA server is a secured physical component of the CSP accessible only by NCHS-designated staff. All direct PII files and data containing personal identifiers will be loaded onto separate files in separate secure sub-shares on the CIPSEA server for verification and editing, with the most strict access controls.

[1] http://csrc.nist.gov/publications/PubsSPs.html [2] http://www.nist.gov/itl/csd/soi/fisma.cfm#