Attachment B.4: Strictly Confidential Brochure

Other safeguards for your privacy

- Items that could be used, either directly or indirectly, to identify health care providers or their patients are removed from public-use data files. Names, addresses, dates of birth, dates of service, and location of the health care establishment are never released to the public.
- NCHS withholds statistical totals if they represent a location so small that the numbers might identify someone.
- Information security procedures, including the use of coded passwords and physical security of computers, prevent unauthorized access to the data.
- All published summaries are presented in such a way that no respondent can be identified.

We believe that our procedures for safeguarding information and our record of protecting the privacy of respondents are some of the reasons why so many providers readily participate and provide reliable information. As a result, information on health care utilization is made available every year to the American public, health care providers, the U.S. government, and the research community.

For further information

NCHS data are released in printed reports, CD-ROMs, and on the NCHS website, **https://www.cdc.gov/nchs/**.

For more information about how NCHS protects the information you provide, visit: **https://www.cdc.gov/nchs/about/policy/confidentiality.htm**.

For specific questions about how NCHS protects the information you provide, contact:

NCHS Confidentiality Office
Telephone: (888) 642-4159
Email: nchsconfidentiality@cdc.gov

CS270274-A

How the National Health Care Surveys Keep Your Information Confidential

National Ambulatory Medical Care Survey

National Hospital Ambulatory Medical Care Survey

National Hospital Care Survey

National Study of Long-Term Care Providers

Centers for Disease Control and Prevention
National Center for Health Statistics

Protecting the public's privacy . . . no idle pledge

Confidentiality

For more than 50 years, the National Center for Health Statistics (NCHS) has protected the confidential information collected in its surveys, and we take your privacy very seriously.

All information that relates to or describes identifiable characteristics of individuals, a practice, or an establishment will be used only for statistical purposes. NCHS staff, contractors, and agents will not disclose or release responses in identifiable form without the consent of the individual or establishment in accordance with section 308(d) of the Public Health Service Act (42USC 242m) and the Confidential Information Protection and Statistical Efficiency Act of 2002 (CIPSEA, Title 5 of Public Law 107-347). In accordance with CIPSEA, every NCHS employee, contractor, and agent has taken an oath and is subject to a jail term of up to five years, a fine of up to $250,000, or both, if he or she willfully discloses ANY identifiable information about you.

The Federal Cybersecurity Act of 2015 permits the monitoring of information systems for the purpose of protecting a network from hacking, denial of service attacks, and other security vulnerabilities.[1] The software used for monitoring information systems may scan information that is transiting, stored on, or processed by the system. If the information triggers a cyber threat indicator, the information may be intercepted and reviewed for cyber threats. The Cybersecurity Act specifies if any information that is scanned by the cybersecurity software programs is found to be suspicious, it 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). The Act further specifies that such information may only be used for the purpose of protecting information and information systems from cybersecurity risks.

[1] "Monitor" means "to acquire, identify, or scan, or to possess, information that is stored on, processed by, or transiting an information system"; "information system" means "a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information"; "cyber threat indicator" means "information that is necessary to describe or identify security vulnerabilities of an information system, enable the exploitation of a security vulnerability, or unauthorized remote access or use of an information system".

A strong record for maintaining privacy during data collection and processing

NCHS collaborates with organizations, for example, the U.S. Census Bureau and private research companies, to collect and process data for the National Health Care Survey (NHCS). These groups have a proven record of protecting the privacy of survey respondents.

HIPAA Privacy Rule on individual patient information and survey participation

The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule permits you to make disclosures of protected health information without patient authorization for public health purposes and for research that has been approved by an institutional review board (IRB) with a waiver of patient authorization. The National Health Care Survey (NHCS) meets both of these criteria.

As part of the IRB approval process, all component surveys of NHCS that collect information on individual patients have had a review of the survey's procedures for handling protected health information. Based on the review, practices were determined to be appropriate for safeguarding respondent confidentiality. Additionally, disclosures may be made under a data-use agreement with NCHS for some surveys that do not collect directly identifiable data.

Copies of IRB approval letters and other related materials, such as data-use agreements, are available upon request for each component survey of NHCS. There are several things that you must do to assure compliance with the Privacy Rule when participating in the survey. First, the privacy notice that you generally provide to your patients must indicate that patient information may be disclosed for either research or public health purposes. Second, you may need to keep a record of the disclosure that shows that some data from the patient's medical record were disclosed to the Centers for Disease Control and Prevention for NCHS (we will provide forms to assist you in record keeping). If you do not transmit health information electronically (such as claims data), you are not subject to the Privacy Rule or the requirements described above.

For additional information on the HIPAA Privacy Rule, visit:
https://www.hhs.gov/ocr/hipaa.