Consent to Share Claims Data with the CDC's National Hospital Care Survey

Introduction:

The Centers for Disease Control and Prevention (CDC)'s National Center for Health Statistics (NCHS) National Hospital Care Survey (NHCS) provides official statistics on healthcare utilization in hospital-based settings that helps develop the nation's healthcare policies. Submitting data to NHCS improves the nation's ability to accurately report on chronic conditions, hospital utilization related to the drug epidemic, and the treatment of patients with respiratory illnesses. NHCS collects all inpatient discharges and emergency department encounters for a calendar year. The data sent from NHSN through a CDC secure internal transfer method are the same as the data submitted to NHSN and submission to NCHS does not require any additional data elements. The NHCS administrative claims data submission includes the patient identifiers, patient demographic information, diagnosis codes, procedure codes, discharge status, and the date of hospital encounter. NHCS collected data may be included in deidentified public use microdata files, restricted use NCHS Research Data Center files, public health dashboards, and peer-reviewed publications. Your participation is considered a service to the Nation as NHCS data will be used to inform policies to improve the state of health care in the U.S.

In addition, your hospital data will be collected, analyzed, and shared back with you. As part of your participation, your hospital will receive the benefit of access to the exclusive **Annual Hospital Report (AHR) Portal**. The AHR portal is an interactive dashboard that allows hospitals to view summarized information on patient characteristics and encounters, opioid-involved encounters and overdoses, and data on post-acute mortality (30/60/90 days mortality post-discharge) for hospitals that provide patient identifiers. This summary information can be easily downloaded from the AHR portal for presentation to hospital staff, board members, and the public you serve.

Further information about NHCS can be found at the NHCS website (https://www.cdc.gov/nchs/nhcs/index.html) and at The Office of Management and Budget report website (https://omb.report/) under OMB No. 0920-0212 (expiration date 09/30/2027).

Authority:

NCHS is authorized to collect hospital data under the authority of Section 306 of the Public Health Service Act (42 United States Code 242k).

General provisions:

Participation in NHCS is completely voluntary. The data collected through the NHCS are used for statistical activities only. A hospital's participation allows more accurate descriptions of all hospitals in national statistics and helps to continue this Survey's ability to be a resource to the hospital community, health care researchers, and policy makers.

NCHS Confidentiality Provisions:

Federal laws require NCHS to follow strict procedures to keep all data regarding patients and hospitals strictly confidential. Any collected data that would permit identification of any individual or establishment is collected with a guarantee that it will be held in strict confidence, will be used for

statistical purposes, including record linkages, and will not be disclosed or released to others without the consent of the individual or the establishment in accordance with Section 308(d) of the Public Health Service Act [42 United States Code 242m(d)] and the Confidential Information Protection and Statistical Efficiency Act (CIPSEA, 44 U.S.C. 3561-3583). In accordance with CIPSEA, every NCHS employee, contractor, and agent has taken an oath and is aware of potential fines and penalties including a jail term of up to 5 years, a fine of up to $250,000, or both if he or she willfully makes a prohibited disclosure of ANY identifiable information about you.

The Health Insurance Portability and Accountability Act of 1996 or HIPAA Privacy Rule (45 CFR Part 160 and Part 164, subparts A and E) recognizes (i) the legitimate need for public health authorities and others responsible for ensuring the public's health and safety to have access to protected health information to conduct their missions, and (ii) the importance of public health reporting by covered entities in identifying threats to the public and individuals. The Privacy Rule permits (i) disclosure of health information without written patient authorization for specified public health purposes, to public health authorities legally authorized to collect and receive the information for such purposes; and (ii) disclosures that are required by state and local public health or other laws [HIPAA regulations (45 CFR 164.501)]. Thus, HIPAA permits hospitals who are covered entities to participate in surveys of this nature for public health purposes. Consistent with NCHS practice, NCHS contractors are specially designated agents of NCHS for this project; as such, it is permissible to disclose data to them for statistical and epidemiological purposes.

Data Security:

In addition to the above cited laws, NCHS complies with the Federal Cybersecurity Enhancement Act of 2018 (6 U.S.C. § 663) which protects Federal information systems from cybersecurity risks by screening their networks. All data collected by NCHS will be protected consistent with the statutes cited above.

NHCS data are stored and processed by Federal automated information systems that have been subjected to CDC's security assessment and authorization process. All federal requirements concerning administrative, physical and technical safeguards to protect the confidentiality, integrity and availability of confidential data collected in the NHCS are met. Data are transmitted to NCHS and its contractors by secure data networks, and no data are transmitted unless encrypted. Once received, confidential data are housed on a secure server with access restricted to authorized users.

Data Release:

Consistent with the above, NCHS will not release the identity of specific hospitals or individual patients in any manner except to NCHS staff and contractors—only when required and with necessary controls. Results of the survey will be published only in an aggregated manner that will not allow identification of any individual hospital or patient. Data intended for inclusion in public use microdata files are reviewed by the NCHS Disclosure Review Board to protect against the disclosure of data that would permit the identification of an individual patient or hospital. Although linkage of patient information with other data sources such as death records and records from the Centers for Medicare & Medicaid Services (CMS) and the Department of Housing and Urban Development (HUD) is planned, there will be no contact with patients. NCHS linkage activities are tightly controlled. Direct personally identifiable

information (PII) is kept separate from other survey data and access is highly restricted in a secure physical environment.

Data Breach Prevention & Response:

The CDC/NCHS/Division of Health Care Statistics (DHCS) (e.g., full-time employees, contractors, and contractor organizations) is responsible for:

- Annually signing the NCHS Nondisclosure agreement.
- Annually completing applicable CDC Security Training for Information Security & Privacy Awareness, Insider Threats Awareness, and Role-Based Training.
- Annually completing the NCHS Confidentiality Training.
- Developing and adhering to processes to control and monitor access/removal/updates of NCHS data.
- Developing and adhering to processes that align with the Office of Management and Budget (OMB) and Department of Health and Human Services (HHS) breach response regulations.
- Developing and adhering to processes for ensuring that all suspected or confirmed PII breaches of systems are identified, tracked, and responded to in an effective, consistent, and timely manner that minimizes risk to CDC, facilities, and individuals. All suspected or confirmed PII losses must be reported within one hour of discovery to the CDC Computer Security Incident Response Team (CSIRT) at #1-866-655-2245.
- Investigating the cause of data breaches for effective responses, responding to breaches in cooperation with the appropriate CDC and/or NCHS personnel to include but not limited to:
    - The NCHS Information Systems Security Officer (ISSO);
    - The NCHS Confidentiality Officer;
    - The CDC Office of the Chief Information Security Officer;
    - The CDC Chief Privacy Officer (CPO), etc.
- Adjusting program procedures accordingly and future planning.