



**Data Use Agreement**  
**Between**  
**Indiana State Department of Health**  
**And**  
**Centers for Disease Control and Prevention (“CDC”), National Healthcare Safety Network (“NHSN”)**

The Indiana State Department of Health and CDC/NHSN enter into this Data Use Agreement (the “Agreement”) effective 08 / 18 / 2017 (“Effective Date”). CDC/NHSN and the Indiana State Department of Health shall be referred to individually as a “Party,” or collectively as the “Parties.”

This Agreement establishes a formal data access and data use relationship between CDC/NHSN and the Indiana State Department of Health. This Agreement covers individual- and institution-identifiable data, received by the CDC/NHSN subject to the Federal Privacy Act, 5 USC §§552 and 552a, from the NHSN Patient Safety Component, Healthcare Personnel Safety Component, and Dialysis Component as listed in the attached document that have been voluntarily submitted to NHSN by healthcare institutions in Indiana and for which there is no State mandate for reporting of such individual- or institution-identifiable data (“COVERED DATA”). However, COVERED DATA shall NOT include data pertaining to federal or tribal healthcare institutions.

The Parties shall abide by all applicable Federal and State laws, rules, and regulations including, without limitation, all patient confidentiality and medical record requirements and any applicable Institutional Review Board (“IRB”) requirements.

**STATE’S USES OF COVERED DATA**

The Indiana State Department of Health agrees to use the COVERED DATA for surveillance and/or prevention purposes only (e.g., evaluating the impact of a targeted program to reduce central line-associated bloodstream infections). The Indiana State Department of Health specifically agrees not to use the COVERED DATA obtained under this data use agreement for purpose of public reporting of institution-specific data or any regulatory or punitive actions against healthcare institutions, such as a fine or licensure action. The Parties acknowledge that COVERED DATA is limited to those data specified in the attached document, which identifies the complete set of data items, e.g., facility survey data, central line associated bloodstream infection numerator data, that the Indiana State Department of Health will have access to as a result of this Agreement.

The Indiana State Department of Health agrees to designate an NHSN Group Administrator and CDC/NHSN agrees to grant the State’s designated NHSN Group Administrator access to the State’s COVERED DATA. In the event that the NHSN Group Administrator leaves that role prior to assigning a replacement via the NHSN application, CDC/NHSN requires notification in writing on official letterhead from the signatory or the signatory’s successor to assure continuity.

- The designated NHSN Group Administrator for the Indiana State Department of Health is Christine Feaster, Healthcare Associated Infections Supervisor, [cfeaster@isdh.in.gov](mailto:cfeaster@isdh.in.gov), Indianapolis, Indiana.



The Indiana State Department of Health agrees that access to individual- and institution-identifiable data provided under the terms of the Agreement will be limited solely to department staff or contractors who are explicitly authorized to use those data for surveillance and/or prevention purposes only.

## DATA PROTECTIONS

CDC's legal authorities to obtain COVERED DATA from healthcare institutions are 42 U.S.C. section 241(a) (Public Health Service Act section 301(a)), pertaining to CDC's broad public health authority to conduct research and investigations, and 42 U.S.C. section 242k (Public Health Service Act section 306), pertaining to the collection of statistical data. CDC's authority to keep the COVERED DATA confidential (i.e., protected from an unauthorized release) is 42 U.S.C. section 242m (Public Health Service Act section 308(d)) and the Federal Privacy Act, 5 USC §§552 and 552a.

The Indiana State Department of Health acknowledges that Federal statutes, including 18 U.S.C. section 1001 (providing penalties for making false statements to the Government of the United States), may be implicated if the State does not protect the COVERED DATA from release pursuant to this Agreement.

The Indiana State Department of Health acknowledges that it will be the custodian of COVERED DATA stored in its data files and, as such, will be responsible for establishing and maintaining appropriate administrative, technical, and physical safeguards to prevent unauthorized access to or use of these files, for example, security awareness training and signed rules of behavior for all persons who have access to COVERED DATA, strong passwords and auditing for all access to COVERED DATA, approved encryption of COVERED DATA stored digitally.

The State will use the following safeguards to protect COVERED DATA stored in its data files:

The State of Indiana Data Encryption Policy IOT-CS-SEC-003: "Protection of information is critical to State security and operations. Below are encryption requirements for confidential, private and sensitive data (i.e. Federal Tax Information, Credit Card Numbers, Personally Identifiable Information, Passwords, or other information not meant for public consumption):

- Information shall not be sent over the internet (e.g., email, ftp, etc.), via remote access or transmitted over public or external networks unless the data is encrypted
- Information shall be encrypted in transit, whether being transmitted internally or externally
- Information shall be encrypted at rest. Information at rest refers to the state of information when it is located on a primary or secondary storage device (server, portable devices, solid state drive, etc.)

The above requirements require strong cryptography and security protocols. All encryption mechanisms and configurations must have a validated Federal Information Processing Standard (FIPS) 140-2 cryptographic module and meet National Institute of Standards and Technology (NIST) 800-131A encryption requirements.

All State issued devices, such as laptops and phones must have IOT approved encryption technologies installed and turned on prior to distribution. Employees shall not install any encryption software not validated and approved by the IOT Security Team."

The Indiana State Department of Health shall take appropriate measures to maintain security of the COVERED DATA including storage on an internal network with limited access that requires



approval from the Indiana Office of Technology. The network can only be accessed on password-protected work computers. Paper copies of COVERED DATA shall be stored in locked filing cabinets within the appropriate employee's workspace. The Indiana State Department of Health shall not share COVERED DATA with any employees who do not need to access the data in order to perform their job duties.

The Indiana State Department of Health specifically agrees that, to the extent permitted by State and federal law, it will not release COVERED DATA requested under a State's open records laws; to media; for litigation purposes; that is proprietary and if disclosed could cause competitive harm; or to anyone other than department staff or contractors who are explicitly authorized to use those data for surveillance and/or prevention purposes only.

The following State statutes, regulations, or policies provide additional safeguards that protect against the release of COVERED DATA:

- Indiana Code § 16-41-8-1: "Potentially disease transmitting offense"
- Indiana Code § 5-14-3-4(a)(3): Records and recordings exempted from disclosure; time limitations; destruction of records
- Indiana Code § 34-43-1-12: Confidential records regarding communicable diseases
- 410 IAC 1-2.5-78: Confidentiality of medical and epidemiological information
- Confidentiality Statement signed by employees, contractors, employees of contractors or volunteers working within the Epidemiology Resource Center of the Indiana State Department of Health

The Indiana State Department of Health agrees to inform CDC/NHSN in advance of any forthcoming changes to State law(s) that will reduce legal safeguards that protect against release of COVERED DATA. The Indiana State Department of Health acknowledges that CDC/NHSN may terminate the Agreement as a result of this information.

#### **PROVISION AND MANAGEMENT OF THE DATA**

The Indiana State Department of Health acknowledges that its access to COVERED DATA will be for adverse healthcare events and/or processes of care that occur subsequent to signing this agreement, specifically occurring on or after the first day of the fourth month following the signing date. COVERED DATA reported to NHSN for prior events or processes will not be accessible.

The Indiana State Department of Health agrees to notify CDC in the event that the Indiana State Department of Health is obligated or chooses to release COVERED DATA for a purpose other than surveillance and prevention.

#### **TERM AND TERMINATION OF AGREEMENT**

This Agreement shall be effective for a period of 5 years beginning on the Agreement Effective Date. The Agreement may be terminated before the 5-year period upon submission by either Party of written notice by Signatory or Signatory successor, in which case the Agreement shall cease 5 days after the date that CDC/NHSN submits the notice to the Indiana State Department of Health OR 5 days after CDC/NHSN receives a notice submitted by the Indiana State Department of Health.



In addition, upon CDC/NHSN's knowledge of a pattern or practice that constitutes a material breach of this Agreement by the Indiana State Department of Health, CDC/NHSN may immediately and unilaterally terminate this Agreement.

CDC requires that in the absence of a conflict with State law the Indiana State Department of Health must delete or otherwise destroy COVERED DATA stored in its files within one year of the conclusion of this Agreement or a successor Agreement. CDC will retain all COVERED DATA in its files.

NOW, THEREFORE, by signing below, the Parties agree that they have read, understand, and agree to the conditions set forth above:

Indiana State Department of Health

CDC/NHSN

  
\_\_\_\_\_  
Signature

**Trent Fox**  
**Interim Chief of Staff**

  
\_\_\_\_\_  
Signature

**Daniel A. Pollock, M.D.**  
**Branch Chief, Surveillance Branch**  
**CDC Division of Healthcare Quality**  
**Promotion**

Date 8/18/2017

Date August 22, 2017