# Data Use Agreement

**Between**

Florida Department of Health

**And**

**Centers for Disease Control and Prevention ("CDC"), National Healthcare Safety Network ("NHSN")**

The Florida Department of Health and CDC/NHSN enter into this Data Use Agreement (the "Agreement") effective ___09_/__09__/__2015__ ("Effective Date"). CDC/NHSN and the Florida 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 Florida 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 and Healthcare Personnel Safety Component as listed in the attached document that have been voluntarily submitted to NHSN by healthcare institutions in Florida 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**

Florida 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). Florida 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 Florida Department of Health will have access to as a result of this Agreement.

Florida 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 Florida Department of Health is Janet Hamilton, Administrator, Surveillance and Surveillance Systems, Janet.hamilton@flhealth.gov, Tallahassee, FL.

Florida 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.

Florida 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.

Florida 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 Florida Department of Health has information security and privacy policies that are applicable to all employees, contractors, and volunteers. Information Security and Privacy Policy 5, DOHP 50-10d-10, states:
>
> Members of the Department of Health (DOH) workforce will receive an initial security and privacy awareness training prior to providing services to clients, accessing confidential information, accessing information technology, or within 30 days of employment start date, whichever is earliest. The training course can be presented one-on-one, as a self-study, or as a formal training course. Regardless of format, the initial training must cover the items outlined in the core training protocol in section VI.D. 1. - 5. and other essential job-specific training as required by position responsibilities. In addition to the initial training, all employees and volunteers shall receive information security and privacy awareness update training at least annually. Documentation of training shall be maintained at the local level and shall be accessible to supervisory personnel.
> Information security and privacy awareness training curriculum and materials shall be consistent with federal regulations, state laws and rules, as well as departmental policies, protocols, and procedures. Training materials and curriculum shall be reviewed at least annually and updated as appropriate.
> …Information security and privacy awareness training updates are provided at least annually to all staff.
> …Information security and privacy awareness training materials and curriculum are consistent with federal regulations, state laws and rules, as well as departmental policies, protocols, and procedures.

Information Security and Privacy Policy 7, DOHP 50-10f-10, regarding confidential information states:

All information/data which is exempt from disclosure by state or federal law, rule, or regulation is confidential. Each Department of Health (DOH) division, office, county health department (CHD), and Children's Medical Services (CMS) area office will classify information/data sets in their custody as confidential or not confidential. Confidential information must be secured using appropriate administrative, technical, and physical safeguards. It is the responsibility of each DOH worker to maintain the confidentiality of information/data.
Areas of Responsibility:
1. General
a. The DOH Office of General Counsel shall maintain a reference list of state and federal statutes and rules relevant to DOH confidential information.
b. Audit logs of access and modifications to confidential information should be maintained.
c. The local information security and privacy coordinators shall be granted access to review audit logs containing accountability details regardless of format.
d. Agreements and procedures shall be in place for sharing, handling, or storing confidential data with entities outside the department.
e. All members of the DOH workforce shall be knowledgeable of the classifications of data/information and the proper handling of data/information.
f. Confidential information shall be accessible only to authorized persons.
Confidential information transferred externally on paper or electronic media must be protected.
h. Information with employee identifiers, client identifiers, or other confidential content is not left unattended or unsecured.
i. Unauthorized persons will be escorted and not left unattended in secured areas.
j. Position computer monitors to prevent unauthorized viewing.
k. Consultations involving confidential information must be held in areas with restricted access.
l. Confidential information must be printed using appropriate administrative, technical, and physical safeguards that prevent unauthorized viewing.
m. Information must be encrypted during transmission over open or public networks.
n. Person(s) having the authority to perform electronic file transfers (including facsimile) of confidential information will be documented in the local operating procedures.
o. Data back ups must be locked in a secured area.
p. Proper authorization to disclose patient medical information must be obtained prior to disclosure. Refer to Information Security and Privacy Policy 8, Disclosure of Patient Medical Information.

Florida 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:

In accordance with Sections 304, 306, and 308(d) of the Public Health Service Act (42 USC 242b, 242k, and 242m(d)), the Florida Department of Health agrees to establish appropriate and necessary administrative, technical, and physical procedures and safeguards including limiting access and appropriate staff training to protect the confidentiality of the data and to prevent the unauthorized use

or access to it. In addition, such confidential data provided to the Florida Department of Health User Group remains confidential as well as being exempt from disclosure under Florida's public record law.

Section 381.0055, Florida Statutes Confidentiality and quality assurance activities.—
(1) All information which is confidential by operation of law and which is obtained by the Department of Health, a county health department, healthy start coalition, or certified rural health network, or a panel or committee assembled by the department, a county health department, healthy start coalition, or certified rural health network pursuant to this section, shall retain its confidential status and be exempt from the provisions of s. 119.07(1) and s. 24(a), Art. I of the State Constitution.
(2) All information which is confidential by operation of law and which is obtained by a hospital or health care provider from the department, a county health department, healthy start coalition, or certified rural health network, or a panel or committee assembled by the department, a county health department, healthy start coalition, or certified rural health network pursuant to this section, shall retain its confidential status and be exempt from the provisions of s. 119.07(1) and s. 24(a), Art. I of the State Constitution.
(3) Portions of meetings, proceedings, reports, and records of the department, a county health department, healthy start coalition, or certified rural health network, or a panel or committee assembled by the department, a county health department, healthy start coalition, or certified rural health network pursuant to this section, which relate solely to patient care quality assurance and where specific persons or incidents are discussed are confidential and exempt from the provisions of s. 286.011, and s. 24(b), Art. I of the State Constitution and are confidential and exempt from the provisions of s. 119.07(1) and s. 24(a), Art. I of the State Constitution, respectively.

Section 395.3025(5), Florida Statutes states: The Department of Health may examine patient records of a licensed facility, whether held by the facility or the Agency for Health Care Administration, for the purpose of epidemiological investigations. The unauthorized release of information by agents of the department which would identify an individual patient is a misdemeanor of the first degree, punishable as provided in s. 775.082 or s. 775.083.

Section 395.3025(7)(a), Florida Statutes states: If the content of any patient treatment record is provided under this section, the recipient, if other than the patient or the patient's representative, may use such information only for the purpose provided and may not further disclose any information to any other person or entity, unless expressly permitted by written consent of the patient. A general authorization for the release of medical information is not sufficient for this purpose. The content of such patient treatment record is confidential and exempt from the provisions of s. 119.07(1) and s. 24(a), Art. I of the State Constitution.

Florida 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. Florida Department of Health acknowledges that CDC/NHSN may terminate the Agreement as a result of this information.

**PROVISION AND MANAGEMENT OF THE DATA**

Florida 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.

Florida Department of Health acknowledges that CDC/NHSN will provide a time-limited opportunity for healthcare institutions participating in NHSN in their jurisdiction to opt out of reporting COVERED DATA to NHSN.

Florida Department of Health acknowledges that CDC/NHSN will notify newly enrolling institutions of the provisions of this Data Use Agreement so that enrolling institutions will have full knowledge of how their COVERED DATA will be used by the Florida Department of Health and can opt out of providing COVERED DATA to NHSN.

Florida Department of Health agrees to notify CDC in the event that the Florida 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 Florida Department of Health OR 5 days after CDC/NHSN receives a notice submitted by the Florida Department of Health.

In addition, upon CDC/NHSN's knowledge of a pattern or practice that constitutes a material breach of this Agreement by Florida 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 Florida 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:

| Florida Department of Health | CDC/NHSN |
|---|---|
| **Anna M. Likos, MD, MPH** | **Director, CDC Division of Healthcare** |
| **State Epidemiologist** | **Quality Promotion** |

**Director, Division of Disease Control and Health Protection**

Anna M. Likos, MD MPH

Date 31 Aug 2015

Date 09 Sept 2015