Responses to legal questions about data sharing

QUESTION POSED

Is inter-jurisdictional sharing permitted or barred under a formal agreement or public health authority or informal agreement? Please provide a copy or hyperlink to the relevant legal agreements (i.e., templates), laws, rules, or other.

RESPONSES

Massachusetts Department of Public Health (Rosa Ergas)
Formally prevented.
See relevant document at https://www.mass.gov/files/documents/2016/07/rc/mdph-confidentiality-procedures.pdf.

New Hampshire (David Swenson)
Informally not accepted.
See Data Sharing and Use Agreement with CDC, beginning on following page.

Centers for Disease Control and Prevention
National Syndromic Surveillance Program
Data Sharing and Use Agreement

Purpose: This Agreement ("Agreement") between the Centers for Disease Control and Prevention ("CDC"), having its primary offices at 1600 Clifton Road, Atlanta GA 30333 and the State of New Hampshire or NH ("Jurisdiction"), through its Department of Health and Human Services (DHHS) having its primary offices at 29 Hazen Drive, Concord NH 03301 establishes the basic terms and conditions concerning voluntary contribution of data by Jurisdiction to the National Syndromic Surveillance Program's (NSSP) BioSense Platform and access, sharing, protection and use of the Data Received by the NSSP BioSense Platform that are submitted by the Jurisdiction.

Background: Syndromic surveillance is a process that regularly and systematically uses health and health-related data in near real-time to make information on the health of a community available to public health officials and government leaders for decision making and enhanced responses to hazardous events and outbreaks.

In response to the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 and the Pandemic and All-Hazards Preparedness Reauthorization Act of 2013, the CDC developed and modified the BioSense Program to establish an integrated system of nationwide public health surveillance for the early detection and prompt assessment of and response to potential bioterrorism-related illness. As of November 2011, the BioSense Program developed a distributed computing environment, which included analytic tools, under state and local advisement. The program has since evolved into the NSSP which is a collaboration among individuals and organizations from the local, state, and federal levels of public health, including departments of health; other federal agencies, including the Department of Defense (DoD) and the Department of Veterans Affairs (VA). NSSP currently includes a community of practice and a cloud-based syndromic surveillance computing platform (the NSSP BioSense Platform) that hosts data submitted by the Jurisdiction and computing applications that include analytic tools and services.

As part of its role under this Agreement, CDC will provide the cloud-based environment for the NSSP BioSense Platform by and through a contract with a vendor ("CDC Contractor") for participating Jurisdictions to facilitate receipt, storage and management of the Jurisdictions' syndromic surveillance data. In addition, working with a CDC Contractor, CDC: 1) has developed and will operate the NSSP BioSense Platform; 2) will continue to provide tools and services therein; 3) will assure compliance of the platform and the available tools and services with the Federal Information Security Management Act (FISMA) and other federal data security policies, to the extent they apply; 4) will provide operational support to the participating Jurisdictions and other authorized users of the NSSP BioSense Platform by conducting processing, quality control, aggregation, sharing, and analysis of data submitted to the BioSense Platform; 5) will support the NSSP community of practice; and 6) will conduct national and regional syndromic surveillance. The NSSP BioSense Platform provides participating Jurisdictions with the ability to contribute, access and share data that will support existing and potential expansion of its public health surveillance systems.

Authorities: CDC is authorized by the Public Health Service Act, Sections 301, 317 and 319D (as amended) (42 U.S.C. 241, 247b and 247d-4, as amended) to maintain active surveillance of diseases

through epidemiologic and laboratory investigations and data collection, analysis, and distribution and to coordinate with states, locals and other appropriate public health partners with respect to the maintenance and collection of such data.

The Jurisdiction is authorized to share de-identified data collected under NH RSA 141-C and NH Administrative Rule He-P 301 with the CDC in accordance with NH RSA 141-C:10, II, which allows the Jurisdiction to share analyses and compilations of data which do not disclose protected health information.

Additionally, CDC is a "public health authority" as defined at 45 C.F.R. §164.501 and as used in 45 C.F.R. §164.512(b), Standards for Privacy of Individually Identifiable Health Information, promulgated under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). To the extent the CDC is an authorized person having a legitimate need to acquire or use protected health information collected under NH RSA 141-C, the Jurisdiction may share only so much of the protected health information as is necessary for the CDC to provide care and treatment to the individual who is the subject of the protected health information, investigate the causes of disease transmission in the particular case, or control the spread of the disease among the public. NH RSA 141-C:10, I.

Definitions: For purposes of this Agreement, the following definitions shall apply:

"NSSP BioSense Platform" means the cloud-based syndromic surveillance computing platform that receives and processes data submitted to the Platform and hosts analytic tools and services.

"Data" means the public health-related information gathered by or contributed to the Jurisdiction or an individual user on behalf of the Jurisdiction that becomes part of the Data Received by the NSSP BioSense Platform.

"Data provider" means hospital, health professional, health facility, health information exchange or other source that submits data to the NSSP BioSense Platform either directly to the Platform or indirectly, e.g., through submission to the Jurisdiction or other agent that submits data to the platform.

"Data received by the NSSP BioSense Platform" means an organized collection of syndromic surveillance data submitted or contributed to NSSP by the Jurisdiction, by any Users, and any Data Providers within the Jurisdiction. The current syndromic surveillance data definitions and exchange standards, developed as part of the Meaningful Use Initiative and supported by NSSP, are defined in the most current version of the *PHIN Messaging Guide for Syndromic Surveillance: Emergency Department, Urgent Care, Inpatient and Ambulatory Care Settings,* available at https://www.cdc.gov/phin/resources/phinguides.html.

"De-Identified data" or "De-Identified information" means data that do not identify an individual and with respect to which there is no reasonable basis to believe the information can be used to identify an individual because the data has been rendered not identifiable in accordance with the *HIPAA* standards set forth in 45 CFR §164.514.

"Individually identifiable information" means information, such as patient name or social security number, that identifies an individual or with respect to which there is a reasonable basis to believe the information can be used to identify an individual.

"Jurisdiction" means the local or state health jurisdiction operating under either statutory or regulatory authority to obtain and use health-related data for population health protection.

"NSSP" means the National Syndromic Surveillance Program (formerly known as the BioSense Program), a collaboration among public health agencies and partners that supports the use and timely exchange of syndromic data for improved nationwide all-hazard situational awareness for public health decision making and enhanced responses to hazardous events and outbreaks.

"Party" means State or Local Jurisdiction or CDC; "Parties" means State or Local Jurisdiction and CDC.

"Syndromic surveillance" means regular and systematic uses of health and health-related data, including patient encounter, laboratory, and pharmacy data from healthcare settings such as emergency departments, urgent care, ambulatory care and inpatient settings, in near real-time for improved all-hazard situational awareness, public health decision making and enhanced responses to hazardous events and outbreaks at local, state, regional and national levels of public health.

"User" means any authorized user of Data available through the NSSP BioSense Platform. All Users must be affiliated with a State or Local Jurisdiction, CDC, VA, or DoD, except as otherwise provided herein.

"Breach" means the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic. With regard to Protected Health Information, "Breach" shall have the same meaning as the term "Breach" in section 164.402 of Title 45, Code of Federal Regulations.

'Security incident" shall have the same meaning "Computer Security Incident" in section two (2) of NIST Publication 800-61, Computer Security Incident Handling Guide, National Institute of Standards and Technology, U.S. Department of Commerce.

Agreement Principles:

1) The jurisdiction agrees to participate in the NSSP by contributing Data to the NSSP BioSense Platform and utilizing the Platform in accordance with the terms and conditions herein. Prior to allowing a Data Provider to submit data to NSSP BioSense Platform (directly or through the Jurisdiction), the Jurisdiction shall work with the Data Provider to ensure that a) Data Provider shall not take any actions that are inconsistent with this Agreement; b) Data Provider shall not submit Data to the BioSense Platform that it is not authorized to submit; and c) Data Provider submission of Data will comply with applicable federal, state, and local laws and requirements. The Jurisdiction shall define and finalize exact nature and form of agreement with the Data Provider, if any.

2) Data Received by the BioSense Platform:
The Jurisdiction represents and warrants that it has authority to enter into this Agreement and to submit the Data to the NSSP BioSense Platform as contemplated by this Agreement and for its intended uses (as described below in section 3), and that doing so will not violate any law or regulation applicable to the Jurisdiction in which it resides or any agreement or arrangement to which the Jurisdiction is a party. The current syndromic surveillance data definitions and exchange standards, developed as part of Meaningful Use and supported by NSSP, are defined in the *PHIN Messaging Guide for Syndromic Surveillance: Emergency Department, Urgent Care, Inpatient and Ambulatory Care Settings (April 2015)*, available at www.cdc.gov/phin/resources/phinguides.html.

3) The jurisdiction acknowledges and agrees that the Data Received by the BioSense Platform may be used and/or disclosed for the following purposes:

a. Operational Support
As a part of accessing and using the NSSP BioSense Platform, tools and services, and for purposes of providing operational support for NSSP as described below, Jurisdiction understands and agrees that designated staff in CDC's Division of Health Informatics and Surveillance (DHIS) and the CDC Contractor will have routine access to the secure individual patient record-level Data Received by the NSSP BioSense Platform from the Jurisdiction or its Data Providers. The operational support is intended to support the Jurisdiction so that it can best utilize the Data, analytic tools and other functions of the NSSP BioSense Platform. DHIS agrees to regularly communicate information on operational activities to the Jurisdiction.

Operational support includes processing data, conducting data quality control activities, creating surveillance categorization algorithms, assuring proper aggregation of data, establishing and supporting mechanisms that allow Jurisdictions to set permissions and share data, and ensuring proper operation and functioning of permission tools and data analysis and visualization tools, as further set out below:

- Data processing includes such activities as de-encrypting electronic health record messages submitted by data providers, creating up-to-date individual patient visit records from multiple electronic record messages submitted for the same patient visit, and categorizing records into syndrome groups;
- Quality control includes assessing messages and records for accuracy, completeness, consistency, timeliness and validity and developing and implementing data quality control processes;
- Creating and refining syndromic surveillance categorization algorithms means using chief complaint, diagnoses and other clinical data to create syndromes, sub-syndromes and other event codes;
- Assuring proper data aggregation includes grouping individual patient records into local, state, regional and national aggregate counts to support use of dashboards and analytic tools;
- Data sharing and permissions means administering permissions for national level users and Jurisdictions' administrators, and ensuring that permissions tools and granted access control is working properly; and

- Data analysis and visualization means assuring that tools and dashboards, including ESSENCE and SAS, that provide data reporting, querying, analysis, and visualization function properly. Results will not be used in public health response.

b. Syndromic Surveillance at the National and U.S. Department of Health and Human Services (HHS) Regional Levels

As a part of accessing and using the NSSP BioSense Platform, tools and services, for purposes of syndromic surveillance at national and HHS regional levels, Jurisdiction understands and agrees that users will have access through dashboards and analytic tools to views of Data Received by the NSSP BioSense Platform from the Jurisdiction aggregated to HHS regional and national levels. In addition, in order to evaluate unusual clusters or patterns that indicate an event of potential public health concern, users will have limited views of selected individual patient record level data elements (HHS region, age-group, gender, syndrome, sub-syndrome, date without time, patient class and disposition). Though currently no changes to this list of selected individual patient record level data elements are planned, a 120-day notice will be given and the community of practice will be engaged prior to changes being made to this list in future. Such views will exclude data elements that identify hospitals, zip codes, counties, states and individually identifiable information such as birthdate. These surveillance activities include routine analysis of regional and national level trends, evaluation of multi-regional events, and special surveillance during events of public health interest at national and regional levels.

c. National and regional syndromic surveillance reports

As a part of accessing and using the NSSP BioSense Platform, tools and services, Jurisdiction understands and agrees that CDC will develop reports focused only on national and regional level syndromic surveillance. CDC may invite collaborators and co-authors from Jurisdictions to participate in the development of such reports. CDC may also share reports with Jurisdictions for review and comment in advance of publication. Jurisdiction agrees to perform the review in timely manner for publication and/or dissemination of the report. Such final reports will be shared with the NSSP community of practice, other health agencies or partners and published on the NSSP web site or in scientific or health professional journals. Such final reports will not contain information specific to any local, territorial or state Jurisdiction and will always be presented with De-Identified Information only.

d. Collaborative Projects with CDC

As a part of accessing and using the NSSP BioSense Platform, tools and services, Jurisdiction understands and agrees that its Jurisdiction NSSP data steward will be responsible for administering access to Jurisdiction Data. If the Jurisdiction elects to participate in a collaborative project with CDC, and potentially other users that use Data Received by the NSSP BioSense Platform, the steward will use web-based NSSP BioSense Platform tools under the steward's control to provide specific users with access for a specified time period to specific sets of the Jurisdiction's data either aggregated to the Jurisdiction Level or at the individual patient record level. Collaborative projects may include: a) coordinating syndromic surveillance at the national and regional levels with surveillance at the Jurisdiction level, b) evaluating unusual clusters or patterns that indicate an event of potential public health concern, c) allowing CDC or other Jurisdictions to provide technical assistance, d) evaluating the NSSP program or BioSense Platform, and e) developing improved methods for conducting

syndromic surveillance. Examples of evaluation and methods development projects include examining different methods for analyzing and detecting a disease outbreak or developing or revising syndrome definitions. During the process of initiating and conducting collaborative projects, CDC and Jurisdiction collaborators will have to reach agreement about publishing reports based on the projects. Such reports may be shared with the NSSP community of practice, other health agencies or partners and may be published on the NSSP web site, or in scientific or health professional journals. Such reports will not contain any Individually Identifiable Information and will always be presented with De-Identified Information only. In addition, data suppression rules will be used to prevent possible identification through publication of tables combining characteristics that could be used to identify an individual, e.g., age, sex, race, ethnicity, and geographic location.

4) Confidentiality and de-identification of data
Minimum required data elements will be submitted to the NSSP BioSense Platform by data provider or Jurisdiction. Data Provider is responsible for de-identification of data prior to submission to NSSP BioSense Platform. De-identification will be done in compliance with federal and state law, including HIPAA and corresponding regulations. Jurisdiction agrees and acknowledges that the data submitted to NSSP BioSense Platform may include certain hospital, physician, or other health care provider identifiers and may contain individual patient record level data elements (e.g., HHS region, age-group, gender, syndrome, sub-syndrome, date, patient class and disposition). New Hampshire will not submit any individual patient identifiers. Jurisdiction agrees that it is the responsibility of the Jurisdiction to obtain any permissions required in order to submit such data to the NSSP BioSense Platform.

5) Open Records Laws
Jurisdiction acknowledges and understands that the Data it submits to the NSSP BioSense Platform, including Data accessed by CDC, other jurisdictions and users may be subject to state and federal (e.g. Freedom of Information Act) open records laws. To the extent data submitted to NSSP BioSense Platform may be subject to the applicable open records laws for the state of origin for Jurisdiction, Jurisdiction is responsible for compliance with such law. Jurisdiction acknowledges that CDC, as a federal agency, must ensure compliance with federal open records law, the Freedom of Information Act, with respect to data in its custody and control at the time of the request.

6) Asset Protection:
CDC will protect the privacy and confidentiality of any Individually Identifiable Information that may be contained in the Data Received by the BioSense Platform and for which access is provided under this Agreement consistent with the Privacy Act of 1974, to the extent applicable, standards promulgated pursuant to HIPAA, and all applicable laws, regulations, and policies. In furtherance of activities set forth in this Agreement and consistent with applicable laws, policies and procedures to ensure the privacy and confidentiality of such Data, CDC may provide data access to appropriate employees, contractors, and other users. CDC users of data, including contractors authorized access to the Platform, are expected to comply with applicable federal laws and CDC policies with respect to the use, safeguarding and maintenance of such Data and will be made aware of the principles set forth in this Agreement. CDC will not attempt to identify records contained in the data submitted under this Agreement or link these data with data from other Jurisdictions for identification purposes. In the case of a public health emergency to protect life and health of individuals and populations, CDC will coordinate with the state or local authority for any additional information or follow-up that may be necessary respective to CDC's responsibilities and authority. CDC also will coordinate with the

Jurisdiction and Data Provider to respond to any data requests from individuals who are not authorized users, e.g., Freedom of Information Act (FOIA) requests. Every effort will be made to protect the privacy and confidentiality of Individually Identifiable Information, but CDC cannot assure that Individually Identifiable Information will not be released in all cases. However, CDC will work collaboratively with the Jurisdiction and Data Provider to ensure that all Parties are aware of and when possible a part of deciding what Data Received by the BioSense Platform, if any, will be released.

The Jurisdiction is responsible for limiting the submission of Individually Identifiable Information, encrypting Data prior to submission to the BioSense Platform and for maintaining the security of any encryption techniques used. Creation of the Data submitted to the BioSense Platform and encryptions will be done in compliance with federal and state law and corresponding regulations. The Jurisdiction should work with the Data Provider to ensure that Data are submitted in accordance with the *PHIN Messaging Guide for Syndromic Surveillance: Emergency Department, Urgent Care, Inpatient and Ambulatory Care Settings.*

Without limitation to any other provision of this Agreement, CDC agrees not to disclose, display or otherwise make available any company proprietary information to any third party, in any form, except to public health officials in connection with the purposes established herein or as otherwise required under the Freedom of Information Act, or other federal law. The Jurisdiction will clearly indicate in writing any information that is considered to be company proprietary, trade secret or confidential business information.

CDC further employs the following measures in order to ensure strong privacy and security controls to protect the Data:

a. Secure NSSP BioSense Platform: The Platform is hosted by a Federal Risk and Authorization Management Program (FedRAMP) approved provider. FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. The NSSP BioSense Platform meets CDC certification and accreditation standards to assure that it is FISMA compliant and is supported by the timely maintenance of security updates, anti-virus updates, malware updates, and hardware/application vulnerability reviews and remediation. Servers are housed in access-controlled, physically secured locations. These locations prevent the unauthorized physical and logical access of servers and network devices, ensuring that only those authorized to maintain the servers are allowed access to them.

b. Authentication: All non-federal NSSP BioSense Platform users use a one factor authentication (password) to access the Platform services and data. In addition, CDC and CDC contractor users are also required to provide a second level of authentication: when the user's credentials are confirmed, the service requested is checked to verify that the user has permission to access the internal application servers.

c. Need-to-Know Access: Access controls within the NSSP BioSense Platform ensure that Data submitted to the Platform are not only restricted to authorized users, but also that those users are restricted to the data they need as provided in this agreement. Any unauthorized access or breach has to be reported to CDC Information Systems Security Officers (ISSO) immediately. Consistent with CDC's policies and procedures, CDC will keep relevant jurisdictions informed of any such rare event. The CDC must notify the Jurisdiction's Privacy Officer,

Information Security Office and Program Manager of any Security Incidents and Breaches within two (2) business days of the time that the CDC learns of their occurrence. This includes a confidential information breach, computer security incident, or suspected breach which affects or includes any Jurisdiction information.

d. Data Encryption: Data travel are encrypted from the client system to the NSSP BioSense Platform, and they are encrypted for storage within the data transformation and warehousing process. This encryption is managed by DHIS and its contractor and is consistent with Federal requirements.

7) Secure Access
The NSSP BioSense Platform's Access & Management Center (AMC) allows a Jurisdiction's NSSP data steward (site administrator) to perform administrative functions, including controlling access to data, create and manage user accounts, changing passwords, creating data sharing rules and allowing data sharing. Jurisdictions are responsible for managing users, access to their site's data, and access to NSSP BioSense Platform tools using the AMC. All users have to acknowledge agreement to the "BioSense Platform Code of Conduct" when first accessing user accounts and at the time of password change.

8) Ownership of Data
The Data Source shall retain ownership of the data it contributes to the NSSP BioSense Platform. Additional terms regarding access and control of these data, asset protection and applicable and governing laws are defined in separate clauses (including but not limited to 3, 5, 6, and 7) of this Agreement.

9) Data Disposition:
Data Received by the NSSP BioSense Platform, including Data that have been used for National and Regional Surveillance and shared with CDC for Collaborative Projects under this Agreement will be archived, stored, protected, or disposed of in accordance with relevant federal records requirements.

10) Severability
If any term or condition of this Agreement is held invalid, such invalidity shall not affect the validity of the other terms or conditions of this Agreement, provided, however, that the remaining terms and conditions can still fairly be given effect.

11) Funding:
This Agreement is not an obligation or a commitment of funds, or a basis for a transfer of funds, and does not create an obligation or commitment to transfer data, but rather is a statement of understanding between the parties concerning the sharing and use of covered data. Expenditures by each party are subject to its budgetary processes and to its availability of funds and resources pursuant to applicable laws, regulations, and policies.

12) Settlement of Disputes:
Disagreements between the parties arising under or relating to this Agreement will be resolved by consultation between the parties and referral of the dispute to appropriate management officials of the parties whenever possible.

13) Applicable Laws:

U.S. federal law shall govern the construction, interpretation, and performance of this Agreement. This MOU shall be governed by the laws of New Hampshire State, to the extent they do not conflict with applicable federal law.

14) Notices:

Any notice, demand or other communication required or permitted to be given under the Agreement shall be in writing and shall be deemed delivered to a Party: (i) when delivered by hand or nationally recognized overnight courier; or (ii) six (6) days after the date of mailing if mailed by United States certified mail, return receipt requested postage prepaid, in each case to the address of such Party set above.

15) Persons to Contact:

A. DHHS contact program Administrator:

State of New Hampshire,
Department of Health and Human Services)
AHEDD Project Manager
David.Swenson@dhhs.nh.gov

Or

Division of Public Health Services Director

lisa.morris@dhhs.nh.gov

B. DHHS contact for Breach notifications:

Elizabeth Gillett, DHHSInformationSecurityOffice@dhhs.nh.gov
Catherine Bernhard, DHHSPrivacyOfficer@dhhs.nh.gov

16) Term of Agreement, Amendment, and Termination:

a. The term of this Agreement shall be five years commencing from the date of final signature. The agreement may be renewed upon mutual written consent of the parties.

b. Except as otherwise expressly provided herein, this Agreement may be amended only by the mutual written consent of the authorized representatives for each party.

c. This Agreement may otherwise be terminated with ninety (90) days advance notice upon written notice by either party. Upon termination of this agreement, to the extent consistent with federal law, a jurisdiction will have the option to remove its data from BioSense Platform by requesting appropriate forms from NSSP help desk and completing an established process for data removal.

State of New Hampshire
Department of Health and Human Services

By: Lisa Morris

Name: Lisa Morris, MSSW
Title: Director, Division of Public Health Services
NH Dept. of Health & Human Services
Division of Public Health Services
29 Hazen Drive
Concord, NH 03301

Date: 1/23/19

Centers for Disease Control and Prevention
U.S. Department of Health and Human Services

By: Paula W. Yoon

Name: Paula W. Yoon, ScD, MPH
Title: Division Director
Div. of Health Informatics & Surveillance
Div. of Health Informatics & Surveillance
Center for Surveillance, Epidemiology, and Laboratory Services
Office of Public Health Scientific Services

Date: 2/13/2019

New Jersey (Teresa Hamby)
Neither expressly permitted nor barred.

New York State (Charlene Weng)
Neither expressly permitted nor barred.

Pennsylvania (Kirsten Waller)
Neither expressly permitted nor barred.

Rhode Island (Maria Lena Wilson)
Neither expressly permitted nor barred.