

**BIOSENSE 2.0 INFORMATION SHARING AND DATA USE AGREEMENT
BETWEEN IDAHO DEPARTMENT OF HEALTH AND WELFARE AND HOSPITALS
Version 3/7/2014**

I.

THE PARTIES AND THE SUBJECT MATTER OF THE AGREEMENT

This **INFORMATION SHARING AND DATA USE AGREEMENT** (the "Agreement") is entered into as of _____, (the "Effective Date"), by and between **the Idaho Department of Health and Welfare (DHW) located at 450 W State Street, Boise, Idaho 83702,** and _____
[A HOSPITAL WITHIN IDAHO], located at _____ (the "Hospital"), concerning the provision by the Hospital of data, as defined below, to be submitted to the BioSense 2.0 Program (as defined below) pursuant to the terms of this Agreement.

II.

RECITALS

A. Background

1. As of November 2011, the BioSense Program has developed a distributed computing environment and tools with state and local control ("BioSense 2.0"). Governance of BioSense 2.0 is facilitated by the Association of State and Territorial Epidemiologists ("ASTHO") in coordination with the Centers for Disease Control ("CDC"), the Council of State and Territorial Epidemiologists ("CSTE"), the National Association of County and City Health Officials ("NACCHO"), and the International Society for Disease Surveillance ("ISDS"), collectively referred to as the "Governance Group". ASTHO has contracted with a vendor to act as a data storage company ("Vendor") for BioSense 2.0 in a process that is compliant with the Federal Information Security Management Act ("FISMA"). Through the Vendor, ASTHO will offer BioSense 2.0 for receiving and managing data for syndromic surveillance. BioSense 2.0 will provide DHW with the ability to control the contribution and access of data that support syndromic surveillance activities.

2. BioSense 2.0 will provide two spaces for the submission or viewing of Data. The first space shall be a secure space in which DHW shall have access and exclusive control over any data it submits or are submitted on its behalf, subject to applicable law. DHW will also have the ability to permit data submitters, such as Hospital, within Idaho, to send health-related data for syndromic surveillance (collectively, "Public Health Data Providers" or "PHDPs") directly to its secure space within BioSense 2.0. The second space within

BioSense 2.0 shall be a shared space in which DHW shall control access to non-identifiable aggregated Data and shall control approval of access to geographic views of non-identifiable aggregated Data according to policies developed by DHW in consultation with the Idaho Health Information Technology Workgroup within the Governor's Health Care Coordination Council.

B. WHEREAS, DHW is utilizing BioSense 2.0 to facilitate the sharing of certain health-related data for syndromic surveillance and to assist in the possible detection, confirmation, situation awareness, monitoring of, and response to public health threats; and

C. WHEREAS, Hospital intends to contribute data to BioSense 2.0 for public health and surveillance purposes as described herein, subject to the terms and conditions of this Agreement, and

D. WHEREAS, within BioSense 2.0 DHW will have access to: (1) a secure space where the DHW and the jurisdictional Public Health District (PHD) will be the only agencies able to view and analyze patient-level data and Protected Health Information (PHI) or Individually Identifiable Health Information (IIHI); and (2) a shared space wherein DHW will have the ability and discretion to determine whether, how, with whom, and at what level to share aggregate data, views, and maps with other data sources, the Centers for Disease Control and Prevention (CDC), or other agencies.

E. NOW THEREFORE, in consideration of the mutual agreements set forth herein and for other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the Parties hereto agree as follows:

III.

DEFINITIONS

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

A. BioSense 2.0 is defined as the cloud-enabled, web-based platform and tools used to store, maintain, process, display, receive, analyze, and destroy data received for the advancement of the BioSense Program as described in Section II of this Agreement.

B. BioSense Program is defined as the federal program under the CDC that tracks health problems as they evolve and provides public health officials with data, information and tools they need to better prepare for and coordinate responses to safeguard and improve the health of American people.

C. Data is defined as the public health-related information gathered by the Hospital or gathered by an individual user on behalf of the Hospital that is submitted to BioSense 2.0.

D. Distributed Computing Environment is defined as the software technology for managing computing and data exchange in a system of distributed computers, and the use the system to solve computational problems by one or more computers that communicate with each other by message passing.

E. Individually Identifiable Health Information or IIHI shall have the same definition as provided by the Health Insurance Portability and Accountability Act (“HIPAA”) and corresponding regulations.

F. Meaningful Use regulations are defined by the Centers for Medicare and Medicaid Services (42 CFR Parts 412, 413, 422 et al.) Medicare and Medicaid Programs; Electronic Health Record Incentive Program; Final Rules (published on July 28, 2010 in the Federal Register) and the Office of the National Coordinator for Health Information Technology (45 CFR Part 170) Health Information Technology: Initial Set of Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology; Final Rule (published on July 28, 2010 in the Federal Register).

G. Party is defined as Hospital or DHW; **Parties** means Hospital and DHW.

H. Protected Health Information or PHI shall have the same definition as is contained in HIPAA and corresponding regulations.

I. User means any authorized user of data available through BioSense 2.0. All Users must be approved by DHW.

IV.

DATE SHARING, ACCESS, AND USE UNDER THIS AGREEMENT

A. Data Sharing. BioSense 2.0 is designed to promote the contribution of health data for syndromic surveillance by all users and the appropriate sharing of aggregated data in the shared space. While DHW, Hospital, and other users are not required to share data, they are encouraged to do so. The Governance Group may consider and make recommendations for data sharing in the shared spaces, which may include recommendations for types of data (e.g., minimum data sets), seasonal data collections, and similar contributions that would enhance the value of BioSense 2.0 to all users. DHW is not, however, required to implement recommendations of the Governance Group.

B. Data Access and Use. Hospital agrees to submit data to BioSense 2.0 in accordance with the terms and conditions herein. Hospital shall not take any actions inconsistent with this Agreement; Hospital shall not submit data to BioSense 2.0 that it is not authorized to submit; and Hospital submission of data will comply with applicable federal, state, and local laws. Any violation of the aforementioned terms and conditions

by Hospital may result in suspension or termination of the Hospital's access to and/or use of BioSense 2.0.

1. The Hospital acknowledges and agrees that as part of BioSense 2.0, the Data may be used and/or disclosed for the following purposes:

a. **Sole Use by DHW or PHDs in Secure Space.** For use by DHW or PHDs for continued maintenance and control of data in BioSense 2.0. For use by DHW or PHDs to manage data and information for internal uses only.

b. **Shared Space.** To facilitate the sharing of views of data, which shall not contain PHI or IIHI, for public health and surveillance purposes, DHW and PHDs may share aggregate views of data at a level determined by DHW. DHW acknowledges such use, access, and publication shall be between jurisdictions, provided, however, that such use, access, and sharing of data shall be determined solely by DHW in accordance with policies developed by DHW in consultation with the Idaho Health Information Technology Workgroup and only after the number of contributing PHDPs is sufficient to obscure the identity of any individual PHDP.

c. **Other health agency uses.** To provide access to views of the data or analyses thereof to local and state public health entities once data are being routinely submitted to BioSense 2.0, and Health and Human Services Region X state public health agencies (Oregon, Washington, and Alaska) only once the number of contributing PHDPs within the aggregate level is sufficient to obscure the identity of any individual PHDP and the legal authority to share such aggregate data has been determined in Idaho, in connection with the conducting of their respective public health responsibilities consistent with applicable Idaho and/or federal law for the following purposes: (1) to facilitate the interchange of information that can be used to coordinate responses and monitor events routinely and during a potential health event; (2) for early detection and characterization of events (or health-related threats) by building on state and local health department systems and programs; (3) to provide health-related information for: (a) public health situation awareness, (b) routine public health practice, and (c) improved health outcomes and public health; and (4) to improve the ability to detect emergency health threats by supporting the enhancement of systems to signal alerts for potential problems in collaboration with federal, state, and local health jurisdictions and other potential stakeholders.

2. DHW or PHDs may use and share data contributed to BioSense 2.0 for the purpose of monitoring and assessing public health activity within Idaho. If DHW or PHDs identify a need to follow-up on data indicating an event of

potential public health concern, data providers will be contacted to gather information about the event.

C. Data Content Restrictions and Requirements. Data shall be transmitted in a manner and in a format compliant with published then-current requirements of the Meaningful Use regulations and the Idaho BioSense 2.0 Syndromic Surveillance Implementation Guide which is compliant with Meaningful Use regulations and BioSense 2.0 records requirements. Such data information requirements shall be available via the DHW Public Health Meaningful Use Reporting website and may be changed from time to time. Hospital agrees that it will comply with all applicable laws and government regulations affecting its use of BioSense 2.0, and DHW shall not have any responsibility relating to Hospital, including, without limitation, any responsibility to advise Hospital of Hospital's responsibility in complying with any laws or governmental regulations affecting its use of BioSense 2.0.

D. Confidentiality and De-Identification/Encryption of Data

1. Neither PHI nor IIHI will be submitted to BioSense 2.0 by Hospital unless transmitted to DHW's secure space in BioSense 2.0. Neither the Hospital, ASTHO, the CDC, the Vendor, nor any other entities (other than DHW and authorized PHDs) shall have access to such Data in the secure space.

2. Hospital is responsible for de-identifying and/or encrypting all PHI and IIHI prior to submission to BioSense 2.0 and is responsible for maintaining the security of any encryption techniques used. De-identification and encryptions shall comply with federal and Idaho law, including HIPAA and corresponding regulations. DHW shall have no responsibility for the encryption of PHI or IIHI. DHW shall have no obligation to ensure Hospital maintains compliance with these concepts and principles. Hospital agrees and acknowledges that the data captured by BioSense 2.0 may include certain hospital, physician, or other health care Hospital identifiers. Hospital agrees that it is Hospital's responsibility to obtain any permission required in order to submit such data to BioSense 2.0.

V.

PUBLIC RECORDS LAWS

Hospital acknowledges and understands that the data it submits to the secure space, including data accessed by other users, may be subject to Idaho public records laws. Hospital acknowledges and understands that the aggregated data submitted to the shared space, including data accessed by other data sources and users, may be subject to federal (e.g., the Freedom of Information Act) public records laws. Hospital is responsible for reviewing and complying with the applicable public records laws when determining the data to be provided.

VI.

DATA RETENTION/ DATA SECURITY

A. Hospital acknowledges and understands that data provided shall be archived, stored, maintained, protected, and disposed of in compliance with federal law and applicable Idaho law, to the extent Idaho law is not superseded by federal law. Data shall be maintained in a distributed computing environment and any and all policies and procedures applicable to the use of such an environment for BioSense 2.0 shall be in compliance with the Federal Information Security Management Act (“FISMA”).

B. Hospital is responsible for creating, maintaining, and protecting user passwords and other secure measures used for accessing and using BioSense 2.0 and for establishing its own security protocols and procedures compliant with DHW guidance (Attachment A) in the use of the passwords and administration of the data and any data viewed through BioSense 2.0. Hospital is further responsible for ensuring that PHI and IIHI are submitted to BioSense 2.0 only as permitted in Sections IV.B. and IV.D. of this Agreement. Hospital shall comply with the data sharing requirements contained in the signed DUA between DHW and ASTHO. Hospital shall maintain written policies and procedures for the transmission of the Data to BioSense 2.0. Hospital shall be responsible for developing, disseminating, and enforcing policies and procedures relating to any misuse or abuse of its passwords and other measures by the Hospital users and any resulting misuse or abuse of BioSense 2.0.

C. The Parties agree to immediately alert the other Party if there is a potential or actual breach of the security of BioSense 2.0 or the data contained within BioSense 2.0, or any actual or potential misappropriation or misuse of data available through BioSense 2.0. The Parties further agree to work cooperatively to investigate and comply with any federal and Idaho laws should a breach occur.

VII.

TERM AND TERMINATION

A. The initial term of this Agreement (the “Initial Term”) shall commence on the effective date and shall continue for three (3) years. Unless this Agreement is earlier terminated as set forth herein, this Agreement shall be automatically and successively renewed without further action by either Party for an indefinite number of successive one-year terms (each such additional term a “Renewal Term” and together with the Initial Term, the “Term”).

B. Either Party may terminate this Agreement upon thirty (30) days prior written notice to the other Party. If this Agreement is so terminated, the Parties shall be liable only for performance rendered in accordance with the terms of this Agreement prior to the effective date of termination. Further, either party may terminate this

Agreement immediately in the event the other Party materially breaches its obligations under the Agreement.

C. Promptly upon termination of this Agreement (1) the Hospital shall have the right to cease providing any additional data and/or any updates to previously submitted data and (2) DHW may retain the data that have been previously contributed to BioSense 2.0 unless otherwise restricted by law. Hospital may request that any previously submitted data be removed from BioSense 2.0 and that DHW and any other user's access to that specific data be terminated; however, such removal shall be subject to whether the specific data was accessed or used, feasibility of removal, and whether the data is subject to related laws, including any outlined as a part of Section V herein.

VIII.

OWNERSHIP OF DATA

DHW retains ownership of any data contributed to BioSense 2.0; but, as indicated in Sections V and VII herein, any data provided may be subject to continued legal requirements, including but not limited to retention and public records laws. As described in Section VII.C., Hospital may request that previously submitted data be removed; however, Hospital has no right to return or destruction of any data contributed to BioSense 2.0, except for data submitted by the Hospital to the secure area of BioSense 2.0. Hospital acknowledges that contribution of data to BioSense 2.0 does not in any way grant Hospital any rights, beyond those provided under this Agreement, to any data that it may access through BioSense 2.0 or to BioSense 2.0 itself. Further, DHW acknowledges that Hospital's contribution of data to BioSense 2.0 does not grant DHW any rights, beyond those provided under this Agreement, to any data the hospital chooses not to submit to BioSense 2.0.

IX.

OTHER PROVISIONS

A. Warranties

1. The Hospital represents and warrants it has the authority to enter into this Agreement and to provide the data to BioSense 2.0 as contemplated by this Agreement for the intended uses as outlined in Section IV.B.

2. Hospital acknowledges and agrees to the following: (a) ASTHO is responsible for the oversight of BioSense 2.0; (b) Hospital shall not submit any data that it is not permitted to disclose; (c) by contributing data to BioSense 2.0, Hospital has not breached, and will not breach, any confidentiality agreement or legal duty that Hospital has to any party and, further, no other person or entity has breached a legal duty in submitting the data to BioSense 2.0; and (d) Hospital submission of data will comply with applicable federal, state, and local

laws. Additionally, if Hospital breaches this section, then DHW shall have a right to terminate this Agreement.

B. Limitation of Liability. DHW makes no representations or warranties as to the accuracy or completeness of the data and disclaims no responsibility for any errors caused by inaccuracies or incompleteness of the data. DHW is only responsible for its own torts. Hospital hereby waives, and covenants not to sue DHW or PHDs for any and all possible claims that it might have against DHW or PHDs arising out of, or resulting from, the operation of the BioSense Program. IN NO EVENT SHALL DHW OR PHDs BE LIABLE TO HOSPITAL FOR ANY INDIRECT, PUNITIVE, SPECIAL, EXEMPLARY, INCIDENTAL, CONSEQUENTIAL OR OTHER DAMAGES OF ANY TYPE OR KIND (INCLUDING LOSS OF DATA, REVENUE, PROFITS, USE OR OTHER ECONOMIC ADVANTAGE) ARISING OUT OF, OR IN ANY WAY CONNECTED WITH THIS AGREEMENT, EVEN IF DHW OR DHW'S LICENSORS HAVE BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

C. Amendment; Waiver. This Agreement, or any term or condition, may be modified only by a written amendment signed by Hospital and DHW. Either party may propose an amendment. Failure or delay on the part of either party to exercise any right, power, privilege or remedy provided under this Agreement shall not constitute a waiver. No provision of this Agreement may be waived by either party except in writing signed by Hospital or DHW.

D. 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.

E. Entire Agreement; No Assignment. This Agreement is the complete agreement between the Parties concerning the subject matter hereof, and supersedes any prior oral or written communications between the Parties. This Agreement may be executed in counterparts. This Agreement may only be assigned by a written agreement executed by duly appointed officers of both Parties.

F. Governing Law. United States federal law shall govern the construction, interpretation, and performance of this Agreement; provided, however, the laws of the state of where the data originated shall govern any disputes, claims or issues arising from, relating to or concerning the data, or the contribution of the data to BioSense 2.0, except to the extent such state law is limited, or superseded, in whole or in part by applicable United States federal law.

G. 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: (1) when delivered by hand or nationally recognized overnight courier; or (2) 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 forth below (or at such other address as the Party may from time to time specify by notice delivered in the foregoing manner):

If to _____
Hospital: _____
Attn: _____

If to Idaho Department of Health and Welfare
DHW: Division of Public Health
450 W. State St. – 4th Flr.
P.O. Box 83720
Boise, Idaho 83720-0036
Attn: Dr. Kathryn Turner

H. Survival. The sections of this Agreement that by their nature are intended to continue in their effect following expiration or termination of this Agreement shall survive any expiration or termination of the Agreement.

IN WITNESS WHEREOF, the undersigned have caused this Agreement to be effective as of the Effective Date.

DHW :

By: _____
Name: Richard M. Armstrong
Date: _____
Title: Director, Department of Health and Welfare

Hospital:

By: _____
Name: _____
Date: _____
Title: _____

Attachment A: Idaho Department of Health and Welfare BioSense 2.0 User Password and Security Guidelines

As an authorized user of BioSense 2.0, and by logging in, you are indicating that you agree to the BioSense 2.0 conditions, including the terms and conditions, to protect the privacy and confidentiality of individuals and the protection of the data. User verifies that he/she is an authorized user of BioSense 2.0 and is carrying out authorized public health activities in his/her jurisdiction. Strong passwords are extremely important to prevent unauthorized access to your electronic accounts and devices.

BioSense 2.0 Password Requirements

- Passwords must contain at least eight (8) characters.
- The password must contain at least one of each:
 - Upper case letter
 - Lowercase letter
 - Number
- Passwords may not contain the username, first name, last name or spaces.
- Never give your password to anyone.
- Protecting your password is very important to guard against unauthorized access and misuse of service in your name.