BioSense: Implementation of Data Standards

Nikolay Lipskiy, MD, DrPH

Health Scientist

National Committee on Vital and Health Statistics (NCVHS),
Subcommittee on Standards

November 12, 2013

Center for Surveillance, Epidemiology, and Laboratory Services
Division of Health Informatics and Surveillance

Background

1. What Is the BioSense Program?

- The BioSense program is a public health surveillance system that increases the ability of health officials at local, state, and national levels to efficiently, rapidly, and collaboratively monitor and respond to harmful health effects of exposure to disease or hazardous conditions[1].
- BioSense provides public health officials a common electronic health information system with standardized tools and procedures for rapidly collecting, sharing, and evaluating information.
- BioSense 2.0 is a CDC-led effort partnering with CSTE, ASTHO, and NACCHO to create a user-driven, nationwide syndromic surveillance system[2].
- Implementation of BioSense promotes utilization of standardized syndromic surveillance data

2. What is the BioSense 2.0?

- The BioSense 2.0 is the latest version of the BioSense system.
- It is a streamlined collaborative data-exchange system that enables its users, who have agreed to share health-related data, to track health issues as they develop and to share this information quickly with other public health jurisdictions in the system.
- BioSense 2.0 provides a mechanism to collect and share information on emergency department visits, hospitalizations, and other health related data from multiple sources, including the Department of Veterans Affairs (VA), the Department of Defense (DoD), and civilian hospitals from around the country.
- BioSense 2.0 aims participants in exchanging data in more secure way.

Source: 1. CDC. BioSense Program. URL: http://www.cdc.gov/biosense/files/13_242388_K2_DHNDI_Biosense_topic_remediated%20508.pdf

Providing Data in a Distributed Cloud Environment

1. BioSense 2.0 is the first Department of Health and Human Services system to move completely to a distributed cloud computing environment.

2. It was developed and is governed through an active collaboration of CDC, state and local health departments, and other public health partners

3. Cloud computing gives participating health departments easily managed on-demand access to a shared pool of configurable computing resources such as networks, servers, software, tools, storage, and services, with limited need for additional IT support.

4. Through the use of these common resources, BioSense 2.0 users gain significant efficiency, cost reduction, and information-sharing capabilities.

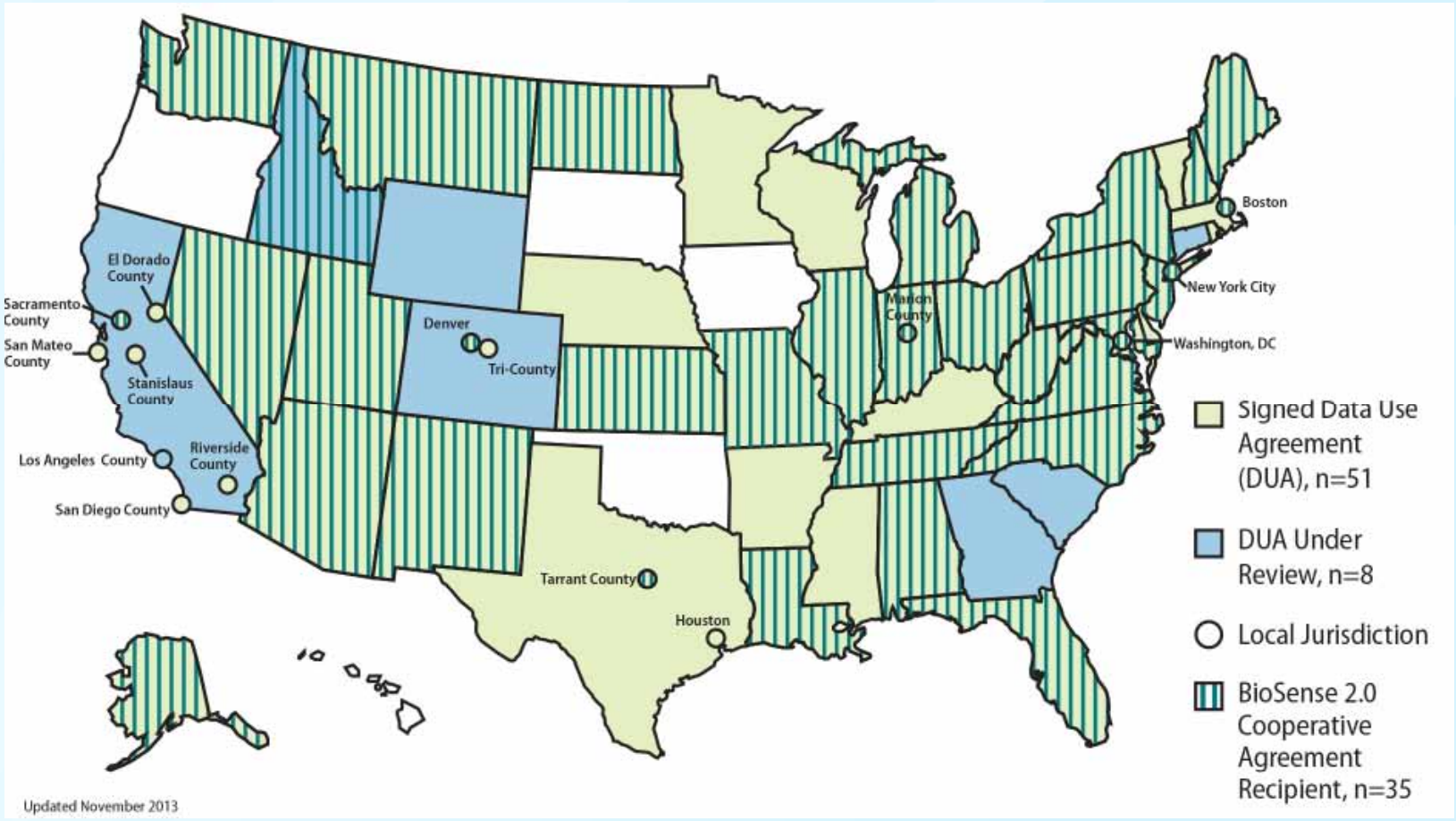
5. BioSense 2.0 enables participants to securely exchange data.

6. BioSense 2.0 also provides local and state users free secure data storage space, an easy-to-use data display dashboard, and, most importantly, a shared environment where users can collaborate and advance public health surveillance practice.

Source: 1. CDC. BioSense Program. URL: http://www.cdc.gov/biosense/files/13_242388_K2_DHNDI_Biosense_topic_remediated%20508.pdf

BioSense 2.0 Signed Data Agreements

Several States and an ever-changing number of local jurisdictions are engaged in ongoing recruitment.



BioSense 2.0 and Meaningful Use (MU) Requirements

1. BioSense 2.0 expands the capacity of state and local health departments to support MU programs intended to expand the use of electronic health records.

2. The capability to submit electronic syndromic surveillance data to public health agencies and actual submission according to applicable law and practice was added as the objective into the CMS Final Rules EHR Incentive Program[1]

3. BioSense 2.0 can serve as a proxy for receiving syndromic surveillance messages in Stage 1 and 2 of MU, and enable a network of surveillance peers to share analyses and data[2]

4. Society for Disease Surveillance (ISDS) and CDC, working with partners, developed *the PHIN Messaging Guide for Syndromic Surveillance: Emergency Department and Urgent Care Data Release 1.0 (HL7 Version 2.5.1 (Version 2.3.1 Compatible))* [3] with a minimum data set and definitions that support syndromic surveillance practice. It was implemented by redesigned BioSense 2.0 program

Source: 1. CMS Final Rules EHR Incentive Program. URL: http://edocket.access.gpo.gov/2010/pdf/2010-17207.pdf
2. Public Health Information Network (PHIN) meaningful Use Fact-Sheet. Syndromic Surveillance. URL: http://www.cdc.gov/phin/library/PHIN_Fact_Sheets/FS_MU_SS.pdf
3. PHIN Messaging Guide for Syndromic Surveillance: Emergency Department and Urgent Care Data Release 1.0 (HL7 Version 2.5.1 (Version 2.3.1 Compatible)). URL: http://www.cdc.gov/phin/library/guides/PHIN_MSG_Guide_for_SS_ED_and_UC_Data_v1_0.pdf

Assuring Security, Privacy and Standardization of Syndromic Surveillance Data

- BioSense 2.0 promotes implementation of the *ISDS Final Recommendation: Core Processes and EHR Requirements for Public Health Syndromic Surveillance, 2011* [1]

- These Recommendations guide on development of a secure and standardized data exchange environment for participants
  - ❑ through described Business processes for
    - ➢ *Data sharing partnership*
    - ➢ *Conducting quality assurance*
  - ❑ by recommending Minimum Data
  - ❑ by recommending standards for data elements

- The public health standard used in BioSense is the Public Health Information Network Messaging System (PHINMS) guide for public health surveillance for emergency rooms, urgent care facilities, and ambulatory clinics [2]

- PHINMS allows the effective exchange of messages as a bi-directional and secure messaging platform. It provides a common approach to security requirements (such as encryption and authentication), as well as a standard method for addressing and routing content [3]

Source: 1. Final Recommendation: Core Processes and EHR Requirements for Public Health Syndromic Surveillance, 2011. URL: http://www.syndromic.org/storage/ISDSRecommendation_FINAL.pdf
2. Implementation Guide. Public Health Information Network Messaging System (PHINMS). URL: http://www.cdc.gov/phin/library/resources/Tools/PHINms/PHINMS%20Implementation%20Guide%20v2%208%2002_10_31_2012.pdf
3. PHIN Messaging System. URL: http://www.cdc.gov/phin/tools/PHINms/installation.html

What Security Standards Should Apply to Data Possessed by Public Health?

- **Federal Information Security Management Act of 2002 (FISMA)** [1]
  - Requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.
  - The National Institute of Standards and Technology (NIST) provides detailed information toward compliance with FISMA[2]

- **NIST Special Publications**
  - Publication 800-53, *Recommended Security Controls for Federal Information Systems and Organizations,2013* [3]. This document lists the control families and the individual controls and enhancements that must be put in place and documented to maintain the security of the data.

- **The Federal Information Processing Standards Publication (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems**
  - Provides a method to determine the impact level of the information and the damage that may be done if the confidentiality, integrity, or availability is compromised.

Resources: 1. Federal Information Security Management Act of 2002. URL: http://csrc.nist.gov/drivers/documents/FISMA-final.pdf
2. NIST. FISMA- Detailed Overview. URL: http://csrc.nist.gov/groups/SMA/fisma/overview.html
3. NIST SP 800-53. Security and Privacy Controls for Federal Information Systems and Organizations. URL: http://csrc.nist.gov/publications/PubsSPs.html#800-53
4. FISP PUB 199. Standards for Security Categorization of Federal Information and Information Systems , 2004. URL: http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

BioSense 2.0 Data Elements

Recommended data elements - 32 data elements from the ISDS *Final Recommendation: Core Processes and EHR Requirements for Public Health Syndromic Surveillance, 2011**

Categories of Data Elements

Treatment Facility Identifiers

- Facility Identifier (Treating)
- Facility Name (Treating)
- Facility Location (Treating)
  - Street Address
  - City
  - County
  - State
- Facility/Visit Type
- Report Date/Time

Patient Demographics

- Unique Patient Identifier
- Medical Record #
- Age
- Age Units
- Gender
- Race
- Ethnicity
- City/Town
- Zip Code
- State
- Country

Patient Residence

Patient Health Indicators

- Unique Visiting ID
- Visit Day/Time
- Date of Onset
- Patient Class
- Chief Complaint/Reason for Visit
- Triage Notes
- Diagnosis/External Cause of Injury Code
- Clinical Impression
- Diagnosis Type
- Discharge Disposition
- Disposition Date/Time
- Initial Temperature
- Initial Pulse Oximetry

Source: Final Recommendation: Core Processes and EHR Requirements for Public Health Syndromic Surveillance, 2011.
URL: http://www.syndromic.org/storage/ISDSRecommendation_FINAL.pdf

Recommended by BioSense 2.0 Data Standards

- Implementing by BioSense 2.0 data elements aims participants in standardization of data exchange
- Data standards for these data elements are referenced in the ISDS Recommendations*
- The following are examples of referenced and recommended data standards:
  - Gender- HL7 v 2.5.1 Administrative Sex (Table 0001)
  - Race- CDC Race Categories
  - Ethnicity – CDC Ethnicity Group Value Set
  - Chief Complain/Reason for Visit- LOINC codes, ICD-9-Clinical Modification (CM), ICD-10-CM or free text
  - Triage Notes – LOINC codes or free text
  - Diagnosis/External Cause of Injury Code- ICD-9 CM (including E- and V- codes), ICD-10-CM, SNOMED
  - Clinical Impression - LOINC

Source: Final Recommendation: Core Processes and EHR Requirements for Public Health Syndromic Surveillance, 2011. URL: http://www.syndromic.org/storage/ISDSRecommendation_FINAL.pdf

CDC Participation in Standardization of Syndromic Surveillance, Implementation of Privacy and Security

- CDC Office of Public Health Scientific Services (OPHSS) leads and coordinates CDC participation is development and implementation of syndromic surveillance standardization, gathering privacy and security recommendations
- The OPHSS Standards and Interoperability program works with internal and external to CDC partners on assessment and sharing privacy and security rules as it regulated by HIPAA, HHS, ONC etc.[1]
- Also, this program works with internal and external to CDC partners on assessment and sharing Syndromic Surveillance Data Interchange Standards through a publicly available web site[2]
- CDC Vocabulary and Distribution System (VADS) [3] maintains a repository of standardized syndromic surveillance value sets and gathers through a publicly available web site [3]

Sources: 1. Public Health Information Network, PHN. Data Interchange Standards. HIPAA Privacy and Security Rules for Public Health Data Exchange. URL: http://www.cdc.gov/phin/resources/standards/data_interchange.html
2. Public Health Information Network, PHN. Data Interchange Standards. Surveillance. Syndromic Surveillance. URL: http://www.cdc.gov/phin/resources/standards/data_interchange.html
3. PHIN Vocabulary and Distribution System (VADS). Value sets associated with PHIN Messaging Guide for Syndromic Surveillance. URL: http://phinvads.cdc.gov/vads/ViewView.action?id=1FF0B1F8-F796-E211-89A9-0017A477041A

Thank you!

For more information please contact Centers for Disease Control and Prevention

1600 Clifton Road NE, Atlanta, GA 30333
Telephone: 1-800-CDC-INFO (232-4636)/TTY: 1-888-232-6348
Visit: www.cdc.gov | Contact CDC at: 1-800-CDC-INFO or www.cdc.gov/info