The Challenge
Centers for Disease Control and Prevention's (CDC) BioSense Program was originally launched in 2003 to address the mandate of the Public Health Security and Bioterrorism Preparedness and Response Act of 2002, to establish an "integrated system" of nationwide "biosurveillance" for early detection and prompt assessment of potential bioterrorism-related illness. Much of the data collected in the program was sent from health care facilities directly to CDC, bypassing the routes established for public health surveillance data, resulting in limited participation in BioSense by state and local health departments and an incomplete, non-representative picture of situation awareness in the US. The data received by the BioSense Program resulted in substantial IT costs associated with data receipt, storage and processing. In order to overcome these challenges, BioSense must: 1) be controlled by the community; 2) be computationally distributed; 3) incorporate State and Local public health partner input; and 4) promote a proactive, collaborative, and transparent community.

The Solution
The redesigned BioSense Program, or BioSense 2.0, offers unique attributes, such as an environment that allows for sharing of data among jurisdictions, the development and support of shared analytical capabilities, shared governance of the program by key stakeholders, and the use of a cloud computing technology to revolutionize the way that public health surveillance is conducted. BioSense 2.0 is the first Department of Health and Human Services (DHHS) system to completely move to the Internet cloud. BioSense 2.0 set and achieved a roll out date of November 15, 2011.

The Benefit
BioSense 2.0 significantly enhances nationwide and regional "all hazards" situation awareness, or monitoring and projecting changes in population health, by accelerating and expanding state and local capacity to conduct syndromic surveillance and share information. This switch from traditional, expensive IT infrastructure allows us to realize a significantly more efficient means for using already limited funds at CDC and at state and local levels. The focus has shifted to sustaining capacity at the state and local health departments by helping to alleviate financial constraints and redirecting funding for human capacity to perform surveillance activity. In coordination with the DHHS mission, BioSense 2.0 has aligned itself with the Medicare and Medicaid Electronic Health Records (EHR) Incentive Programs ("Meaningful Use" programs) where syndromic surveillance is one of three population health options. BioSense 2.0 provides state and local public health authorities with a low-cost option for receiving and processing these EHR data from healthcare providers, aka the "Catcher's Mitt".

Information Assurance Summary for BioSense 2.0
BioSense 2.0 was accredited and approved to operate on 14 Nov 2011 (approved at FISMA-MODERATE)

- The system went into live operations on 15 Nov 2011
- The BioSense 2.0 application / environment received an Authorization to Operate (ATO) from CDC. It has been through the CDC's Certification & Accreditation process, which meets Federal Information Security Management Act (FISMA) requirements.
- CDC incorporates the use of National Institute of Standards and Technology (NIST) Special Publications (computer security guidance) in its Certification and Accreditation (C&A) processes. Some of the guidance specifically incorporated can be found in:
    - NIST SP 800-18: Guide for Developing Security Plans for Federal Information Systems
    - NIST SP 800-37: Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
    - NIST SP 800-53: Recommended Security Controls for Federal Information Systems and Organizations

  Note: The FISMA requirements and NIST guidance are publicly available. The NIST guidance is collected in the Computer Security Resource Center of the National Institute of Standards and Technology (NIST) site: http://csrc.nist.gov/publications/PubsSPs.html
- BioSense 2.0 system information is backed-up by system administrators on a nightly basis and is reviewed on a monthly basis for completeness and correctness.
- The Amazon S3 storage infrastructure employs multiple copies of data to ensure it can be recovered if necessary.
- The BioSense 2 partitioned storage architecture makes use of AWS native infrastructure protections
    - AWS distributed storage (S3) provides robust countermeasures against data loss
    - Objects stored in a Region never leave the Region unless you transfer them out. For example, objects stored in the GovCloud never leave the GovCloud.
    - Authentication mechanisms are used to ensure that data is kept secure from unauthorized access.
    - Only data owners have access to the Amazon S3 resources they create.

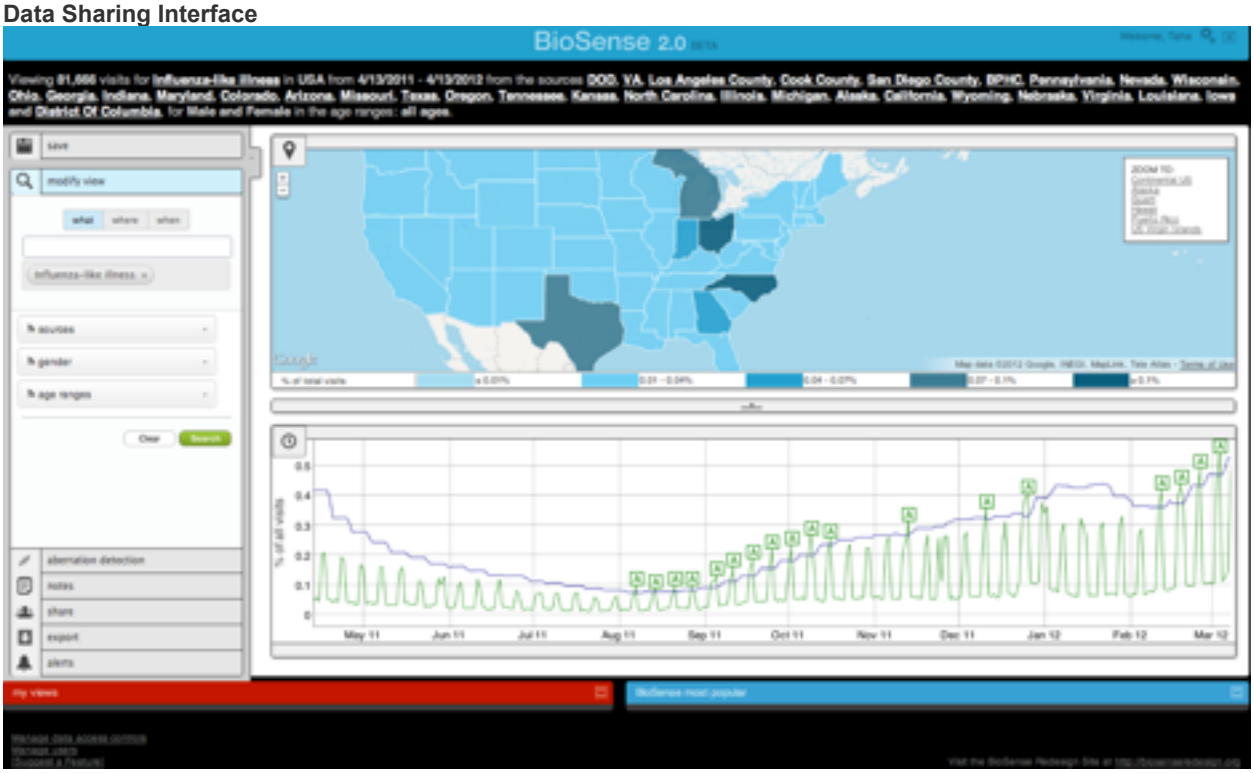
Additional Details
For additional information, please refer to the following:

- BioSense 2.0: Public Health Surveillance thru Collaboration
- CDC's BioSense Site

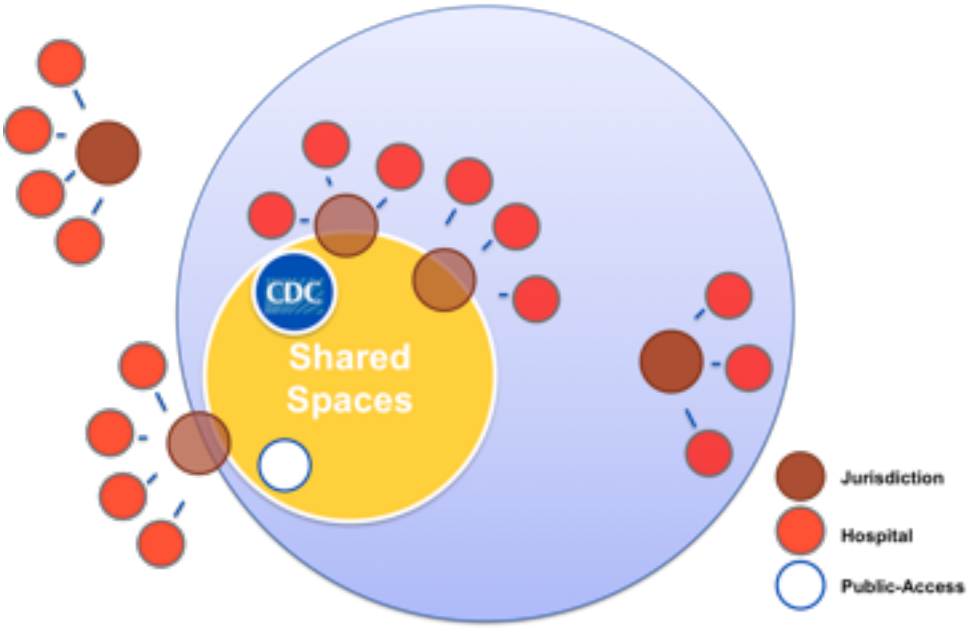
- BioSense 2.0 Collaboration Site
- CDC's BioSense 2.0: Bringing Together the Science and Practice of Public Health Surveillance, The American Journal of Preventive Medicine's Blog
- Trust for America's Health (TFAH 2011): Ready or Not? Page#67
- Link to Video here

For more information, email info@biosen.se

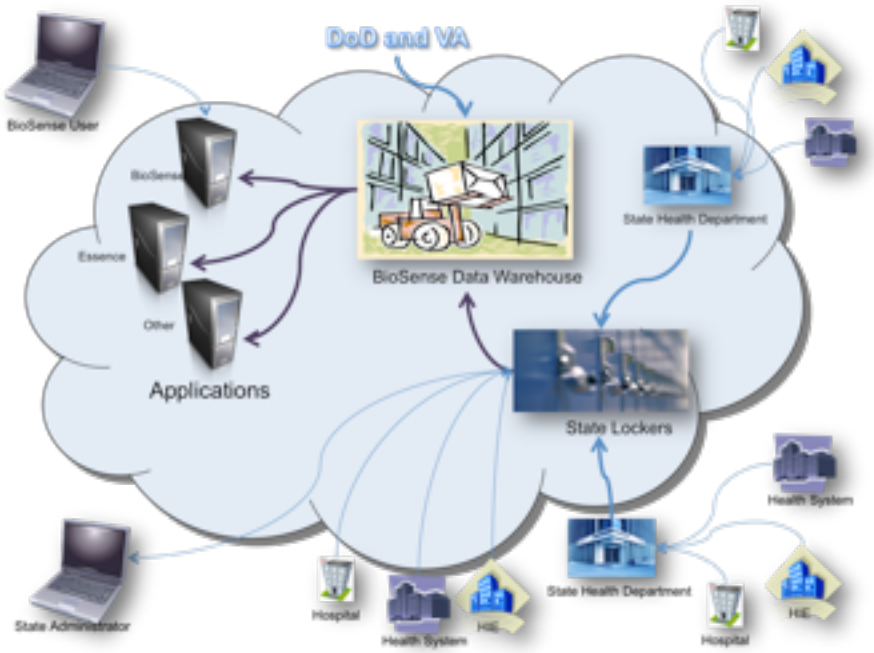
Data Sharing Interface



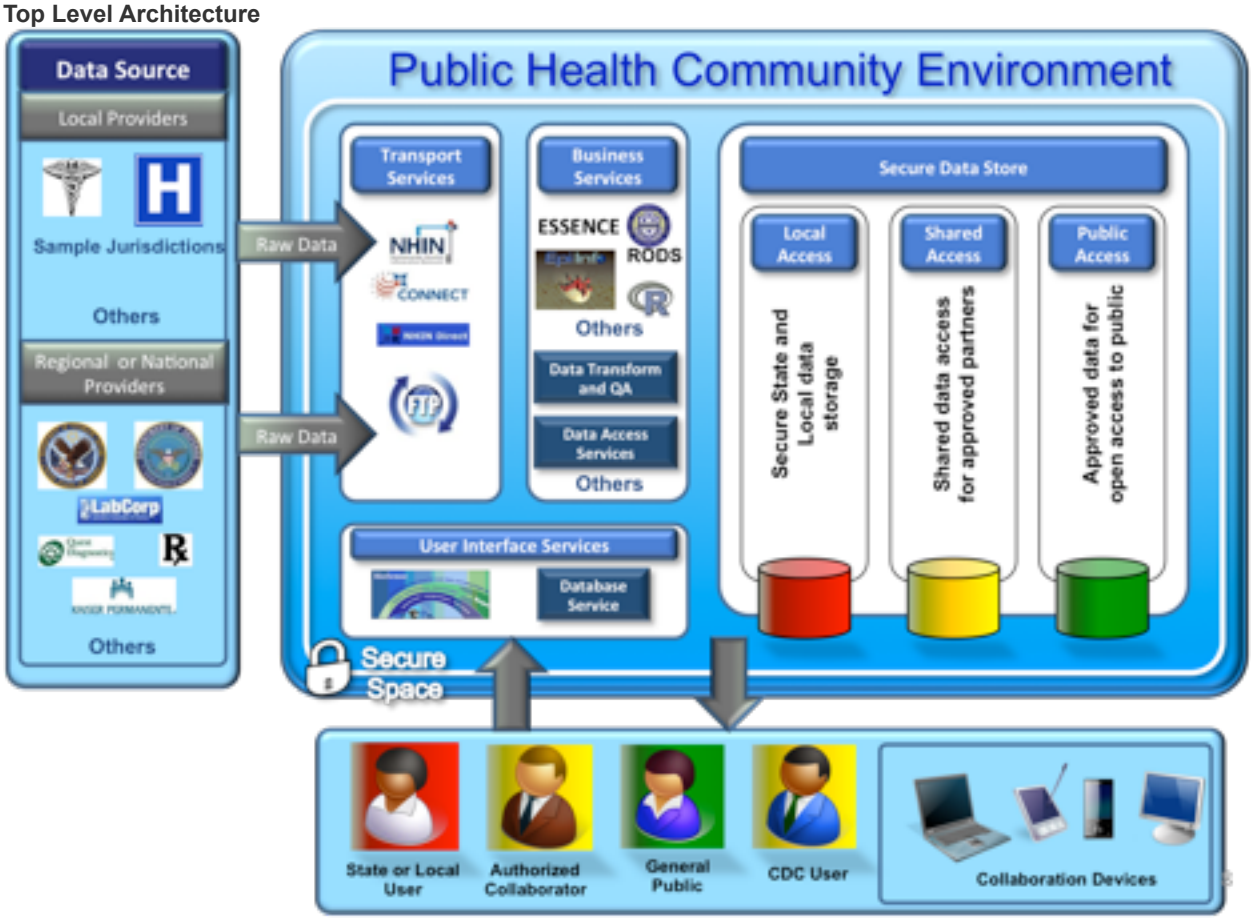
Business Model



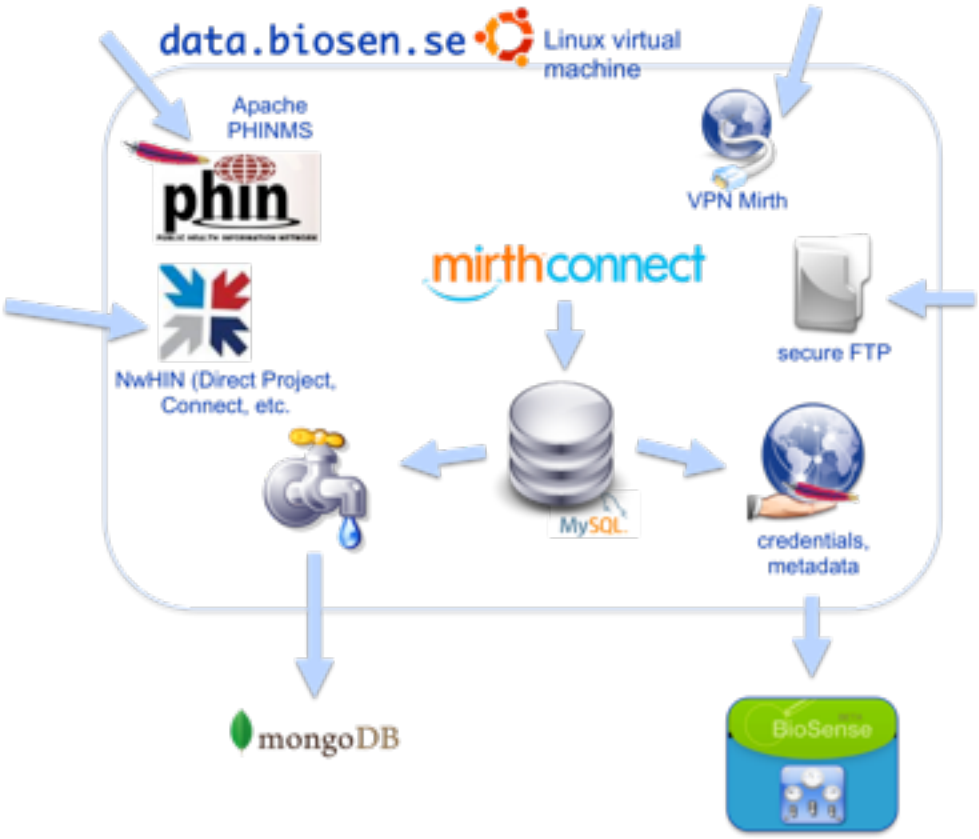
Functional Diagram



Top Level Architecture



Transport Services



Direct and NwHIN

Application

http://biosen.se Linux virtual machine

mongoDB

php

NGINX