

# Bio Terror Bible

## EXPOSING THE COMING BIO-TERROR PANDEMIC

**BIO TERROR BIBLE.COM:** There are seven major bio-terror surveillance and response networks that have been identified as operational throughout the United States and the World. Should a major bio-terror attack occur followed by a real or engineered pandemic, the following entities will be responsible for monitoring, guiding, **hyping** and ultimately stopping the pandemic.

1. [BioWatch](#)
2. [ESSENSE](#) (Electronic Surveillance System For The Early Notification of Community-Based Epidemics)
3. [GEIS](#) (Global Emerging Infections Surveillance)
4. [HAN](#) (Health Alert Network)
5. [LRN](#) (Lab Response Network)
6. [RODS](#) (Real-Time Outbreak Disease Surveillance)
7. [SS](#) (Syndromic Surveillance)

## 1. BioWatch

**Title:** [BioWatch](#)  
**Date:** 2012  
**Source:** [Wikipedia](#)

**Abstract:** BioWatch is a United States Federal Government program to detect the release of [pathogens](#) into the air as part of a [terrorist](#) attack on major [American](#) cities. Reportedly operating in [Philadelphia](#), [New York City](#), [Washington, DC](#), [San Diego](#), [Boston](#), [Chicago](#), [San Francisco](#), [St. Louis](#), [Houston](#), [Los Angeles](#) and 21 other cities, the BioWatch program was created in 2001 in response to the increased threat of bioterrorism sparked by the [2001 anthrax attacks](#), and was announced in [President George W. Bush's State of the Union Address](#) of 2003.

The program, described as "the nation's first early warning network of sensors to detect biological attack" operates via a system of filters located within existing [Environmental Protection Agency](#) air filters which monitor the quality of the air. Results from these filters are analyzed by the [Centers for Disease Control and Prevention](#) who then pass any significant results to the Federal Bureau of Investigation ([Wikipedia, 2012](#)).

**Title:** [U.S. Is Deploying A Monitor System For Germ Attacks](#)  
**Date:** January 22, 2003  
**Source:** [UCLA](#)

**Abstract:** To help protect against the threat of bioterrorism, the Bush administration on Wednesday will start deploying a national system of environmental monitors that is intended to tell within 24 hours whether anthrax, smallpox and other deadly germs have been released into the air, senior administration officials said today.

The system uses advanced data analysis that officials said had been quietly adapted since the Sept. 11 attacks and tested over the past nine months. It will adapt many of the Environmental Protection Agency's 3,000 air quality monitoring stations throughout the country to register unusual quantities of a wide range of pathogens that cause diseases that incapacitate and kill.

Officials said that although the system would not by itself protect Americans against a germ attack, early detection of such a strike would give the government more time to mobilize medical resources that could save thousands, and even hundreds of thousands of lives. The faster those exposed to most deadly pathogens are vaccinated against a disease, or treated with antibiotics to combat it, the lower the death rate.

Under the system, the E.P.A. monitoring stations will send samples of a tissue-like paper from newly upgraded machines that filter air to the closest of some 120 laboratories across the country associated with the federal Centers for Disease Control and Prevention. Results will be available within 24 hours, and possibly within 12 hours.

Although officials declined to say which or how many E.P.A. monitoring stations would ultimately be used, experts on the government's program said the first environmental monitoring stations in the new system, called Bio-Watch, were in New York. The city has more than seven such stations. The stations, which are all outdoors, now mainly monitor for air pollution.

"We will ramp up to other cities and areas of concentrated populations very quickly," one official said. "Within a matter of days, we will be able to tell in almost any major urban area whether a large release of a dangerous pathogen has occurred, what was released, and where and when it occurred."

Officials said today the introduction of the system by the newly created Department of Homeland Security was not linked to a specific terrorist threat. The intelligence community, one senior official noted, has "no credible evidence that Al Qaeda has acquired biological weapons, or any weapon of mass destruction at this time."

But the system is being deployed as the Bush administration moves toward deciding whether to use military force against Iraq. After the 1991 Persian Gulf war, Iraq declared having made thousands of gallons of liquid anthrax, botulinum toxin and other pathogens that cause disease, and it may have kept stocks of deadly smallpox virus as well.

Although Baghdad says it has destroyed these stockpiles, American officials believe it is hiding some of its chemical and germ agents, and that it tested anthrax as an aerosol before the gulf war.

However, one senior official said, the new environmental surveillance system was not being deployed specifically because of Iraq, but "to prepare the country for whatever the weapon and whomever the culprit might be."

While environmental monitoring does not provide instant detection of the release of a dangerous germ, the new system is aimed at giving health officials more time to send doctors, vaccines, antibiotics and medical equipment to the scene of a bioterror attack. Doctors and terrorism experts have long said that the lack of such a system is one of the most glaring deficiencies in the nation's biodefenses.

While the government is still working to develop cheap and reliable instant detectors, the technology has yet to be perfected, officials said. The hand-held detectors, which have been distributed in some cities, and others that are now being tested provide what experts call too many "false positives" — mistaken identifications of a germ release.

The new environmental surveillance system uses monitoring technology and methods developed in part by the Department of Energy's national laboratories. Samples of DNA are analyzed using polymerase chain reaction techniques, which examine the genetic signatures of the organisms in a sample, and make rapid and accurate evaluations of that organism.

Officials who helped develop the system said that tests performed at Dugway Proving Ground in Utah and national laboratories showed that the system would almost certainly detect the deliberate release of several of the most dangerous pathogens. "Obviously, the larger the release, the greater the probability that the agent will be detected," an official said. "But given the coverage provided by the

E.P.A. system, even a small release, depending on which way the wind was blowing and other meteorological conditions, is likely to be picked up."

The [anthrax attacks](#) of October 2001 would probably not have been detected by the new system, officials said, mainly because the outbreak was caused by a tiny amount of anthrax — one to two grams — and because the release was indoors, where the sensors do not monitor.

Officials said the new system would not detect releases in such places as shopping malls, subways and other covered areas.

"But the system is calibrated to detect relatively small amounts of some of the agents of greatest concern," an official said, referring to smallpox and larger releases of anthrax.

While officials declined to disclose how much the program would cost, they said it was relatively inexpensive. They said it would cost about \$1 million to provide upgraded filters to the selected air quality monitoring stations and another \$1 million per city a year for analyzing samples.

A senior administration official said the White House did not plan to announce the start of the system ([UCLA, 2012](#)).

## 2. ESSENSE

**Title:** Essence (Electronic Surveillance System For The Early Notification of Community-Based Epidemics)

**Date:** 2012

**Source:** [Wikipedia](#)

**Abstract:** Essence is the [United States Department of Defense](#)'s Electronic Surveillance System for the Early Notification of Community-based Epidemics. Essence's goal is to monitor health data as it becomes available and discover [epidemics](#) and similar health concerns before they move out of control ([Wikipedia, 2012](#)).

**Title:** ESSENCE II And The Framework For Evaluating Syndromic Surveillance Systems

**Date:** September 24, 2004

**Source:** [CDC](#)

**Abstract:** The Electronic Surveillance System for the Early Notification of Community-Based Epidemics (ESSENCE II) is a prototype syndromic surveillance system for capturing and analyzing public health indicators for early detection of disease outbreaks.

### Objectives

This paper presents a preliminary evaluation of ESSENCE II according to a CDC framework for evaluating syndromic surveillance systems.

### Methods

Each major topic of the framework is addressed in this assessment of ESSENCE II performance.

### Results

ESSENCE captures data in multiple formats, parses text strings into syndrome groupings, and applies multiple temporal and spatio-temporal outbreak-detection algorithms. During a recent DARPA evaluation exercise, ESSENCE algorithms detected a set of health events with a median delay of 1 day after the earliest possible detection opportunity.

### Conclusions

ESSENCE II has provided excellent performance with respect to the framework and has proven to be a useful and cost-effective approach for providing early detection of health events.

## Introduction

In response to the threat of biologic terrorism and the resurgence of virulent forms of infectious diseases, technologic advances are being applied to disease surveillance. Syndromic surveillance systems have emerged to capture and analyze health-indicator data to identify abnormal health conditions and enable early detection of outbreaks. Given the limited public health experience with biologic terrorism and the variety of possible terrorism scenarios, the research community is exploring the application of advanced detection technology to prediagnostic syndromic data. In 2003, CDC issued a draft framework for evaluating syndromic surveillance systems (1), which was later revised and published in MMWR (2). The CDC framework is designed for evaluation of relatively mature, fully operational syndromic surveillance systems. The technology to support syndromic surveillance is just maturing, with current operational experience gained from test-bed use. This paper applies the framework to the Electronic Surveillance System for the Early Notification of Community-Based Epidemics (ESSENCE), a series of prototype systems developed by Johns Hopkins University Applied Physics Laboratory (JHU/APL) and the Division of Preventive Medicine at the Walter Reed Army Institute of Research.

## System Description

### Purpose

Multiple versions of ESSENCE have been developed, each for different purposes. ESSENCE I provides worldwide surveillance for military personnel and their dependents at all military treatment facilities by using ambulatory records generated for TriCare, the military's health-care system. ESSENCE II is a regional system that supports advanced surveillance within the National Capital Region (NCR) test bed. The system is being developed by JHU/APL in collaboration with the Maryland Department of Health and Mental Hygiene, the District of Columbia Department of Health, and the Virginia Department of Health. Other versions of ESSENCE have been developed for military facilities and deployed forces. This description focuses on ESSENCE II only.

ESSENCE II is a test-bed system for 1) evaluating nontraditional health-care indicators, 2) developing and evaluating analytic techniques for early identification of abnormal disease patterns, and 3) providing an integrated view of NCR military and civilian health department data (3) (Figure 1). The system captures data on military ambulatory visits and prescription medications and merges them with civilian emergency department (ED) chief-complaint records, school-absenteeism data, over-the-counter (OTC) and prescription medication sales, civilian ambulatory visits, veterinary health records, and health department requests for influenza testing. All data are de-identified by their providers before being transferred to ESSENCE II, where they are archived, analyzed, and provided through secure Internet sites to local health departments and to hospitals that have data-sharing agreements with their health departments.

### Stakeholders

NCR health departments conduct surveillance by using ED chief-complaint data from hospitals within and around the District of Columbia metropolitan area. ESSENCE II helps automate the processes of capturing hospital data, parsing chief-complaint text strings, and analyzing data for abnormalities.

ESSENCE technology is being used to form a regional collaborative disease-surveillance network. The network consists of four major nodes, one at each state and District of Columbia health department and a regional node for performing analysis across jurisdictional boundaries. The architecture permits fully identifiable information to be captured and archived at health departments for patients within their jurisdiction. The regional node negotiates the acquisition and distribution of data (e.g., military health-care data and OTC medication sales) across the region. The architecture also permits de-identification, aggregation, and sharing of information among the region's health departments while increasing the sensitivity for detection of abnormal health events occurring across jurisdictional boundaries.

### Operation

The data flow through an ESSENCE II node is illustrated. First, to expedite data collection and maintain confidentiality, the data providers create automated query software to extract recent data elements from their archives. These extractions are assembled into a de-identified update record, encrypted, and posted to a secure file transfer protocol (FTP) site. The query software automatically

executes at a regular interval (e.g., daily at midnight or once every 8 hours) that can be changed easily. Although ESSENCE II can accept Health Level 7 (HL7) (4) data streams, the majority of data providers prefer the automated query approach. ESSENCE II polls the FTP sites to look for new entries, which are then ingested, cleaned, formatted, and archived in the primary system archive.

Data-sharing policies across the region have not been approved by all NCR health departments. After these policies are approved, selected data fields or aggregates of counts will be transmitted to other nodes in the network.

Chief-complaint data from hospital EDs 1) are received as text strings, which are of variable length; 2) include punctuation, misspellings, or abbreviations; and 3) can use varying syntax and vocabularies. A chief-complaint parsing algorithm developed for ESSENCE II converts text strings into syndrome groupings (5). The syndrome groupings agreed to by the NCR health departments are death, gastrointestinal, neurologic, rash, respiratory, sepsis, unspecified, and other, but the chief-complaint parsing algorithm can easily accommodate modifications. After ED data are entered into the primary archive, the parsing algorithm automatically converts the text strings into syndrome groupings. When the parser's performance is compared with that of human coders, the parser provides, on average, 97% sensitivity and 99% specificity. Whenever new hospital EDs are added to the system, the parser's performance is assessed to adjust for unfamiliar textual information. The algorithm provides approximately perfect conversion into syndrome groupings for the most prevalent syndromes (respiratory and gastrointestinal) and degraded performance for those less frequent (neurologic).

In addition to ED chief-complaint information, ESSENCE II also receives data from physician-encounter claims in the form of International Classification of Diseases, Ninth Revision (ICD-9) codes and from retail merchants in the form of Universal Product Codes (UPCs) for OTC medications. These data are grouped into the same syndrome categories as the chief-complaint data to enable outbreak detection by syndrome.

Next, ESSENCE II applies outbreak-detection algorithms. These algorithms use a working archive known as the detection archive. New records are moved into the detection archive at the launching of the detection process. The detection algorithms are run every 4 hours, although this interval is adjustable. ESSENCE II can accommodate HL7 data streams if they are available from the hospital. Temporal and spatio-temporal algorithms are implemented in ESSENCE II to determine abnormalities. Also included are reference algorithms for assessing the performance enhancement provided by the ESSENCE II algorithms. CDC's Early Aberration Reporting System (6) algorithms were chosen as reference algorithms because they were already in use by regional health departments.

ESSENCE II uses two temporal algorithms: 1) an autoregressive modeling algorithm that predicts syndrome counts and looks for differences between actual counts and estimates and 2) the exponentially weighted moving average (EWMA), a statistical process control method. Details on these algorithms are published elsewhere (7). The autoregressive algorithm is based on a linear regression model that predicts a continually fluctuating daily expected count and threshold. The model bases its daily predictions on the previous 4 weeks of ESSENCE data, accounting for the day of the week and whether the day is a holiday or the day after a holiday. (The holiday function serves to explain artificial peaks in the data attributable to surges in patient visits after days when clinics are closed.) EWMA compares each observation to an average of past data that weights observations exponentially by time so that the most recent observations are most influential. Therefore, EWMA can be used when daily visit counts do not have the temporal structure required by a regression model. ESSENCE II uses a built-in goodness-of-fit statistic to determine whether the regression is useful in explaining the data; when this test fails, the automated checking process switches to EWMA.

A variant of the spatial scan statistic (8) is used to form clusters in time and space across the region by using zip codes as the smallest spatial resolution. The scan statistic has been modified to include multiple sources (9), which increases the sensitivity while controlling the false-alert rate.

ESSENCE II uses a secure website to transfer information to its users. Users must use individual passwords to access the website and can only access information for their respective jurisdictions. Four ESSENCE II portals enable users to view raw data and results from processed data:

1. A map portal displays geographic distribution of raw data and clusters formed by scan statistics. The user can select data elements for geographic display and access details by clicking on the location of the data provider or the zip code(s) of interest. The details can be presented as tables or time graphs.
2. The second portal provides alert lists for the output of the detection processes. These lists consist of color-coded flags to indicate algorithm outputs that are higher than expected. Upper confidence limits (UCLs) for the daily predictions are computed and used as alerting thresholds. If an observed count exceeds the 95% UCL but not the 99% UCL, a low-level (yellow) alert is generated; if it exceeds the 99% UCL, a high-level (red) flag results. The user can organize the lists to provide flags on data of interest, sort lists by elements of interest, and access data or link to the map portal to view the spatial distribution that resulted in the flag.
3. The query portal enables a user interested in specific data to select from drop-down menus and view selected data elements over a selected timeframe as graphs or tables. All tabular information can be cut and pasted into a spreadsheet program for analysis offline.
4. The fourth portal enables users to generate summary reports for export outside ESSENCE II. The user can select any data elements in the archive and view historic counts as well as upward or downward trends. This portal also contains tutorial material on operating ESSENCE II and a message board for making suggestions to developers or sharing thoughts with other users.

## **Outbreak Detection**

### **Timeliness**

The purpose of syndromic surveillance is to detect as early as possible abnormal disease patterns that could result in high mortality. This new technology should be evaluated and compared with traditional techniques to determine whether it improves upon detection timeliness. At least five layers of possible improvement exist (Figure 4). At each layer, the improvement is compared with a standard method to determine whether timelier notification is possible.

1. The first layer is the acquisition of a data source that contains an early indicator. For example, one promising data source is the nurse hotline service provided by certain health-care organizations.
2. The second layer involves filtering of the data stream to more closely match the population that exhibits early symptoms of disease. For example, because symptoms consistent with the release of a biologic agent at a facility (e.g., the Pentagon) would probably be observed among active-duty personnel at that facility, military data could be filtered by age to separate active-duty, retired, and dependent populations.
3. The third layer removes confounders from nontraditional data sources. For example, OTC medication sales are strongly influenced by sales promotions, seasonal effects, and day-of-week activity, as well as by the socioeconomic status of the community in which the sale occurred. ESSENCE II uses algorithms to model these confounders and remove their influence, thus allowing identification of the underlying pattern attributable solely to increases in disease.
4. The fourth layer addresses improvements to outbreak-detection algorithms that use a single data stream. Signal processing, regression modeling, and process control methods have been used to monitor single data streams.
5. The fifth layer addresses multivariate methods for gaining sensitivity needed for early recognition of an abnormality.

Improvements at any of the five layers or combination of layers can improve notification timeliness.

CDC's framework (1,2) provides a timeline, consisting of nine "anchor points," for measuring timeliness and performance of syndromic surveillance. The first three anchor points, point-source exposure, symptom onset, and health-seeking behavior, are independent of system performance; symptom onset is a function of the incubation period of the disease, and health-seeking behaviors depend on socioeconomic factors. The fourth anchor, capture of the behavior in the record, varies by

data source, taking only seconds for scanning in OTC medications or hours to days for electronic claims. The fifth anchor point, data source ready to share, depends on the data provider and on system requirements for data updates. Data can be sent in real time (e.g., an HL7 feed from a hospital), hourly, daily, or at other predetermined intervals (e.g., ED chief-complaint data could be accumulated over 1 day and sent at midnight). ESSENCE II accepts both HL7 and ED chief-complaint data feeds. The data-ingestion module within ESSENCE II automates the capture data into the system process (anchor point six) within seconds. The seventh anchor point, apply pattern-recognition tools/algorithms, is also a function of the data-capture rate. If data are captured in real time, the detection algorithms must also operate in near real time. If data are captured daily, then the algorithms must be applied daily. ESSENCE II captures data throughout the day and applies the detection process every 4 hours but can alter the processing period when real-time data are received. After the detection process is complete, the automated alert generation process (anchor point eight) takes only seconds to minutes. The ninth anchor point, initiate public health response, depends upon policies and personnel at individual health departments and is independent of the syndromic surveillance system.

### **Validity**

Algorithm performance can also be evaluated by detection of actual disease events within the community. In summer 2003, the ESSENCE II project participated in a blind evaluation conducted by the Defense Advanced Research Projects Agency (DARPA) Bio-ALIRT Program (11). This evaluation provided the opportunity for independent validation of results from the ESSENCE II outbreak-detection process and independent evaluation of participating syndromic surveillance systems. To conduct the evaluation, DARPA assembled an independent team of epidemiologists and physicians to identify respiratory and gastrointestinal events in data streams from five cities. The data included military and civilian ambulatory records and military prescription records. Team members identified eight respiratory and seven gastrointestinal events and, given only the raw data streams, were asked to estimate 1) start dates for the event, 2) date when a health department might recognize the event, 3) the peak of the event, and 4) the end of the event. Participants whose algorithms were being evaluated were provided only the raw data streams and asked to identify events.

Three ESSENCE II detection methods were selected for this evaluation (10): 1) a multivariate statistical process control algorithm applied to the residuals of a regression technique used to control for unexplained data dropouts, 2) a multiple univariate method based on the EWMA control chart, and 3) a Bayesian Belief Network applied to the outputs of the first two algorithms to optimize the decision for the two detectors. The results of these algorithms' detection performance and timeliness are provided as a function of false-alert rate, for rates of one false alert every 2 weeks, 4 weeks, or 6 weeks (Figure 5). In this context, a false alert does not imply the need for a laborious outbreak investigation but rather a more detailed review of the data and use of human judgment to dismiss alerting flags. For the highest false-alert rate, all three algorithms detected the eight respiratory events with a median detection time of 1 day after the start of the event (as determined by the epidemiology team). If the false-alert rate was constrained to once every 6 weeks, only the multiple univariate SPC method maintained its level of performance. For gastrointestinal events, only the Bayesian Belief Network successfully detected all seven events with a median delay of 1 day. Results might vary when the same algorithms are applied to other data streams and other seasons.

The majority of events used in the evaluation were seasonal epidemics attributable to colder weather, limited outdoor activity, and increased communicability during holiday gatherings; few, if any, of the cases comprising these events would result in death or were reportable diseases.

### **Experience**

#### **System Usefulness**

ESSENCE II is used routinely by the Montgomery County (Maryland) Department of Health and Human Services for different purposes, including to accredit county hospitals for the capability to respond to mass casualties resulting from terrorism, to identify foodborne outbreaks, and to provide general knowledge of the county's health status. The department also requests changes to detection thresholds during high-profile events in the region that might affect public health in the county. The county health department continues to find new uses for ESSENCE II outputs; in 2004, it used the system to determine when to initiate and cancel an influenza-vaccination program.

Flexibility and Portability

ESSENCE II acquires data feeds with minimal burden to data providers. The system accepts different data standards for acquisition and data sharing. Adding a new data source is more of a legal chore than a technical one because sources can be added with minimal hours of coordination or software development. ESSENCE is designed to enable persons with minimal programming skill to create new syndrome categories or change syndrome groupings in minutes. The system also allows users to access historic data to perform retrospective studies.

Multiple versions of ESSENCE II exist to accommodate different jurisdictions, data volumes, and data providers for both military preventive medicine and civilian health departments. ESSENCE II is also being provided to state and local health departments. Modifications are needed for local geographic shape files, zip codes, and data providers; these modifications can be performed by state health department IT staff.

#### System Acceptability

Acceptance by the majority of data providers has been exceptional. Currently, the test-bed version of ESSENCE II is used primarily when the level of risk increases. After the NCR network is fully implemented, usage levels are expected to increase. Full implementation is expected in 2004.

#### System Stability

Versions of ESSENCE II have been acquiring data since 1999 and have operated since then with minimal interruption. The system's size and complexity have expanded from the NCR military population and certain Maryland counties to include all of Maryland, Virginia, and the District of Columbia.

#### System Costs

System size and cost are a function of the jurisdiction's size, the number of data providers, and the size of the epidemiology department assigned to surveillance and follow-up. A minimum county-level configuration requires one or two computers, \$15,000 for off-the-shelf software, one part-time epidemiologist, and one part-time IT professional. Cost-effectiveness depends upon the resources of the health department and the vulnerability of its population.

#### Conclusions

ESSENCE II is the first disease-surveillance system to incorporate both military and civilian data to improve the sensitivity and specificity of detecting abnormal disease occurrence. The design requires minimal resources from data providers, thus encouraging their participation. Research into algorithm improvements has been enhanced by operation of a test bed and by rapid upgrades to test improvements in an operational environment. Implementation of the NCR disease-surveillance network should provide operational insights for other jurisdictions considering collaborative surveillance systems.

CDC's framework for evaluating syndromic surveillance systems provides a needed reference for developers and health departments wishing to develop and implement new systems. Evaluation would be enhanced if CDC provided standard data sets to test the processes embedded within the systems and provide a benchmark for comparing system performance ([CDC, 2012](#)).

**Title:** Spotting The Hot Zones: Now We Can Monitor Epidemics Hour By Hour

**Date:** June 23, 2008

**Source:** [Wired](#)

**Abstract:** If you want to stop a disease outbreak — or a bioterrorist attack — you have to act fast. But health information typically moves at the pace of the receptionist at your doctor's office. The goal of Essence, the Department of Defense's Electronic Surveillance System for the Early Notification of Community-based Epidemics, is to pick up the tempo. Begun in 1999 to collect health data in the Washington, DC, area, Essence now monitors much of the Military Health System, which includes 400 facilities around the world.

"You don't have to be accurate to detect things," says Jay Mansfield, director of strategic information systems at the Global Emerging Infections Surveillance and Response System, one of the agencies that developed Essence. "But you do need to be precise."

Reports from every clinic, doctor, and pharmacy get broken into broad syndrome categories rather than specific diseases. One doctor might diagnose bronchitis and another pneumonia, but Essence doesn't care. It's just looking for similar illnesses and where and when they occur. "It's like a fire alarm," Mansfield says. "It goes off if there's smoke, so you can get in the kitchen and see what's going on."

Because 100 megabytes of data come in every day — the team stores 18 months' worth, about 2.5 terabytes — there's often more smoke than fire. A pharmacy running out of antidiarrheals could signal an outbreak of *E. coli* or just a two-for-one sale.

Essence expanded to include new sources (like radiology and laboratory tests) this spring, which means the data issues just got even more complicated. The trick is parsing the data as it comes in so that patterns emerge in hours instead of days. "We detected a gastrointestinal outbreak in Korea," Mansfield says. "I called my boss, and he asked me, 'When did it happen?'" Korea is 13 hours ahead of Washington. So Mansfield simply answered: "Tomorrow" ([Wired, 2008](#)).

**Title:** Assessment Of ESSENCE Performance For Influenza-Like Illness Surveillance After An Influenza Outbreak --- U.S. Air Force Academy, Colorado, 2009

**Date:** April 8, 2011

**Source:** [CDC](#)

**Abstract:** The Electronic Surveillance System for the Early Notification of Community-Based Epidemics (ESSENCE), version II, designed by the Johns Hopkins University Applied Physics Laboratory and the U.S. Department of Defense (DoD), is an Internet-based syndromic disease surveillance system used by civilian and military health departments ([1](#)). ESSENCE was designed to increase the timeliness of outbreak detection, serving as an early warning system and providing opportunities to prevent and control the spread of infection. After a 2009 pandemic influenza A (H1N1) outbreak at the U.S. Air Force (USAF) Academy in Colorado, CDC was invited to conduct an evaluation of the ESSENCE influenza-like illness (ILI) surveillance system to assess its performance during the outbreak ([2,3](#)). Medical records at the USAF Academy clinics from June 25 through July 8, 2009, the period of the outbreak, were reviewed. This report summarizes the results of the evaluation, which demonstrated strengths in data quality, flexibility, and representativeness; however, ESSENCE was not useful for detecting or monitoring the H1N1 outbreak because of its lack of timeliness (1--3 day delay), inadequate sensitivity (71.4%), and poor predictive value positive (PVP) (31.8%) for identifying ILI cases. In this localized, single-source outbreak, ESSENCE did not serve as an early warning system for an emerging infectious disease and did not detect the outbreak soon enough to institute prevention and control measures that might have slowed the spread of infection. More frequent Internet data transmissions from the clinics to the ESSENCE server could improve timeliness, and PVP could be enhanced by including measured body temperature in the ESSENCE ILI case definition.

The utility of syndromic disease surveillance for early outbreak detection and improvement of public health response remains controversial ([4-7](#)). A survey of U.S. health departments indicated that the most common application for syndromic surveillance was to monitor the start and stop of the annual influenza season, but that it was less useful for local outbreak detection ([4](#)). Other studies found that syndromic surveillance has been useful to identify localized respiratory, dermatologic, and gastrointestinal disease outbreaks ([5-7](#)).

During June 25--July 24, 2009, an H1N1 outbreak occurred at the USAF Academy in Colorado, with 134 cases confirmed among a population of USAF 1,376 basic cadet trainees ([3](#)). Although ESSENCE is used at the USAF Academy, public health officials became aware of the outbreak before ESSENCE indicated the increase in ILI cases. After this large outbreak, the USAF Academy invited CDC to evaluate ESSENCE as an ILI surveillance system.

The U.S. military has used ESSENCE since 2003 to detect and monitor disease outbreaks. DoD provides an annual budget for system maintenance and development and releases updated versions of the system as surveillance needs change. ESSENCE identifies patients based on provider-assigned International Classification of Diseases, Ninth Revision, Clinical Modification (ICD-9-CM)

codes that are entered into the electronic medical record (1). The ESSENCE ICD-9-CM code set for ILI\* was established based on an analysis of medical records and respiratory specimens to determine the codes that most accurately represent ILI (8,9). By regular secure data transmissions via the Internet, the ESSENCE server identifies new cases and, using temporal algorithms that predict expected daily fluctuation, determines whether an increasing trend has occurred, indicating a possible outbreak (1,8,9). Raw data and aggregate reports, in the form of line graphs, are available via a password-protected ESSENCE website. An increase in syndromic cases above predicted thresholds is highlighted as a color-coded alert. Privacy and confidentiality are maintained with patient identification numbers and annual information protection training for users. In 2003, using past military and civilian data, an initial evaluation determined that ESSENCE detected eight of eight respiratory disease outbreaks within an average of 1 day after the event.

CDC's Updated Guidelines for Evaluating Public Health Surveillance Systems was used to assess the usefulness, simplicity, flexibility, data quality, acceptability, representativeness, timeliness, stability, sensitivity, and PVP of ESSENCE for the USAF. To determine sensitivity and PVP, medical record data from ILI case-patient visits at the USAF Academy acute care and cadet clinics during June 25--July 8, 2009, were collected. For the medical record review, ILI was defined as measured temperature  $\geq 100.0^{\circ}\text{F}$  ( $\geq 37.8^{\circ}\text{C}$ ) and cough or sore throat. Medical record data collection included cough, sore throat, measured temperature, and the results of respiratory disease laboratory tests for influenza A, influenza B, H1N1, adenovirus, and group A streptococcus bacteria. Patients from the same period were identified on the ESSENCE ILI website to collect the ICD-9-CM codes. Sensitivity and PVP were calculated using 1) medical record--confirmed ILI, as defined and 2) laboratory confirmation of a respiratory infection, as criterion standards. USAF Academy, USAF School of Aerospace Medicine (USAFSAM), DoD, and CDC staff members who used ESSENCE daily were interviewed to assess the remaining evaluation criteria.

This evaluation found that the usefulness of ESSENCE varied by user. CDC, which used the aggregate USAF and DoD data, found ESSENCE useful to monitor national syndromic disease activity, and USAFSAM staff members found it useful to monitor disease activity at each base. The USAF Academy indicated ESSENCE was useful to monitor the local influenza season and determine syndromic baselines. Although users investigated ESSENCE alerts and worrying trends, most alerts and trends were time-consuming false alarms that revealed normal disease variations.

Regarding simplicity of operations and structure, the ESSENCE website's aggregate reports, line graphs, and color-coded alerts were easy to comprehend. ESSENCE's flexibility to adapt was demonstrated by the updated versions released by DoD based on user feedback and changes in surveillance needs, and the raw data query functions available to ESSENCE users. Data quality, or the completeness and validity of the data, was established by extracting demographic and medical information from official DoD systems, and scheduling automated batched data transmissions to the ESSENCE server at night, during periods of lower Internet usage to reduce transmission interruptions. For acceptability, or the willingness to participate in the surveillance system, data transmission to the ESSENCE server was automated, and personnel at the Academy and USAFSAM had passwords, although cumbersome to attain and maintain, to use ESSENCE in their daily operations. ESSENCE was determined to have a high degree of representativeness, in that it included all DoD beneficiaries visiting all USAF outpatient clinics, and thus it reported all medical events. Timeliness, or the time of the clinic visit to the time the information appeared on the ESSENCE website, was 1--3 days (10). Stability, or the reliability and availability of the system, was maintained by the annual DOD budget and the infrequent occasions when ESSENCE was unavailable to the user.

Of the 540 medical records reviewed to assess sensitivity and PVP, 189 had a laboratory test result. Compared with medical record--confirmed ILI, ESSENCE ILI sensitivity was calculated at 71.4% and PVP at 31.8%. Compared with laboratory-confirmed respiratory infections, ESSENCE ILI sensitivity and PVP were 78.6% and 49.5%, respectively. When the evaluators added a documented, measured body temperature of  $\geq 100.0^{\circ}\text{F}$  ( $\geq 37.8^{\circ}\text{C}$ ) to the ESSENCE ILI case definition, the ESSENCE ILI sensitivity, compared with medical records, remained the same, but PVP increased to 95.5%; however, when compared with laboratory confirmation, ILI sensitivity was 65.7%, and PVP was 66.7%.

Reported by C Witkop, MD, USAF Academy, Colorado. M Duffy, DVM, USAF School of Aerospace

Medicine, Wright-Patterson Air Force Base, Ohio. L Cohen, MD, Scientific Education and Professional Development Program Office, Office of Surveillance, Epidemiology, and Laboratory Svcs; D Fishbein, MD, Div of Global Migration and Quarantine, National Center for Emerging and Zoonotic Infectious Diseases; M Selent,\* DVM, EIS Officer, CDC. \*Corresponding contributor: Monica Selent, Div of Global Migration and Quarantine, National Center for Emerging and Zoonotic Infectious Disease, CDC, 404-520-2332, [mselect@cdc.gov](mailto:mselect@cdc.gov).

### **Editorial Note**

This evaluation found that the major strength of ESSENCE ILI surveillance was its usefulness for monitoring annual seasonal influenza activity. Other strengths included simplicity, flexibility, data quality, representativeness, and stability. Weaknesses included low PVP, lack of timeliness, and limited usefulness to detect and monitor an ILI outbreak.

Retrospectively, ESSENCE showed an increasing ILI trend 2--4 days before an Academy mass gathering; however, the combination of the ESSENCE time delay, occurrence of the gathering over a holiday weekend, and short incubation period of H1N1 meant the increasing trend was not detected in time to institute preventive measures. To improve timeliness, medical data transmission could be scheduled in smaller, more frequent batches throughout the day so that changing trends would appear on the ESSENCE website sooner.

After USAFSAM judged that the ILI PVP of the surveillance system was too low to distinguish actual outbreaks, the addition of a measured body temperature  $\geq 100.0^{\circ}\text{F}$  ( $\geq 37.8^{\circ}\text{C}$ ) to the ESSENCE case definition was evaluated to determine whether PVP, and potentially sensitivity, could be improved. Compared with medical record--confirmed ILI and laboratory-confirmed respiratory infections as criterion standards, PVP did increase with the addition. An independent study using only laboratory confirmation and ICD-9-CM--based ILI surveillance also found that PVP increased by adding measured body temperature (10). The large PVP increase with medical record confirmation was attributed to the low number of ESSENCE ILI cases with an elevated temperature at the clinic, potentially resulting from antipyretic use or actual afebrile infection. When compared with laboratory-confirmed respiratory infections, sensitivity decreased. However, with medical record confirmation, sensitivity stayed the same, because all the ILI cases still had an elevated temperature, per the medical record case definition, and an ILI ICD-9-CM code, per the ESSENCE case definition. Despite the improvement in PVP by adding a measured body temperature to the ESSENCE case definition, the potential loss in sensitivity might reduce the ability to detect actual ILI outbreaks. Users need to determine if this loss is acceptable for their purposes.

The findings in this report are subject to at least three limitations. First, as new data arrive in ESSENCE, the web page does not record the date additional case-patients appeared. Therefore, evaluators could only estimate when ESSENCE issued an alert to the ILI outbreak, based on historical documentation. Second, this evaluation collected data from only one outbreak at one USAF base. Additional outbreak analyses from other USAF bases are needed to judge the effectiveness of ESSENCE as an early-warning outbreak system for the USAF. Finally, the results of this evaluation are not generalizable to the other military services or civilian public health agencies, which might use ESSENCE differently.

This evaluation showed that, despite strengths in data quality, flexibility, and representativeness, ESSENCE did not serve as an early warning system for an emerging infectious disease during a localized, single-source outbreak, and did not detect the outbreak soon enough to allow prevention and control measures to be instituted. For enhanced outbreak detection and monitoring, more frequent Internet data transmissions would improve ESSENCE's timeliness. Additionally, the inclusion of measured body temperature in the ESSENCE ILI case definition could improve PVP, but with a possible loss in sensitivity resulting from exclusion of afebrile cases. As the strengths, weaknesses, and limitations of ILI surveillance as an early warning system for emerging infectious disease become better understood, future development should investigate how informatics and information technology can overcome ILI surveillance weaknesses.

### **Acknowledgments**

This report is based, in part, on contributions by K Cox, MD, US Army Center for Health Promotion and Preventive Medicine; J Collins, R Devine, A Cox, A Owens, M Green, US Air Force Academy; and C Hales, PhD, N Molinari, PhD, N Megateli-Das, MS, P Szymanowski, MPH, C Adams, and J Herrera, CDC ([CDC, 2011](#)).

### 3. GEIS (Global Emerging Infections Surveillance)

**Title:** Global Emerging Infections Surveillance (GEIS) Operations

**Date:** 2012

**Source:** [AFHSC](#)

**Abstract:** The Global Emerging Infections Surveillance and Response System (GEIS) Operations Division at AFHSC aims to be a scientifically credible and recognized worldwide surveillance system for emerging infections. Through developing, implementing, supporting and evaluating an integrated global emerging infections surveillance and response system, GEIS contributes to protection of all DoD health care beneficiaries and the global public health community.

GEIS has developed several strategic goals to bolster DoD and global public health efforts. These goals include surveillance and detection, response and readiness, integration and innovation, cooperation and [capacity building](#) with partner host countries, and the integration of the World Health Organization's International Health Regulations (2005) core capacities into all surveillance activities.

**Each strategic goal encompasses five emerging disease priorities:**

1. [Respiratory infections \(RI\)](#), especially influenza;
2. [Gastrointestinal infections \(GI\)](#);
3. [Febrile vector-borne infections \(FVBI\)](#) with an emphasis on [malaria](#);
4. [Antimicrobial resistant organisms \(AR\)](#); and
5. [Sexually transmitted infections \(STI\)](#).

Surveillance activities are conducted through a network of Continental US (CONUS) and Outside the Continental US (OCONUS) partners ([AFHSC, 2012](#)).

### 4. HAN (Health Alert Network)

**Title:** Health Alert Network

**Date:** 2012

**Source:** [Wikipedia](#)

**Abstract:** The Health Alert Network (HAN) is a program under the [Centers for Disease Control and Prevention](#) which is an agency of the [United States Department of Health and Human Services](#). The HAN project is intended to "ensure that each community has rapid and timely access to emergent health information; a cadre of highly-trained professional personnel; and evidence-based practices and procedures for effective public health preparedness, response, and service on a 24/7 basis." Currently, HAN is a strong national program, providing vital health information and the infrastructure to support the dissemination of that information at the state and local levels, and beyond. A vast majority of the State-based HAN programs have over 90% of their population covered under the umbrella of HAN. The HAN Messaging System currently directly and indirectly transmits Health Alerts, Advisories, and Updates to over one million recipients. The current system is being phased into the overall PHIN messaging component ([Wikipedia, 2012](#)).

**Title:** Health Alert Network (HAN)

**Date:** 2012

**Source:** [CDC](#) (Center for Disease Control)

**Abstract:** Providing Health Alerts, Health Advisories, Updates, and Info Service Messages to State and Local Health Officers, Public Information Officers, Epidemiologists and HAN Coordinators as well as Clinician organizations.

### What is HAN?

The Health Alert Network (HAN) is a strong national program, providing vital health information and the infrastructure to support the dissemination of that information at the State and Local levels, and beyond. A vast majority of the State-based HAN programs have over 90% of their population covered under the umbrella of HAN.

### HAN ensures that each community has:

1. Rapid and timely access to emergent health information.
2. A group of highly-trained professional personnel.
3. Evidence-based practices and procedures for effective public health preparedness, response, and service on a 24/7 basis.

The HAN Messaging System currently directly and indirectly transmits Health Alerts, Advisories, Updates, and Info Service Messages to over one million recipients.

### HAN Message Types

1. **Health Alert:** Conveys the highest level of importance; warrants immediate action or attention.
2. **Health Advisory:** Provides important information for a specific incident or situation; may not require immediate action.
3. **Health Update:** Provides updated information regarding an incident or situation; unlikely to require immediate action.
4. **Info Service:** Provides general information that is not necessarily considered to be of an emergent nature. ([CDC, 2012](#)).

**Title:** Dimension Data Launches Health Alert Network Solution To Help Combat Bioterrorism

**Date:** August 28, 2007

**Source:** [PR Newswire](#)

**Abstract:** Increased risk for potential major bioterrorist activities has raised an immediate need for comprehensive systems to share information quickly and securely. Dimension Data Holdings, plc (London: DDT), a global technology services company, has developed a Health Alert Network portal solution to allow secure, immediate and collaborative content sharing and alerting functions.

Dimension Data has developed its solution in compliance with the Centers for Disease Control and Prevention's (CDC) mandate for all local and state governments to implement a nationwide, integrated information and communications system that links emergency medical responders with public health officials. The company is currently doing work with one of the major U.S. metropolitan cities to address its health response initiatives. Dimension Data's Health Alert Network portal solution enables early warning information, surrounding unusual disease outbreaks and bioterrorist events, to be distributed quickly and facilitates sharing of diagnostic and treatment information.

Doctors and hospital workers can have immediate access and distribution rights to documents such as disease fact sheets, protocols, and clinical guidelines. The portal is designed to educate, support, and mobilize communities of interest on distinct health threats via a proven platform and intuitive interface that provides a high level of security. Dimension Data's portal solution was developed in conjunction with HP, Intel and Microsoft and was designed using the company's expertise in the healthcare industry. Depending on a state or local health department's budget, resources, and existing IT infrastructure, Dimension Data's Health Alert Network can be either fully customized, custom packaged, or subscription-based. In addition to the distribution of health alerts and prevention

guidelines, the system brings departments of health and the CDC a coordinated communications channel to conduct initiatives such as national disease surveillance and electronic laboratory reporting.

**Main features of the Dimension Data's Health Alert Network include:**

1. High-speed, secure Internet connection to provide instantaneous access to disease reports, CDC information, and response plans
2. Early warning systems, including multi-channel alerting capabilities with sophisticated call-down abilities, to alert authorities and media of potential emergency situations
3. Coordinated public health response
4. Secure and scalable channel for local, state, and federal health authorities to coordinate with each other and law enforcement \* Distance-learning capacity to educate health care professionals
5. Central library of current, accessible, and searchable clinical material for researching treatments

**Some examples where the Health Alert Network portal solution could be of use include:**

1. A health department administrator posts an alert to the system. The system recognizes the alert and sends a message to the alert broadcast system. This system sends the message to local hospitals and CDC through pagers, cell phones, and e-mail.
2. Hospital "A" uploads a document and Hospital "B" downloads the same document, healthcare professionals at both locations can log into a chat room to discuss it.
3. The department of health has an infectious disease specialist giving a seminar so hospitals can log into the conferencing system to view the seminar online.

Dimension Data is uniquely equipped to provide state and local governments with the multi-faceted communication system. The company's Health Alert Network solution includes a network assessment, building and deployment of the portal application, infrastructure integration, as well as training, hosting and maintenance. Departments of Health can rely on Dimension Data as a single source throughout the lifecycle of the engagement thereby avoiding the need to manage multiple vendors. "For local and state governments, implementing an integrated communications system can be a daunting challenge," said Andrew Cohen, director of homeland security initiatives for Dimension Data North America. "The Health Alert Network provides governments with an easy-to-implement, cost effective system that meets the CDC's requirements and, at the same time, delivers far-reaching benefits for citizens" ([PR Newswire, 200?](#)).

## 5. LRN (Laboratory Response Network)

**Title:** Laboratory Response Network

**Date:** 2012

**Source:** [Wikipedia](#)

**Abstract:** The Laboratory Response Network (LRN) is a collaborative effort within the US federal government involving the [Association of Public Health Laboratories](#) and the [Centers for Disease Control and Prevention](#) (CDC). Most state public health laboratories participate as reference laboratories (formerly level B/C) of the LRN. These facilities support hundreds of sentinel (formerly level A) laboratories in local hospitals throughout the United States and can provide sophisticated confirmatory diagnosis and typing of [biological agents](#) that may be used in a [bioterrorist](#) attack or other bio-agent incident. The LRN was established in 1999.

### Levels

The LRN consists of a loose network of government labs at three levels.

### Sentinel Laboratories

These laboratories, found in many hospitals and local public health facilities, have the ability to rule out specific bioterrorism threat agents, to handle specimens safely, and to forward specimens to higher-level labs within the network.

### Reference Laboratories

These laboratories (more than 100), typically found at [state health departments](#) and at military, veterinary, agricultural, and water-testing facilities, can rule on the presence of the various biological threat agents. They can use [BSL-3](#) practices and can often conduct [nucleic acid amplification](#) and [molecular typing studies](#).

### **National Laboratories**

These laboratories, including those at CDC and [U.S. Army Medical Research Institute of Infectious Diseases](#) (USAMRIID), can use [BSL-4](#) practices and serve as the final authority in the evaluation of potential bioterrorism specimens. They provide specialized reagents to lower level laboratories and have the ability to bank specimens, perform serotyping, and detect [genetic recombinants](#) and [chimeras](#) ([Wikipedia, 2012](#)).

**Title:** [Detecting Biothreat Agents: The Laboratory Response Network](#)

**Date:** 2003

**Source:** [ASM News](#) (PDF)

**Abstract:** In response to the threat of bioterrorism and following a presidential order, officials at the Centers for Disease Control and Prevention (CDC), Association of Public Health Laboratories (APHL), Federal Bureau of Investigation (FBI), and United States Army Medical Research Institute of Infectious Diseases (USAMRIID) established the Laboratory Response Network (LRN) in 1999. This national system is designed to link state and local public health laboratories with other advanced-capacity clinical, military, veterinary, agricultural, water, and food-testing laboratories, including those at the federal level.

The LRN is a critical component of CDC's public health mission, enhancing U.S. readiness to detect and respond to bioterrorism incidents. In addition to biothreat agents, the LRN is expanding to include the ability to detect chemical agents. Funding for LRN to build infrastructure, obtain state-of-the-art equipment, and train personnel is helping to rebuild the country's public health laboratory capacity, improving our ability to respond not only to bioterrorism incidents but also to other infectious diseases outbreaks.

Part of these efforts include developing a welltrained laboratory workforce, including members who are certified by the American Board of Medical Microbiology (ABMM) or its equivalent, raising the capacity of LRN to respond quickly and appropriately to public health emergencies.

After officials in the Department of Health and Human Services told CDC to prepare the public health system for dealing with the bioterrorism threat, CDC developed a series of cooperative agreements with every state and several large municipalities that focus on preparedness.

These agreements initially emphasized five critical areas: (i) preparedness planning and readiness assessment; (ii) surveillance and epidemiology capacity, (iii) biologic laboratory and chemical laboratory capacity, (iv) health alert network, and (v) information technology. Since the Bacillus anthracis bioterrorism incident of late 2001, CDC has added several critical areas, including communicating health risks, disseminating health information, education, and training.

Bioterrorism may be either covert or overt. Because a covert release of a biological agent would likely not be noticed immediately, the first signs could come days or weeks later when individuals seek medical care. Thus, the first responders will likely be astute clinicians, laboratorians, or public health workers who recognize the index case or identify the infectious agent. In the case of an announced release, traditional first responders will likely respond to actual biological agents or hoaxes. In all these cases, the incident could occur anywhere, necessitating a comprehensive public health plan for responding to bioterrorism or any infectious disease outbreak. This response will involve epidemiologic investigation, medical treatment and prophylaxis for affected persons, and other disease prevention activities. The success of these activities also depends on rapidly and accurately identifying threat agents ([ASM News, 2003](#)).

## 6. RODS (Real-Time Outbreak Disease Surveillance)

**Title:** RODS (Real-Time Outbreak Disease Surveillance)

**Date:** Present

**Source:** [Wikipedia](#)

**Abstract:** Real-time outbreak and disease surveillance system (RODS) is a [biosurveillance](#) system developed by the [University of Pittsburgh](#), Department of Biomedical [Informatics](#). It is "prototype developed at the University of Pittsburgh where real-time clinical data from emergency departments within a geographic region can be integrated to provide an instantaneous picture of symptom patterns and early detection of [epidemic](#) events."

**RODS uses a combination of various monitoring tools:**

1. The first tool is a [moving average](#) with a 120-day sliding phase-I-window.
2. The second tool is a nonstandard combination of [CUSUM](#) and [EWMA](#), where an EWMA is used to predict next-day counts, and a CuSum monitors the residuals from these predictions.
3. The third monitoring tool in RODS is a [recursive least squares](#) (RLS) algorithm, which fits an [autoregressive model](#) to the counts and updates estimates continuously by minimizing [prediction error](#). A Shewhart I-chart[[clarification needed](#)] is then applied to the residuals, using a threshold of 4 [standard deviations](#).
4. The fourth tool in RODS implements a [wavelet](#) approach, which decomposes the time series using [Haar wavelets](#), and uses the lowest resolution to remove long-term trends from the raw series. The residuals are then monitored using an ordinary Shewhart I-chart with a threshold of 4 standard deviations ([Wikipedia, 2012](#)).

**Title:** History of the RODS Laboratory

**Date:** September 1999 - Present

**Source:** [University of Pittsburgh](#)

**Abstract:** In September 1999, researchers at the University of Pittsburgh created the Real-time Outbreak and Disease Surveillance (RODS) system. RODS, being based on earlier work by the same researchers in building a clinical event monitor (CLEM) and a clinical communication system, became operational almost immediately and has continued to grow in size, function, and use.

RODS is currently in use in multiple cities, states and countries. The RODS System represented the first real-time public health surveillance system. It contributed basic results about disease outbreak detection from coded chief complaints, from free text, and electronic laboratory reporting in real time. It also demonstrated methods for the rapid investigation of an outbreak using a link to an electronic medical record.

Initial funding for this research came from a grant from the National Library of Medicine (NLM 5 R29 LM06233) "Belief-Network Based Reminder Systems that Learn." The principal developers of the system are Drs. Rich Tsui, Jeremy Espino, and Michael Wagner. [Currently, several years after RODS coined the term, "real-time" has found its way into the active vocabulary of those not only describing the RODS system itself but also describing any information that can be immediately available and is geared towards identifying disease outbreaks.]

**RODS Milestones**

1. September 1999 - Formation of the RODS Laboratory by Drs. Jeremy Espino, Fu-Chiang Tsui and Michael Wagner. Prototype of RODS Surveillance System begins to monitor emergency departments of University of Pittsburgh Medical Center.
2. October 2001 - Established 13 county surveillance of emergency departments for Western Pennsylvania. Deployment of the Health System Resident Component

3. November 2001 - Dr. Michael Wagner delivers a report on biosurveillance before the US Congress
4. January 2002 - Deployment of Utah RODS for 2002 Winter Olympics
5. February 2002 - President George W. Bush visits the RODS lab and calls RODS the "modern DEW line" 6
6. December 2002 - RODS Software is made publically available as free software
7. November 2002 - The National Retail Data Monitor is created
8. February 2002 - The Biomedical Security Institute is formed
9. August 2003 - The RODS Software is made open source
10. May 2006 - The Handbook of Biosurveillance is published
11. September 2009 - The University of Pittsburgh becomes a CDC Center of Excellence in Public Health Informatics

As a result of this project's success, Drs. Wagner and Tsui founded the RODS Laboratory with a mission to explore the use of information technology for the detection of disease outbreaks—both naturally occurring and bioterroristic. In 2000, additional funding for the research came from the Agency for Health Care Research and Quality (AHRQ/Mellon Pitt Corporation 290-00-0009) "Using Information Technology to Improve Clinical Preparedness for Bioterrorism." Two commissioned reports to the AHRQ formed the basis for the future direction of RODS research: The Nation's Current Capacity for the Early Detection of Public Health Threats including Bioterrorism (78 pages), delivered June 8 (revised September 26), 2001; and Availability and Comparative Value of Data Elements Required for an Effective Bioterrorism Detection System (184 pages), delivered November 28, 2001.

In October 2001, RODS began to demonstrate the feasibility of real-time data collection under a trusted broker arrangement in a 13-county region in Western Pennsylvania. This work demonstrated the use of Trusted Data Broker for public health surveillance, established a minimal de-identified data set that is widely available, and resulted in the creation of model memoranda of understanding and an application service provider (ASP) model.

Also beginning in October 2001, a Health-System-Resident component was created with extended funding from the CDC. The goal of this project was to explore in detail the interaction between health care and public health in the area of infectious disease control utilizing a special purpose component residing within a health system.

After the Anthrax attacks of October 2001, the work of the laboratory took on additional urgency and significance. On November 1, 2001, Dr. Wagner testified at the Hearing of the Oversight and Investigations Subcommittee of the House Committee on Energy and Commerce: ["A Review of Federal Bioterrorism Preparedness Programs: Building an Early Warning Public Health Surveillance System"](#) in Washington, D.C.

### **2002 Winter Olympics and Deployment of Utah RODS**

In January 2002, working in collaboration with Per Gesteland, M.D., Bob Rolfs, M.D., MPH, Reed Gardner, Ph.D., Peter Haug, M.D., and Brent James, M.D., MPH at the University of Utah, Intermountain Healthcare, and the Utah Department of Health, the laboratory helped deploy RODS in Utah for surveillance coverage of the 2002 Winter Olympic Games (see published papers from 2002 and 2003). Its successful deployment resulted in a permanent RODS system, currently collecting de-identified data for more than 80% of the healthcare visits in the state of Utah.

### **Recognition by Present George W. Bush**

On February 5, 2002 President George W. Bush, Homeland Security Director Tom Ridge, and Health and Human Services Secretary Tommy Thompson visited Pittsburgh for a demonstration of the RODS system. Following the demonstration, [The President called the system the "modern DEW line," referring to the Distant Early Warning radar system employed during the Cold War to guard against an attack from the Soviet Union.](#)

For Cover Story on the visit of President Bush, Homeland Security Director Tom Ridge, and Health and Human Services Secretary Tommy Thompson, see the [University of Pittsburgh "PITT" magazine \(June 2002 issue\)](#).

Additional and subsequent funding for RODS research came from the Defense Advanced Research Projects Agency beginning August 2001 (Air Force Research Laboratory Cooperative Agreement with Mellon Pitt Corporation, F30602-01-2-0550) "Scalable Bio-Surveillance Systems," and a \$6M grant from the Pennsylvania Department of Health beginning July 2002 (Center for Biomedical Informatics/Pennsylvania Department of Health, ME-01-737) "Building an Early Warning Public Health Surveillance System," the goal of which was to build an early warning public health surveillance system throughout the Commonwealth of Pennsylvania.

Graduate student personnel in the RODS Laboratory were, and continue to be, supported by research grants and a training grant from the National Library of Medicine (NLM 5 T15 LM/DE07059) "The Pittsburgh Biomedical Informatics Training Program" awarded to the Center for Biomedical Informatics (Principal Investigator: Gregory F. Cooper, PhD).

### **RODS Made Publically Available**

On December 2, 2002, U.S. Senators Arlen Specter (R-PA) and Rick Santorum (R-PA) visited Pittsburgh for an update on the growth and development of the RODS system and to announce that the University of Pittsburgh and Carnegie Mellon University were taking the unprecedented step of making the RODS software available without cost to other academic institutions and health departments capable of sharing this national responsibility. Senator Specter, the ranking member of the U.S. Senate's Veterans Affairs Committee and a member of the Defense Appropriations Subcommittee has provided important support for the RODS Laboratory.

### **The National Retail Data Monitor**

In November 2002, researchers at the RODS Laboratory unveiled the National Retail Data Monitor (NRDM; also see published article), which receives information about the quantity of over-the-counter (OTC) healthcare products, such as cough syrups, sold each day in different regions. What stores are selling is of great interest to the field of early-warning surveillance because when people are sick, they buy OTC products before they seek medical treatment.

### **The Biomedical Security Institute**

In February 2002, Dr. Wagner became the Co-Director of the Biomedical Security Institute (BMSI) at the University of Pittsburgh, together with Andrew W. Moore, Ph.D., A. Nico Haberman Associate Professor of Robotics and Computer, Science Carnegie Mellon University. Dr. Moore is also a member of the RODS Laboratory. (In 2005, Dr. Moore was tapped by Google Inc. to head the company's new engineering office in Pittsburgh.) BMSI was a research and development collaboration between the University of Pittsburgh and Carnegie Mellon University dedicated to the prevention of, preparation for, and response to acts of terrorism and natural events involving biological agents. BMSI received its initial funding in September 2000 from the Centers for Disease Control and Prevention (CDC) through a grant (U90/CCU318753) "Carnegie Mellon University Focus Area Immunization and Infectious Disease." The award was distributed between researchers involved in bioterrorism research at Carnegie Mellon University and the University of Pittsburgh. The RODS Laboratory received a substantial portion of the award, which helped hasten the growth of the RODS system. In January 2003, the expansion of the RODS system and the broadening mission of the RODS Laboratory led Drs. Wagner and Moore to stepdown as Co-Directors of the BMSI in order to focus exclusively on the RODS project.

### **The RODS Open Source Project**

In August 2003, the University of Pittsburgh open-sourced the RODS software under the GNU General Public License (GPL) and later the Affero GPL. The objectives of the RODS Open Source Project are to (1) accelerate the development of software for disease outbreak surveillance in terms of both quality and functionality, and (2) stimulate and support the formation of a community of disease outbreak surveillance developers. As a result of the open source licensing model of RODS, its use has grown throughout the world and code from the RODS system has been used in other biosurveillance systems.

### **The Department of Homeland Security and BioWatch**

In the summer of 2004, the Department of Homeland Security (DHS) initiated BioWatch—a Homeland Security program that guards 30 U.S. cities against possible biological attack. The RODS Laboratory was selected as one of two facilities to perform work under the BioWatch program. With funding from

DHS, the laboratory is installed the RODS system for the purpose of real-time data collection in civilian hospitals and outpatient facilities in several large BioWatch cities, extending the National Retail Data Monitor to support the project, conducting decision analyses of the decision problems faced by users of the BioWatch system, deploying and extending existing advanced detection algorithms developed by our group (including spatial scanning, Bayesian modeling, and inverse aerosol dispersion modeling that will combine BioWatch data, clinical, spatial, weather, and retail data to form overall probabilistic assessments of threat) and combining the probabilistic output of the detection algorithms and the results of decision analyses to create an implemented response decision-making system in conjunction with the response decision makers in each BioWatch city.

### **The Handbook of Biosurveillance**

In May 2006, the RODS Laboratory and its collaborators write and publish "The Handbook of Biosurveillance," the first book to comprehensively cover the field of Biosurveillance.

### **CDC Center of Excellence in Public Health Informatics**

In September of 2009, the RODS Laboratory along with the University of Pittsburgh's Graduate School of Public Health and Carnegie Mellon's Center for Human Computer Interaction was recognized as a CDC Center of Excellence in Public Health Informatics ([University of Pittsburgh, 2012](#)).

## **7. SS (Syndromic Surveillance)**

**Title:** Syndromic Surveillance

**Date:** Present

**Source:** [Wikipedia](#)

**Abstract:** Syndromic surveillance is the analysis of medical data to detect or anticipate [disease outbreaks](#). According to a [CDC](#) definition, "the term 'syndromic surveillance' applies to surveillance using health-related data that precede diagnosis and signal a sufficient probability of a case or an outbreak to warrant further public health response. Though historically syndromic surveillance has been utilized to target investigation of potential cases, its utility for detecting outbreaks associated with [bioterrorism](#) is increasingly being explored by public health officials.

The first indications of disease outbreak or [bioterrorist](#) attack may not be the definitive diagnosis of a physician or a lab.

Using a normal influenza outbreak as an example, once the outbreak begins to affect the population, some people may call in sick for work/school, others may visit their drug store and purchase medicine over the counter, others will visit their doctor's office and other's may have symptoms severe enough that they call the [emergency telephone number](#) or go to an emergency room.

Syndromic surveillance systems monitor data from school absenteeism logs, emergency call systems, hospitals' over-the-counter drug sale records, Internet searches, and other data sources to detect unusual patterns. When a spike in activity is seen in any of the monitored systems disease epidemiologists and public health professionals are alerted that may be an issue.

An early awareness and response to a bioterrorist attack could save many lives and potentially stop or slow the spread of the outbreak. The most effective syndromic surveillance systems automatically monitor these systems in real-time, do not require individuals to enter separate information (secondary data entry), include advanced analytical tools, aggregate data from multiple systems, across geo-political boundaries and include an automated alerting process.

A syndromic surveillance system based on search queries was first proposed by [Gunther Eysenbach](#), who began work on such a system in 2004. Inspired by these early, encouraging experiences, [Google](#) launched [Google Flu Trends](#) in 2008. More [flu](#)-related searches are taken to indicate higher flu activity. The results closely match [CDC](#) data, and lead it by - 1–2 weeks. The results appeared in [Nature](#). Extending [Google's](#) work researchers from the Intelligent Systems

Laboratory ([University of Bristol](#), UK) created [Flu Detector](#); an online tool which based on [Information Retrieval](#) and [Statistical Analysis](#) methods uses the content of [Twitter](#) to nowcast flu rates in the UK ([Wikipedia, 2012](#)).

**Title:** [Syndromic Surveillance: An Effective Tool for Detecting Bioterrorism?](#)

**Date:** 2004

**Source:** [Rand Corporation](#) (PDF)

**Abstract:** In responding to a bioterrorist attack, time is critical. The sooner public health officials know about a bioterrorist event, the more decisively they can intervene to stem its spread. To aid the early detection of bioterror events, public health officials and researchers have developed a new method called *syndromic surveillance*. This type of surveillance involves collecting and analyzing statistical data on health trends — such as symptoms reported by people seeking care in emergency rooms or other health care settings — or even sales of flu medicines. Because bioterrorist agents such as anthrax, plague, and smallpox initially present “flu-like” symptoms, a sudden increase of individuals with fever, headache, or muscle pain could be evidence of a bioterrorist attack. By focusing on symptoms rather than confirmed diagnoses, syndromic surveillance aims to detect bioterror events earlier than would be possible with traditional disease surveillance systems.

Many city and state public health agencies have begun investing substantial sums to develop and implement these surveillance systems. However, the method is new and still largely untested. To make informed decisions, public health officials need to know more about these systems, including how well they work, their limitations, and how they fit into the broader public health system.

To shed light on these issues, a team of analysts led by RAND Health researcher Michael Stoto examined the strengths and limitations of syndromic surveillance. The analysts also compared various types of syndromic surveillance and drew implications for public health decisionmaking. The findings raised questions about the effectiveness of syndromic surveillance. The study reached two main conclusions: (1) that syndromic surveillance systems face inherent trade-offs among their levels of sensitivity, timeliness, and false positive rates that limit their effectiveness as bioterror-detection tools and (2) that their benefits have not yet been clearly established.

**The study addressed three principal questions:**

1. Under what conditions is syndromic surveillance effective?
2. Do more sophisticated detection methods outperform simple methods?
3. How should syndromic surveillance be integrated into public health practice? ([Rand Corporation, 2004](#)).