



- RAND RESEARCH AREAS
- CHILDREN AND ADOLESCENTS
- CIVIL JUSTICE
- EDUCATION
- ENERGY AND ENVIRONMENT
- HEALTH AND HEALTH CARE
- INTERNATIONAL AFFAIRS
- U.S. NATIONAL SECURITY
- POPULATION AND AGING
- PUBLIC SAFETY
- SCIENCE AND TECHNOLOGY
- SUBSTANCE ABUSE
- TERRORISM AND HOMELAND SECURITY
- TRANSPORTATION AND INFRASTRUCTURE

Syndromic Surveillance

An Effective Tool for Detecting Bioterrorism?

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.

Key findings:

- Syndromic surveillance systems face inherent trade-offs (among sensitivity, timeliness, and the number of false positives) that limit their effectiveness.
- The benefits of any syndromic surveillance system will depend on how effectively it is integrated into the public health system.
- Until the benefits of syndromic surveillance are more clearly established, cities and states should proceed cautiously before investing in costly systems.

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

This product is part of the RAND Corporation research brief series. RAND research briefs present policy-oriented summaries of individual published, peer-reviewed documents or of a body of published work.

Corporate Headquarters
1700 Main Street
P.O. Box 2138
Santa Monica, California
90407-2138
Tel 310.393.0411
Fax 310.393.4818

© RAND 2004

This Highlight summarizes RAND Health research reported in the following publication:

Stoto, Michael A., Matthias Schonlau, and Louis T. Mariano, “Syndromic Surveillance: Is It Worth the Effort?” *Chance*, Vol. 17, No. 1, 2004, pp. 19–24.

tools and (2) that their benefits have not yet been clearly established.

The study addressed three principal questions:

- Under what conditions is syndromic surveillance effective?
- Do more sophisticated detection methods outperform simple methods?
- How should syndromic surveillance be integrated into public health practice?

Under What Conditions Is Syndromic Surveillance Effective?

Potentially, syndromic surveillance systems can detect certain kinds of serious disease outbreak days in advance of conventional surveillance systems. However, the size and timing of an outbreak for which syndromic surveillance gives an early advantage may be limited. In a case involving hundreds or thousands of simultaneous infections, no special detection methods would be needed. Conversely, in a case involving only a few individuals, such as the anthrax episode of 2001, even the best syndromic surveillance system might not work.

In addition, surveillance systems are susceptible to false positives—detecting an event that isn't there. These false alarms are a concern because they cost money—resources are required to respond to phantom events—and may desensitize responders to real events. Given that thousands of jurisdictions across the United States might be running syndromic surveillance simultaneously, decisions must be made about what constitutes an acceptable rate of false positives. Collecting more or better data or analyzing the data longer can reduce false positives, but this would mean either sacrificing some timeliness or reducing the system's sensitivity to attacks.

To examine the effectiveness of syndromic surveillance, the RAND researchers simulated a bioterrorist attack. Using the daily number of admissions of patients with flu-like symptoms to the emergency department of a typical urban hospital, they added a hypothetical number of extra cases spread over a number of days to mimic the pattern of a potential bioterror attack. The simulation study suggests the minimum size and speed of outbreaks that are detectable. The results are sobering: Even with an excess of 9 cases over two days (see Figure 1, explained in more detail below), which is three times the daily average, there was only a 50 percent chance that the alarm would go off. When 18 cases were spread over nine days (see Figure 2), chances were still no better than 50-50 that the alarm would sound by the ninth day. Moreover, this finding only holds true outside of the winter flu season.

Which Methods of Syndromic Surveillance Are Most Effective?

The researchers also compared four specific detection algorithms. The first used hospital admissions data from a single day; the second used a moving daily average that gave greater weight to more recent data; the third used cumulative deviations from a constant expected value; and the fourth used cumulative deviations from an expected value that is adjusted for seasonal variation in flu symptoms.

The analysis found that all of the algorithms were equally effective in detecting a fast-spreading agent (one in which all simulated new cases were spread over three days—see Figure 1). However, the more sophisticated statistical methods had a higher probability of detecting a slow-moving attack (in which simulated new cases were spread over nine days—see Figure 2). Conceivably, this performance could be improved by monitoring a less common syndrome, pooling data across multiple hospitals, analyzing more indicators or hospitals, or studying geographic patterns. However, additional data or more comprehensive analysis would confront new trade-offs among the sensitivity and timeliness of detection and the false positive rate.

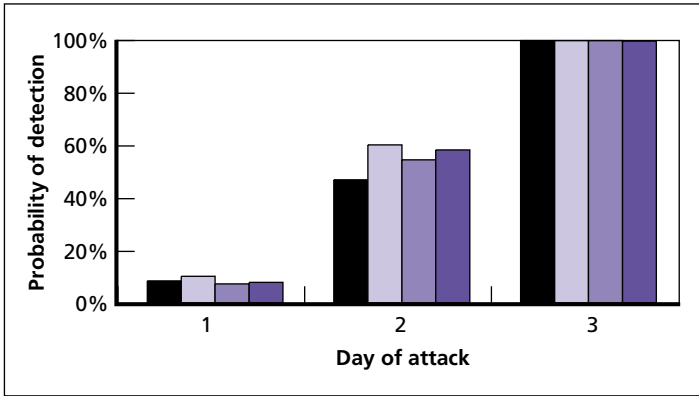
Integrating Syndromic Surveillance into the Public Health System

No matter how well a syndromic surveillance system performs, its benefits ultimately depend on how effectively it is integrated into the broader public health system. Syndromic surveillance only sets off alarms. A process for investigating such alarms and responding effectively must be in place beforehand. Physicians, in particular, are essential for active surveillance of symptoms (in which physicians can report symptoms directly to public health officials), epidemiologic investigations, or large-scale responses such as inoculation or other prophylactic efforts. One way of integrating surveillance more effectively into the public health system could be to increase physician involvement, which some syndromic surveillance systems tend to minimize.

Implications for Public Health Policy and Research

Given that syndromic surveillance is still relatively untested, city and state health departments should be cautious about investing in costly new syndromic surveillance systems. In the meantime, researchers need to learn more about what data to monitor and how to analyze them. Metrics for measuring system performance must also be developed and refined. Given that bioterror events are rare, assessing system

Figure 1

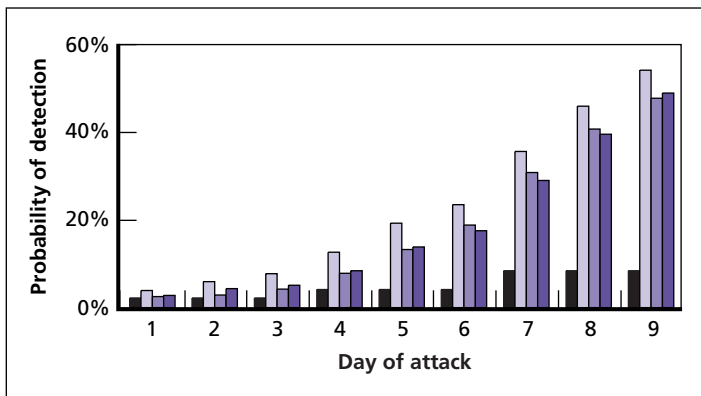


The bars correspond to four detection algorithms: the first using only one day's data, the other three combining data from multiple days. All four syndromic surveillance methods worked equally well for fast-spreading bioterror attacks, but had only about a 50-50 chance of detecting the outbreak by day 2.

performance under real conditions requires considerable creativity. One approach might be to assess how effectively existing systems have detected natural disease outbreaks. Indeed, if these systems prove useful for detecting naturally occurring outbreaks or the beginning of the annual flu season, their public benefit would increase substantially. Their potential beyond bioterrorism may make syndromic surveillance systems worth the investment.

These findings should not be generalized to cast doubt on the value of information technology for strengthening public health. Beyond syndromic surveillance per se, information technology can significantly improve public health practice. Communications systems, for instance, can make it easier for physicians and laboratories to report suspicious cases quickly and efficiently, and database systems can help epidemiologists manage their investigation of an outbreak. ■

Figure 2



Methods that combine data from multiple days (the purple bars) were more effective at detecting slow-spreading attacks, but even the best method took until day 9 to have a 50-50 chance of detecting a slow outbreak.

Abstracts of all RAND Health publications and full text of many research documents can be found on the RAND Health web site at www.rand.org/health. The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors. RAND® is a registered trademark.

RAND Offices Santa Monica • Washington • Pittsburgh • New York • Doha • Leiden • Berlin • Cambridge