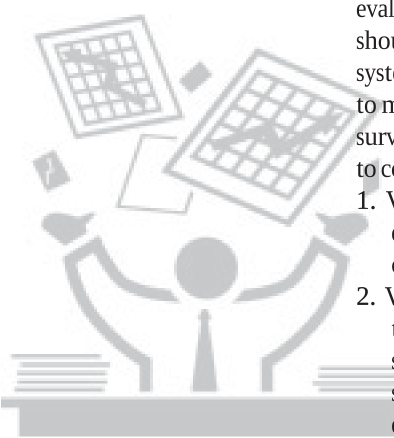
Evaluating the New Electronic Disease Surveillance Systems

Bryant T. Karras
William B. Lober
Gregory T. Smith



Since September 2001, directors of public health departments have been inundated with brochures and advertisements for electronic disease surveillance systems. Each company claims that no health department can be properly alerted to a widespread bioterrorist attack without purchasing its solution to the terrorism crisis. Many of these companies are new to the market or are using the threat of bioterrorism to resell systems designed for clinical health care providers.

Public health's relatively new-found prominence, and the money accompanying that prominence, has made it the latest hot prospect for many vendors. Unfortunately, due to the newness of the field, there is little common agreement about the utility of these systems, what they should cost, and what data they should track.

Until new standards are developed, however, evaluation of the new epidemiologic systems should meet the criteria of traditional surveillance systems. For public health professionals who have to make decisions about the new electronic surveillance systems, here are 10 important points to consider.

1. Vendor. Does the vendor have any past experience working with public health agencies or population-based data?
2. Validation. Has there been any attempt to assess the sensitivity and specificity of the system or solution in detecting potential cases? A system should not generate false alarms or miss real events. Strategies for validation have included using proxy diseases with similar characteristics and using traditional communicable disease outbreaks.
3. Flexibility. Is the system flexible in the ways it can acquire data—flat file imports, SQL queries, and so on—or does it require that incoming data be sent as health level 7 (HL-7) messages? Many information systems, especially small ones such as those found in clinics or emergency departments (EDs), cannot "speak" HL-7. Even when both systems can communicate, often substantial work is required to build an interface capable of converting data in one message stream to a format usable by another application. We don't mean to downplay the value of HL-7, which is certainly a huge head start in getting data from one system to another. But make sure to budget for these interfaces.
4. Expandability. How easy is it to add additional hospital, pharmacy, primary-care clinic, or urgent care data streams to the system? What are the database's limitations in terms of concurrent data entry and data storage? Systems based on desktop database products may work fine for small counties with a single hospital but may not scale up to a large metropolitan area. Similarly, how easily can the system store data of multiple types? Can it store pharmacy data and ED visit data, or is it designed for collection and analysis of a single data type?
5. Operation/timeliness/reliability. How often are data compiled and how often are data analyzed? Does the system operate 24 hours a day, seven days a week, with automated posting of potential cases from existing databases, or does it require human or manual intervention on either end? Both types of solutions are applicable to disease surveillance. Manual systems are not the most effective way of collecting large volumes of data during disease outbreaks, but are vital for collecting data for traditional disease investigation and reporting.
6. Notification. How does the system alert end-users or health officials in the case of missing data for suspected events? Does it page or send e-mail? Does it require acknowledgments to alerts? Can it escalate alerts if not acknowledged, or does it require daily inspection of its output to determine unusual patterns?
7. Usability. How interpretable is the output from different systems? Are epidemiologists and other users able to interpret information and differentiate real events and disease outbreaks from background noise?
8. Security. Over what security protocols is information transmitted and what protections have been taken to ensure network security? Standard e-mail is not an acceptable mode of data transmission. Communications should be made using strongly encrypted protocols, such as SSL, SSH, or using file encryption strategies.

9. Compatibility. Is the system contributing to and taking part in efforts to integrate these types of notifiable disease reports into the National Electronic Disease Surveillance System (NEDSS) or its state implementation? Is the system integrated with the Health Alert Network?
10. Supportability. Interfaces change, standards change, and hospital information systems change. Any surveillance system will require ongoing development and maintenance to remain viable. Without strong in-house technical expertise, a typical health department will need to turn to a vendor or consultant to maintain the system. Factor in costs of ongoing maintenance, operations, and training.

An effort to draft new guidelines specifically for evaluating electronic disease surveillance systems will be discussed at the National Syndromic Surveillance Conference in September 2002.

Authors

Bryant T. Karras, MD, is on the faculties of the School of Public Health and Community Medicine and the School of Medicine at the University of Washington. William B. Lober, MD, is on the faculty of School of Medicine at the University of Washington. Karras and Lober are helping build and evaluate a metropolitan data collection system to support syndromic surveillance. Gregory T. Smith, MPA, directs the development of a statewide system for combined laboratory and syndromic surveillance for the Washington State Department of Health.

Resources

Updated Guidelines for Evaluating Public Health Surveillance Systems. MMWR 2001; 50(RR-13). www.cdc.gov/mmwr/PDF/RR/RR5013.pdf

National Syndromic Surveillance Conference, www.nyam.org/events/syndromicconference/