Agency for Healthcare Research and Quality

Evidence Report/Technology Assessment

Number 59

Bioterrorism Preparedness and Response: Use of Information Technologies and Decision Support Systems

Summary

Overview

The Nation's capacity to respond to bioterrorism depends in part on the ability of clinicians and public health officials to detect, manage, and communicate during a bioterrorism event. Information technologies and decision support systems (IT/DSSs) have the potential to aid clinicians (e.g., physicians, nurses, nurse practitioners, and respiratory therapists) and public health officials to respond effectively to a bioterrorist attack.

The Evidence Report from which this summary was taken details the methodology, results, and conclusions of a systematic and extensive search for published materials on the use of IT/DSSs to serve the information needs of clinicians and public health officials in the event of a bioterrorist attack. The information is intended to assist clinicians, public health officials, and policymakers to improve preparedness for a bioterrorism event.

Reporting the Evidence

The University of California at San Francisco (UCSF)–Stanford Evidence-based Practice Center staff, in conjunction with a panel of expert advisors and the Agency for Healthcare Research and Quality (AHRQ), developed the following four Key Questions to be addressed in this report:

1) *What are the information needs of clinicians and public health officials in the event of a bioterrorist attack?*
2) *Based on the information needs identified for these decisionmakers, what are the criteria by which IT/DSSs should be evaluated with respect to usefulness during a bioterrorism event?*
3) *When assessed by these criteria, in what ways could existing IT/DSSs be useful during a bioterrorism event? In what ways are they limited?*
4) *In areas where existing IT/DSSs do not meet the information needs of clinicians or public health officials, what functional and technical considerations are important in the design of future IT/DSSs to support response to bioterrorism events?*

Methodology

Conceptual Model

A conceptual model was developed to specify the decisions and tasks involved in diagnosis, management, prevention, surveillance, and communication by clinicians and public health officials in the event of a bioterrorist attack. The investigators used a process called task decomposition to specify the data requirements that need to be incorporated into an IT/DSS for it to assist clinicians and public health officials in making these decisions. This list of tasks and data requirements served as the foundation of the evaluation system of the currently available IT/DSSs.

Inclusion and Exclusion Criteria

Based on input from the expert advisory panel, the conceptual model, the task decomposition, and practical considerations, an inclusion-exclusion strategy was developed to identify articles that described or evaluated IT/DSSs.

Selection of Quality Scales

A scale developed at McMaster University was used to rate the quality of evidence from peer-reviewed evaluations of IT/DSSs for diagnosis, management, and communication. For reports of surveillance systems, an evaluation scale published

by the Centers for Disease Control and Prevention (CDC) was used.

Literature Sources

In consultation with professional research librarians, a search strategy for references from three sources was developed: peer-reviewed articles, government reports, and Web-based information. For the peer-reviewed articles, five databases of medical, scientific, and government references likely to contain reports of relevant IT/DSSs were identified: MEDLINE® (January 1985 to April 2001), the Catalog of U.S. Government Publications, GrayLIT, the Library of Congress, and the National Technical Information Service. The investigators identified the 16 government agencies most likely to fund, develop, or use IT/DSSs that could also be used by clinicians or public health officials. Internet searches to retrieve reports of potentially relevant IT/DSSs from sites other than those operated by government agencies (e.g., academic and commercial sites) were also planned.

Search Strategies

Separate search strategies were developed, one for MEDLINE® and one for the government documents and Web-based information. Each included terms such as *bioterrorism, biological warfare, information technology, decision support system, diagnosis, management, therapeutics, communication, surveillance, public health*, and *epidemiology*. Additional articles were identified by members of the expert advisory panel, from conference proceedings, and by review of reference lists.

Data Collection and Analysis

Titles, abstracts, and full-length articles were reviewed as necessary to identify potentially relevant articles. All peer-reviewed articles that met the inclusion criteria were blinded to the investigators, two of whom independently abstracted study information on to a data-abstraction and quality-assessment form.

The following data were abstracted from all included articles: the purpose and description of the system (e.g., detection, diagnosis, management, surveillance, or communication), whether the system had been clinically evaluated and the results of these evaluations, what security measures the system uses, what kind of reasoning the system uses, and information about the quality of the report. A draft Evidence Report was critiqued by 16 expert advisors and 17 peer-reviewers who had expertise in nursing, clinical medicine, public health, hospital management, informatics, diagnostics, emergency management, epidemiology, national security, toxicology, and food safety.

Findings

The investigators reviewed a total of 16,888 citations of peer-reviewed articles, 7,685 Web sites of government agencies, and 1,107 non-government Web sites. Of these, 251 articles, 36 government Web sites, and 54 non-government Web sites met the inclusion criteria. From these, descriptions were abstracted of 217 IT/DSSs of potential use by clinicians and public health officials in the event of a bioterrorist attack. They are comprised of 55 detection systems, 23 diagnostic systems, 18 management systems, 90 surveillance systems, 26 communication systems, and 7 systems that integrate surveillance, communication, and command and control functions (some systems have more than 1 function and are described in more than 1 section). Most reports only described IT/DSSs; however, 79 studies evaluated 58 systems for at least 1 performance metric. Some types of systems have been evaluated more than others. For example, 10 of the 18 management systems have been evaluated in at least 1 study; but none of the 7 integrated surveillance, communication, and command and control systems has been evaluated. Most of the 217 included systems were not designed specifically for bioterrorism; instead, they were created for detecting and managing naturally occurring illness. The few systems that were designed for bioterrorism are principally for detection and integrated command and control purposes, and most were designed by the military and are being converted for civilian use. There are almost no publicly available evaluative data on these systems, although the military developers may have performed comprehensive evaluations.

Key Question 1

What are the information needs of clinicians and public health officials in the event of a bioterrorist attack?

Based on the conceptual model and task decomposition, the information required by clinicians and public health officials while preparing for and responding to bioterrorist events relates to the decisions they have to make and the tasks they have to perform.

Clinicians require the necessary information to make diagnostic, management, prevention, and reporting decisions. Diagnostic decisions require information to accurately estimate the pre-test probability of disease for a given patient. Clinicians' interpretations of test results require information about the sensitivity and specificity of the test. Management decisions require information about how to appropriately distinguish between those patients who need treatment and those who do not, how best to treat the acutely ill, whom to isolate and how, how to manage scarce resources, and how to maintain personal safety. Prevention decisions require information about prophylaxis and vaccination protocols. Reporting decisions rely on information about what

constitutes a reportable case or cluster of cases and about the kinds of data that public health officials seek.

The information that public health officials require to prepare for and respond to a bioterrorism event can be considered in relation to the decisions they must make: the interpretation of surveillance data; the investigation of outbreaks; the institution of epidemiologic control measures; and the issuance of surveillance alerts. The decision to perform outbreak investigation requires information about the baseline characteristics of the surveillance data and threshold levels that suggest that an outbreak resulting from naturally occurring or bioterrorism-related illness may have occurred. Once a bioterrorism event has been identified, public health officials require information that will enable them to perform ongoing surveillance in the midst of the crisis to track the extent and spread of the epidemic. The decisions regarding the institution of epidemiologic control measures that prevent the spread of disease require information about the transmissibility of the suspected biothreat agent(s) and about the criteria for and effectiveness of prophylaxis and quarantine strategies. Decisions to issue a surveillance alert require information about the nature of the suspected bioterrorist attack and the characteristics and expected natural history of the suspected biothreat agent(s). Other communication decisions relate to the specific information that needs to be conveyed to other public health officials, clinicians, the media, and other decisionmakers.

Key Question 2

Based on the information needs identified for these decisionmakers, what are the criteria by which IT/DSSs should be evaluated with respect to usefulness during a bioterrorism event?

The evaluation criteria vary depending on the purpose of the IT/DSS and the information needs of the users of the system as determined by task decomposition methodology.

- All included systems—the purpose of the system; type of hardware required; methods for maintaining security of samples and data collected; timeliness; and measures of the accuracy of the system (e.g., sensitivity, specificity, collection efficiency, or concentration of organisms detected).
- Detection systems—portability; number of samples that can be run simultaneously; number of biothreat agents that can be identified; and whether both toxins and organisms can be identified.
- Diagnostic, management, and prevention DSSs—the type of information required by the DSS (e.g., a manually entered list of signs and symptoms provided by the clinician or patient information from an electronic medical record); the type of information provided by the DSS (e.g., a list of differential diagnoses, antibiotic recommendation, or quarantine recommendation); whether the biothreat agents and their associated illnesses are included in the knowledge base; the method of reasoning used by the inference engine; and information regarding the ability to update the probability of biothreat-related illness as the epidemic progresses or from reports of a known attack.
- Surveillance systems—the type of surveillance data collected; methods for determining when an outbreak has occurred; and information regarding the public health importance of the health event under surveillance, the system's usefulness, simplicity, flexibility, acceptability, representativeness, and the direct costs needed to operate the system.
- Reporting and communication systems—the type of information the system is intended to communicate; the intended provider and recipient of the information; and whether the recipient has to actively seek the information from the provider (e.g., by visiting a Web site) or the information is transmitted by phone, fax, e-mail, or other means to the recipient (i.e., passive on the part of the recipient).

Key Question 3

When assessed by these criteria, in what ways could existing IT/DSSs be useful during a bioterrorism event? In what ways are they limited?

The review identified 217 IT/DSSs, few of which were designed specifically for response to bioterrorism events. Most included systems had other intended purposes but could potentially be useful to clinicians or public health officials in response to a bioterrorism event. The evidence by which to judge the usefulness of these systems is limited. Many of the systems were not evaluated even for their intended purpose. Of the studies that did evaluate systems for their intended purpose, few adhered to published criteria for high-quality evaluations. In addition, even if a system received a favorable evaluation for its intended purpose, it may not necessarily be feasible to evaluate its usefulness for response to bioterrorism.

Detection systems. Fifty-five detection systems that collect and identify potential biothreat agents within environmental and clinical samples were identified. Many of these systems were developed for use by the military and some were adapted for civilian purposes. Few reports compare detection systems to a gold standard, and their sensitivity (i.e., the likelihood that the detection system will give a positive result when testing a sample containing a biothreat agent) and specificity (i.e., the likelihood that the detection system will give a

negative result when testing a sample that does not contain a biothreat agent) remain poorly characterized in the publicly available literature. Most identification systems are limited in that each test cycle can evaluate a sample for only a single biothreat agent, often run only a limited number of samples at a time, and cannot test for many of the most worrisome agents (e.g., smallpox). No reports were found that directly compared two or more of the commercially available systems in any given category. The paucity of comprehensive evaluative information about these systems prevents conclusions about whether or not these systems are likely to serve the detection needs of first-responders, clinicians, and public health officials during a bioterrorist event.

Diagnostic systems. Twenty-three diagnostic systems with potential utility for enhancing the likelihood that clinicians consider the possibility of bioterrorism-related illness were identified. These systems are generally designed to assist clinicians in developing a differential diagnosis for a patient who has an unusual clinical presentation. The investigators found six general diagnostic systems, four systems designed to improve radiologic diagnoses, four telemedicine systems, four systems for the diagnosis of infectious diseases, one system for the diagnosis of dermatologic lesions, one system for the diagnosis of community-acquired pneumonia, and three systems for other purposes. None of these DSSs has been evaluated formally with respect to bioterrorism response. In an evaluation of a DSS for infectious diseases that has more than 20 biothreat agents in its knowledge base, the system was able to list the actual diagnosis in an output of possible diagnoses for nearly 95 percent of 495 actual and hypothetical cases. However, this system is limited in that it is specific for infectious diseases; consequently, even those clinicians with access to this technology may not use it if the patient does not present with a fever or other signs or symptoms of infectious disease.

Three of the general diagnostic DSSs have been evaluated for their intended (non-bioterrorism related) purposes. In these evaluations, the general diagnostic DSSs typically performed better than physicians-in-training but not as well as experienced clinicians. However, the accuracy of the DSSs decreased for difficult cases. The need for clinicians to manually enter patients' signs and symptoms into diagnostic DSSs—a laborious step that may be a barrier to the use of these systems and has been demonstrated to increase inter-user variability—is eliminated by the few systems that automatically collect patient data from an electronic medical record. For example, there are diagnostic DSSs currently available in hospitals with electronic medical records that provide clinicians with an estimate of the likelihood of community-acquired pneumonia or active pulmonary tuberculosis based exclusively on data collected from the medical record. Many diagnostic DSSs use probabilistic information about the likelihood of disease. Because bioterrorism-related illness is relatively rare, in the event of bioterrorism these systems will have inappropriately low pretest probabilities for biothreat agents. None of the reports of diagnostic DSSs described the ability to change the probability of disease based on information about suspected bioterrorism events.

Management and prevention systems. Management and prevention systems are designed to make recommendations to clinicians by abstracting clinical information from electronic medical records to make patient-specific recommendations. None of the 18 systems identified in this review has been specifically designed or evaluated for utility in providing management or prevention recommendations during a bioterrorism event; however, 10 of them have been evaluated for their intended purpose. These evaluations demonstrate that the expert systems that continuously search electronic medical records (including data from the laboratory, radiology reports, and clinician notes) for new evidence of infection and apply clinical practice guidelines to those data are able to affect clinicians' antibiotic selection decisions and increase compliance with clinical practice guidelines. No information was found as to whether the knowledge bases of these systems include comprehensive information about bioterrorism-related illnesses. The systems that are not linked to electronic medical records share many of the limitations of the general diagnostic systems—including that clinicians may not use the system to seek advice for patients presenting with common viral syndromes (i.e., the bioterrorism-related syndromes). Antibiotic recommendation programs are typically designed to provide recommendations for antibiotics with the narrowest possible spectra, thereby reducing the risk of developing resistant organisms. If clinicians make antibiotic selection decisions while unaware of the true bioterrorism-related diagnosis and select narrow-spectrum antibiotics, they may not be effective against biothreat agents. Therefore, whether the use of these systems would be helpful or detrimental is not known.

Surveillance systems. Ninety surveillance systems that collect a variety of surveillance reports were identified: 7 for syndromal surveillance, 6 for reports from clinicians, 11 for influenza-related data, 23 for laboratory and antimicrobial resistance data, 16 for hospital-based infections data, 10 for food-borne illness data, 6 for zoonotic illness data, and 11 for other types of surveillance data. For a surveillance system to detect a covert bioterrorist event, it must collect data that are sensitive and specific for biothreat agents, analyze the data, and report results to public health decisionmakers in a timely manner. None of 90 included surveillance systems has been evaluated for its utility in detecting a bioterrorism event. Forty

of 61 reports of evaluations or descriptions of surveillance systems described the timeliness, importance of the health event under surveillance, and usefulness of the system. However, less than one-third of the reports of evaluations of surveillance systems described the representativeness, simplicity, sensitivity, specificity, acceptability, or flexibility of the system. The quality of the evidence regarding the effectiveness of the systems reported by these articles is therefore limited. Most of the evaluations of surveillance systems demonstrated that the electronic collection and reporting of surveillance data improved detection over older, manual methods. When the 90 surveillance systems described in this report are considered, there are relatively few systems collecting the earliest surveillance data—such as school and work absenteeism, calls to telephone care nurses, over-the-counter pharmacy sales, or veterinary or zoonotic illness—a potentially significant gap in available surveillance systems.

- *Syndromal surveillance.* The earliest symptoms caused by most biothreat agents are flu-like illness, acute respiratory distress, gastrointestinal symptoms, febrile hemorrhagic syndromes, and febrile illnesses with either dermatologic or neurologic findings. Therefore, patients with these syndromes are the targets of bioterrorism-related syndromal surveillance programs. None of the seven syndromal surveillance systems identified has been clinically evaluated; however, several evaluations are ongoing. These systems are highly heterogeneous with respect to the syndromes under surveillance, the definition of the syndromes, and the type of data collected. Some systems use routinely collected diagnostic codes, others use syndromal reports collected from triage nurses for all patients presenting to an emergency department, and several use clinicians' reports of syndromal data collected on selected patients. No evidence was found to determine which of the methods of collecting syndromal data is the most sensitive, timely, acceptable, and cost-effective.

  Syndromal surveillance systems have been used both for ongoing surveillance and for event-based surveillance. One syndromal surveillance tool, designed for ongoing collection of demographic and clinical data from remote regions of the developing world, downloads information daily to a national public health department. In event-based surveillance, the system is deployed for a limited period before, during, and after an event thought to be a potential target for bioterrorism, such as a major sporting or political event.
- *Surveillance networks of sentinel clinicians.* Because clinicians may be the first to recognize unusual or suspicious illnesses, reports from clinician networks are an important source of surveillance data for detection of bioterrorism-related diseases. Of the systems that have been evaluated for the collection of clinician reports, Eurosentinel provides the timeliest data (however, this is only true for influenza; data on other diseases and syndromes have a longer delay). The timeliness of the other systems varies from days to months. Systems that collect data on a weekly basis will be substantially less useful for bioterrorism surveillance than systems that can provide more rapid collection and analysis.
- *Influenza surveillance.* Although none of the 11 surveillance systems that collect influenza data has been evaluated specifically for the detection of bioterrorism-related illness, they are potentially useful for bioterrorism surveillance in 3 ways. First, sentinel clinicians who report on patients with suspected influenza are experienced at applying a case definition to a clinical population for the collection of public health data. Because many bioterrorism-related illnesses present with a flu-like illness, this network of trained sentinel clinicians could provide valuable surveillance data. (One should note that the evaluation of these sentinel clinicians is derived from heterogeneous surveillance networks in North America, Europe, and Australia. It is difficult to know whether the cultures of medicine, the training that sentinel clinicians receive, and their commitment to public health surveillance efforts are sufficiently similar that one can assume that the results of an evaluation of a surveillance network in France will be generalizable to clinicians in the United States.) Second, examples exist of effective influenza surveillance systems that integrate clinical and laboratory data for the detection of influenza outbreaks. Surveillance for bioterrorism may be aided by similar integration of multiple data sources. Finally, influenza surveillance, like bioterrorism surveillance, requires a coordinated global effort. New programs for the surveillance of bioterrorism-related illness could utilize the historical relationships that have been developed for influenza surveillance. Several of the influenza systems rely on weekly reporting by clinicians—for bioterrorism surveillance, this time lag is likely to be problematic.
- *Laboratory surveillance.* Laboratory surveillance systems are an essential component of any system for the detection of a covert bioterrorist event, both for the detection of uncommon organisms (e.g., smallpox, anthrax, and Ebola) and common organisms with unusual antimicrobial resistance patterns. Systems that facilitate the collection, analysis, and reporting of notifiable pathogens and antimicrobial resistance data could potentially facilitate the rapid detection of a biothreat agent. This search identified 12 systems for the surveillance of laboratory data (4 of which were described in peer-reviewed evaluation reports) and 11 systems for the surveillance of antimicrobial data (1 of which was

described in a peer-reviewed evaluation report). In general, the evaluative and descriptive reports of the systems collecting laboratory and antimicrobial resistance data suggest that the electronic systems improve the timeliness and sensitivity of conventional methods. Few reports specifically described how laboratory samples are handled, acceptability, or cost of implementation.

Laboratories that already report data in an electronic format to local public health officials could be incorporated into bioterrorism surveillance systems at local, State, national, and international levels—creating a "network of networks." A principal challenge for laboratory networks is the timely communication of data from collection sites to central surveillance agencies. Efforts are ongoing to address these issues. Specifically, the Laboratory Response Network, which builds on existing laboratory capacity and is currently under active expansion, has been designed with the specific intention of being able to be integrated into surveillance networks (such as the CDC's National Electronic Disease Surveillance System) and communication networks (such as the California initiative to develop a Rapid Health Electronic Alert, Communication, and Training [RHEACT] system). These systems are under development and have not been evaluated.

- *Hospital-based surveillance.* The 16 hospital-based surveillance systems could play 2 roles in the early detection of a covert bioterrorist attack: the identification of a cluster of cases recently admitted suggestive of a community-based outbreak, and the identification of a cluster of cases within the hospital suggestive of inpatients with an unrecognized communicable disease. However, the reports of the surveillance systems for hospital-acquired infections suggest that, although these systems could be a valuable tool for hospital infection control officers, there is little evidence to demonstrate that they have sufficient sensitivity, specificity, or timeliness to detect a community-based bioterrorism event.
- *Foodborne and zoonotic disease surveillance.* Terrorism attacks may be made against food and agriculture production facilities (domestically or abroad), transportation systems, water supplies (for either human consumption or to contaminate food production), farm workers, food handlers, and processing facilities. Similarly, concerns exist that a bioterrorist attack could involve the dissemination of a zoonotic illness among animal populations with the intention of infecting humans or livestock and causing economic and political chaos. Six ITs designed to collect, process, and disseminate information on zoonotic and animal diseases were found, none of which has been described in a peer-reviewed evaluation. Mosquito-borne viruses such as West Nile Virus, St. Louis encephalitis, and Western equine encephalomyelitis are all targets of ongoing zoonotic surveillance programs. The search found reports of only two zoonotic surveillance systems—a major gap in the literature of bioterrorism surveillance efforts. Most of the reports provided little or no information about the timeliness of these systems; those that did suggest lag times that would be too long for effective bioterrorism surveillance. None has been specifically evaluated for this purpose. In addition, the surveillance systems that collect data on food-borne illnesses and laboratory information about DNA strains of food-borne pathogens are limited in that they only collect routine surveillance data on a small number of pathogens (and do not typically include all of the most worrisome agroterrorism-related agents).

Communication systems. Eight of the 26 communication systems were designed for communication among public health officials at local, State, and Federal levels (e.g., Web-based discussion and reporting of surveillance data). In pilot evaluations directed by individual State health departments, these systems securely managed the disease reporting needs of local and State public health officials. However, these systems were limited to communication within a State. No single system was found that effectively links members of the public health community at national, State, and local levels. However, there are ongoing efforts (such as the Urban Security Initiative project of Los Alamos National Laboratory, EpiX, Health Alert Network and RHEACT) designed to integrate communication of public health information vertically and horizontally within the U.S. public health system. Five systems were designed for the automated communication of information from hospital-based electronic medical records to clinicians (e.g., alerting systems to notify clinicians of abnormal laboratory tests). These systems have been subjected to the greatest evaluation of all the communication systems. Despite being limited to institutions with electronic medical records, they could potentially play an important role in improving the timely recognition of bioterrorism-related illness. Three systems facilitated communication between emergency departments and first-line emergency response personnel. ProMED© has demonstrated the capacity for rapid reporting and dissemination of information on a wide range of infectious diseases resulting from both naturally occurring and bioterrorism-related events. During a bioterrorism event, clinicians must be able to rapidly communicate with their patients. Systems exist that enable Web-based communications between these parties in a manner compliant with the Health

Insurance Portability and Accountability Act of 1996 (HIPAA). Robust security measures that ensure patient confidentiality and resist cyberattack will be a necessary component of any bioterrorism-related communication system.

Key Question 4

In areas where existing IT/DSSs do not meet the information needs of clinicians or public health officials, what functional and technical considerations are important in the design of future IT/DSSs to support response to bioterrorism events?

No evaluations or studies that directly assess the functional and technical requirements that are important for future IT/DSSs were identified. This section provides the investigators' interpretation of factors that could be considered for the design of future IT/DSSs.

- IT/DSSs for bioterrorism need to have documented sensitivity, specificity, and timeliness that are appropriate for their intended use. Because both false-positive and false-negative results can result in serious adverse outcomes, sensitivity and specificity should generally be high. Similarly, timeliness is of critical importance for IT/DSSs that aid with detection, diagnosis, management, communication, and surveillance. Systems should have measures to maintain security of samples and data collected.
- Detection and diagnostic systems must be in use in the affected area. In the event of a covert attack, collection systems will have to be in place in areas of likely attack. In the event of a known attack, these systems must be portable and sufficiently rapid that they can be used in a variety of field and clinical situations.
- Clinicians would be helped by detection methods that include all of the most worrisome biothreat agents, by systems that can test an individual sample for multiple biothreat agents simultaneously, and by systems that can run multiple samples simultaneously.
- Because the individuals collecting and analyzing the environmental and clinical samples are often at considerable distance from public health decisionmakers, detection systems could benefit from the capacity for secure transmission of data to these decisionmakers.
- Efforts to link diagnostic and management or prevention DSSs to other hospital information systems would reduce the data entry burden substantially.
- The knowledge bases of diagnostic and management systems need to include current information and clinical practice guidelines about bioterrorism-related illness. The systems need to be able to appropriately adjust the probability of disease caused by biothreat agents if a known bioterrorism event has occurred.
- Efforts to integrate surveillance data may benefit from definitions of the syndromes under surveillance; comprehensive analysis of the sensitivity, specificity, and timeliness of each source of surveillance data; improved spatial and temporal analysis methods; and systems that collect sources of data reflecting disease earlier in the course of illness (e.g., school and work absenteeism and over-the-counter pharmacy sales).
- Communication systems that protect patient confidentiality and have adequate security measures would be useful for the rapid dissemination of outbreak-related information among all relevant decisionmakers, including public health officials, clinicians, and the public.

Conclusions

IT/DSSs have the potential to help clinicians and public health officials make better decisions when responding to a bioterrorism event. IT/DSSs were identified that could potentially aid with detection, diagnosis, management, prevention, surveillance, and communication. However, most of these systems were not designed specifically for bioterrorism. Many of these systems have not been described in peer-reviewed literature, and fewer still have been evaluated rigorously. The existing evaluations primarily assess the usefulness of systems for their intended purpose, and often do not provide direct evidence about the usefulness of the IT/DSSs for bioterrorism.

The lack of evaluative studies creates difficulties in assessing the usefulness of IT/DSSs. For detection systems, almost no information is available on sensitivity and specificity. Without this information, interpretation of test results is highly problematic. Diagnostic DSSs have not been used widely, and several of the available systems require time-consuming manual input of patient data, which is impractical in many clinical settings. Whether management DSSs could be useful for bioterrorism-related disease remains unanswered. Surveillance systems hold promise, and although many are undergoing evaluation, the systems designed for bioterrorism response have been fielded only recently. Web-based communication systems are increasingly available to link public health officials with clinicians and the public; however, their efficacy in crisis situations is untested.

This review suggests important gaps in the available literature. One should note, however, that lack of evidence about effectiveness is not evidence for lack of effectiveness. Many of the systems reviewed may indeed be useful for response to bioterrorism and are reasonable candidates for further evaluation. Such evaluations would clarify their value

both for response to bioterrorism and for the other purposes for which they were designed.

Future Research

In addition to the development of systems described in the answer to Key Question 4, the following future research could provide additional insights into the information needs of clinicians and public health officials and the types of IT/DSSs that may best serve those needs:

- Further research is needed for the development and evaluation of systems as outlined in the answer to Key Question 4.
- Further research is needed that investigates the decisions and tasks of specific types of clinicians (e.g., primary care providers, emergency medicine specialists, and infectious disease specialists), different types of public health officials (e.g., those working in county public health departments, at the CDC, and in the Department of Health and Human Services), and other groups of relevant decisionmakers (e.g., laboratory personnel, paramedics, veterinarians, and hospital administrators).
- Evaluations of current systems and the interaction of these systems during simulated bioterrorism events are currently under-reported, not available yet, or potentially classified. Detailed evaluations of IT/DSSs and situations where their use might enhance decisionmaking would guide further system development and evaluation research.
- Methodologies other than systematic review would provide additional valuable insight into the answers of the Key Questions addressed in this report. For example, surveys of clinicians and public health officials could be used to better describe the information needs of these groups in preparing for and responding to bioterrorism events, the IT/DSSs currently in use, and the performance of these systems in routine use and times of crisis.
- Further research is needed on how to provide effective training in the use of IT/DSSs and how to provide effective continual medical education to enhance the diagnostic capabilities of clinicians for bioterrorism-related illness through DSSs or other approaches.
- Further research is needed on how to maintain the security and availability of systems in times of crisis.

Ordering Information

The full Evidence Report from which this summary was taken was prepared for AHRQ by the UCSF-Stanford Evidence-based Practice Center under contract No. 290-97-0013. It is expected to be available in summer 2002. At that time, printed copies may be obtained free of charge from the AHRQ Publications Clearinghouse by calling 800-358-9295. Requesters should ask for Evidence Report/Technology Assessment No. 59, *Bioterrorism Preparedness and Response: Use of Information Technologies and Decision Support Systems.* Internet users will be able to access the report online through AHRQ's Web site at www.ahrq.gov.

AHRQ Pub. No. 02-E027
June 2002

ISSN 1530-440X