A Conceptual Framework for Evaluating Information Technologies and Decision Support Systems for Bioterrorism Preparedness and Response

Dena M. Bravata, Kathryn M. McDonald, Herbert Szeto, Wendy M. Smith, Chara Rydzak and Douglas K. Owens

Med Decis Making 2004 24: 192
DOI: 10.1177/0272989X04263254

A Conceptual Framework for Evaluating Information Technologies and Decision Support Systems for Bioterrorism Preparedness and Response

Dena M. Bravata, MD, MS, Kathryn M. McDonald, MM, Herbert Szeto, MD, MS, MPH, Wendy M. Smith, BA, Chara Rydzak, BA, Douglas K. Owens, MD, MS

Objectives. *The authors sought to develop a conceptual framework for evaluating whether existing information technologies and decision support systems (IT/DSSs) would assist the key decisions faced by clinicians and public health officials preparing for and responding to bioterrorism.* ***Methods.*** *They reviewed reports of natural and bioterrorism-related infectious outbreaks, bioterrorism preparedness exercises, and advice from experts to identify the key decisions, tasks, and information needs of clinicians and public health officials during a bioterrorism response. The authors used task decomposition to identify the subtasks and data requirements of IT/DSSs designed to facilitate a bioterrorism response. They used the results of the task decomposition to develop evaluation criteria for IT/DSSs for bioterrorism preparedness. They then applied these evaluation criteria to 341 reports of 217 existing IT/DSSs that could be used to support a bioterrorism response.* ***Main Results***. *In response to bioterrorism, clinicians must make decisions in 4 critical domains (diagnosis, management, prevention, and reporting to public health), and public health officials must make decisions in 4 other domains (interpretation of bioterrorism surveillance data, outbreak investigation, outbreak control, and communication). The time horizons and utility functions for these decisions differ. From the task decomposition, the authors identified critical subtasks for each of the 8 decisions. For example, interpretation of diagnostic tests is an important subtask of diagnostic decision making that requires an understanding of the tests' sensitivity and specificity. Therefore, an evaluation criterion applied to reports of diagnostic IT/DSSs for bioterrorism asked whether the reports described the systems' sensitivity and specificity. Of the 217 existing IT/DSSs that could be used to respond to bioterrorism, 79 studies evaluated 58 systems for at least 1 performance metric.* ***Conclusions.*** *The authors identified 8 key decisions that clinicians and public health officials must make in response to bioterrorism. When applying the evaluation system to 217 currently available IT/DSSs that could potentially support the decisions of clinicians and public health officials, the authors found that the literature provides little information about the accuracy of these systems.* ***Key words:*** *decision support techniques; bioterrorism; public health; information systems; expert system.* ***(Med Decis Making 2004;24:192–206)***

On 4 October 2001, the first confirmed case of inhalational anthrax caused by an act of bioterrorism was identified in the United States.[1] During the months that followed, clinicians and public health officials across the country endeavored to care

Received 4 March 2003 from the Center for Primary Care and Outcomes Research, Stanford University, Stanford, California (DMB, KMM, WMS, CR, DKO); the Department of Internal Medicine, Kaiser Permanente, Redwood City, California (HS); Veterans Affairs Palo Alto Healthcare System, Palo Alto, California (DKO); and the Department of Health Research & Policy, Stanford University School of Medicine, Stanford, California (DKO). This work was performed by the UCSF-Stanford Evidence-Based Practice Center under contract to the Agency for Healthcare Research and Quality (contract number 290-97-0013) Rockville, Maryland. The project also was supported in part by the Department of Veterans Affairs. Portions of this work were presented at the 24th annual meeting of the Society for Medical Decision Making, Baltimore, Maryland, 22 October 2002. We thank Sara Cody, Santa Clara County communicable disease officer, for her many valuable suggestions informed by her frontline experiences and Emilee Wilhelm and Jon-Erik Holty for their careful editorial assistance. Revision accepted for publication 12 January 2004.

Address correspondence and reprint requests to Dena M. Bravata, MD, MS, Center for Primary Care and Outcomes Research, 117 Encina Commons, Stanford, CA 94305-6019; e-mail: bravata@healthpolicy.stanford.edu.

DOI: 10.1177/0272989X04263254

for the victims of anthrax bioterrorism, those who were potentially exposed to the *Bacillus anthracis* spores, and the worried as well. These efforts were complicated by a lack of accurate rapid diagnostic technologies, automated processes for bioterrorism surveillance, and methods for rapid communication among relevant clinical and public health decision makers.[1–10] The anthrax cases of 2001 emphasized that the capacity of the United States to respond to bioterrorism depends on the ability of clinicians and public health officials to detect the event rapidly, to manage the consequences efficiently, and to communicate with each other effectively.[1–10]

To improve the infrastructure to respond to future infectious disease outbreaks resulting from either naturally occurring or bioterrorism-related illness, the US government has significantly expanded its budget for public health preparedness activities, including the deployment of information systems for bioterrorism surveillance, outbreak investigation, laboratory services, and communication. However, few information systems have been evaluated to determine whether they will meet the needs of users responding to a bioterrorism event. Moreover, the evaluation of existing technologies is complicated by the lack of a clear understanding of the information needs of clinicians and public health officials or an established framework for evaluating whether an information system serves these needs.

Under the auspices of the University of California, San Francisco (UCSF)-Stanford Evidence-Based Practice Center, we systematically reviewed the evidence that evaluates the ability of available information technologies and decision support systems (IT/DSSs) to serve the information needs of clinicians and public health officials during a bioterrorism response.[11] The results of the systematic review can be found elsewhere.[11] Briefly, we found 217 IT/DSSs of potential use by clinicians and public health officials during a bioterrorism response. These include 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. 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 (e.g., 10 of the 18 management systems have been evaluated in at least 1 study, whereas none of the 7 integrated surveillance, communication, or command and control systems have been evaluated). Specifically, there are no published evaluations of the systems designed specifically for bioterrorism responses.

Several existing frameworks for evaluating information systems are relevant to considerations of methods for evaluating IT/DSSs for bioterrorism preparedness and response. These evaluation frameworks differ according to the type of information system, purpose of the evaluation, and outcomes of interest.[12–16] We briefly describe 3 evaluation frameworks that informed our conceptual framework for evaluating IT/DSSs for bioterrorism preparedness and response. First, Eliyahu Goldratt's theory of constraints provides a framework for specifying the relevant stakeholders or decision makers, their decision processes, their information resources, and the evaluation processes relevant to a particular decision or conflict.[17,18] Thus, for a given bioterrorism response decision (e.g., diagnosis or management), evaluators of IT/DSSs could consider the relevant stakeholders (e.g., public health officials, clinicians, and patients), their responsibilities, their information needs, and methods for providing that information. Different stakeholders are often interested in different outcomes of evaluations of IT/DSSs for bioterrorism preparedness and response. For example, system developers are often interested in evaluating whether the system performs its intended function, users are often interested in whether the system provides recommendations that are fast and accurate, and purchasers are often interested in whether the system is cost-effective, reliable, and safe.[19] Second, Avedis Donabedian described a framework for evaluating IT/DSSs based on the 3 aspects of the health care system that can be influenced by an IT/DSS: structure (e.g., the physical characteristics of the IT/DSS such as the availability of equipment, costs, and number of staff who will use it), processes (e.g., the number and appropriateness of diagnostic and therapeutic interventions administered), and outcomes (e.g., morbidity, mortality, and quality of life).[20,21] An IT/DSS for bioterrorism may result in improved patient outcomes but deteriorations in structural components such as increased cost.[13,20] Because IT/DSSs typically contain several distinct structural components such as databases of medical knowledge and patient data, reasoning programs, and user interfaces, published evaluations of IT/DSSs often focus on 1 or more of these components. Finally, Friedman and Wyatt broadly described the 5 categories of interest in evaluations of medical IT/DSSs: the clinical need the resource is intended to address; the process used to develop the resource; the resource's intrinsic structure; the functions that the resource carries out; and the resource's influence on users, patients, and other aspects of the clinical environment.[13]

In this article, we describe the conceptual framework that we developed to identify the key decisions

and tasks that clinicians and public health officials are likely to face while responding to a bioterrorism event, specify the data and methods required of an IT/DSS to assist these key decisions and tasks, and describe the evaluation criteria to assess whether an IT/DSS is likely to facilitate decision making by clinicians and public health officials during a bioterrorism response. This evaluation framework could inform ongoing evaluations of IT/DSSs for bioterrorism preparedness and response.

METHODS

We present our approach for developing a conceptual framework and performing a systematic review to evaluate reports of IT/DSSs for bioterrorism preparedness and response in Figure 1. Because evaluations of information systems require a careful delineation of the tasks and information needs of users, we sought methods to systematically determine these tasks and information needs.[13,19,22–26] To describe the decisions that clinicians and public health officials would have to make while preparing for and responding to a bioterrorism event, we reviewed reports of naturally occurring and bioterrorism-related outbreaks of infectious diseases and bioterrorism preparedness exercises and solicited additional information from relevant experts.[1–10,27–44] We represented these decisions schematically using influence diagram notation.[23,24] This enabled us to identify and evaluate the relationships between the uncertain events that affect the decisions and what is observable to the decision maker. We then used task decomposition to identify the characteristics of IT/DSSs necessary to assist these decisions. Use of the task decomposition method facilitated a systematic appraisal of the component functions required of IT/DSSs.[22] From the schematic and task decomposition, we developed evaluation criteria for IT/DSSs designed to facilitate a bioterrorism response. In our systematic review, we then applied these evaluation criteria to 341 reports of 217 existing IT/DSSs that could be used for a bioterrorism response.[11]

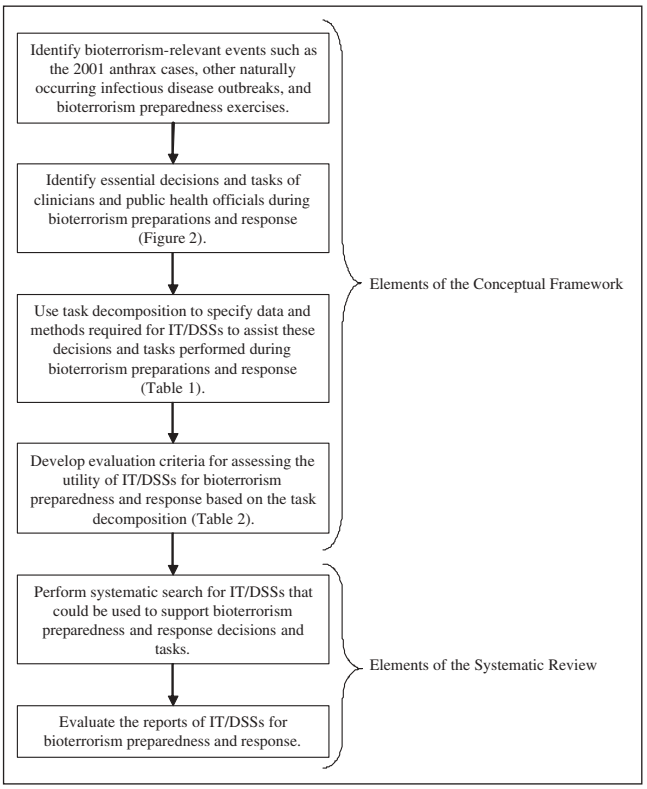

Figure 1 Approach to evaluating reports of information technologies and decision support systems (IT/DSSs) for bioterrorism preparedness and response. This figure describes the elements of the conceptual framework and systematic review for evaluating reports of IT/DSSs for bioterrorism preparedness and response. The conceptual framework is the subject of this article. The results of the systematic review are available elsewhere.[11]

Data Sources for the Determination of Key Decisions and Tasks

To describe the decisions that clinicians and public health officials have to perform to effectively respond to a bioterrorist attack, we reviewed reports of the 2001 anthrax cases,[1–10] TOPOFF and Dark Winter bioterrorism preparedness exercises,[27–29] a massive outbreak of *Cryptosporidium parvum* infection resulting from contamination of the public water supply in Milwaukee during March and April 1993,[30] an outbreak of West Nile Virus in New York City in late August 1999,[31] clinical practice guidelines for the treatment of the most relevant biothreat agents,[32–36] emergency preparedness assessments and planning documents,[37–40] standards for reporting public health surveillance data,[41–43] and standards for maintaining the security of electronic data.[44] In addition, we solicited input from local, state, and national public health officials and experts in bioterrorism preparedness and response, clinical medicine, and medical informatics.

When evaluating the information provided by these sources, we attempted to identify the nature of the infectious disease outbreak described, the types of decision makers involved in the response to the outbreak, the information needed to make their decisions and perform their tasks, the information technologies used during the response and their effects on the outcome, and any lessons learned by the key decision makers. For example, we reviewed descriptions of a weapons of

mass destruction exercise called TOPOFF (because it was designed to test the readiness of TOP OFFicials of the government to respond to terrorist attacks) conducted by the US Department of Justice in May 2000 at a cost of $3 million.[27] TOPOFF simulated an aerosol release of *Yersinia pestis* in Denver. The officials participating in this exercise included public health officials, clinicians, and emergency management professionals. During the exercise, major problems were experienced in the following areas: leadership and decision making, resource distribution, and management of the crisis situations resulting from exceeding the capacity of the local hospital system.[27] Information technologies were unavailable for assisting in many of the decision-making processes during this exercise. In particular, IT/DSSs could have facilitated diagnostic decisions (e.g., the rapid diagnosis of plague among exposed individuals), management decisions (e.g., isolation of exposed individuals, treatment of the acutely ill, and maintenance of personal safety), outbreak control decisions (e.g., prevention of contagion), and communication among all participating decision makers and organizations.

Representation of the Key Decisions in a Schematic Using Influence Diagram Notation

We represented the key decisions made by clinicians and public health officials during a bioterrorism response identified from the sources described in the previous section in a schematic using influence diagram notation. Influence diagrams are graphical representations of formal mathematical models that facilitate the compact representation of the probabilistic structures of complex problems.[24,45,46] We adopted standard influence diagram notation such that decisions are represented by rectangular nodes.[25–27] Arrows between decision nodes indicate that at the time of the 2nd decision, the decision maker has knowledge of the previous decision. Probabilistic events are represented by elliptical (chance) nodes. Arrows between chance nodes indicate that a probabilistic relationship may exist. That is, the outcome of the 1st chance event may change the probability of the outcome of the 2nd. Arrows from a chance node to a decision node indicate that the outcome of the uncertain event is known at the time the decision is made.

The schematic allowed us to assess the relationships between the decisions made by the 2 types of decision makers, to identify the uncertain events that affect these decisions, and to evaluate the information that is observable by the decision makers at the time they make their decisions. The complexities of the processes involved in clinicians' and public health officials' responding to a bioterrorist attack created unique challenges for the application of standard influence diagram notation. Specifically, our conceptual model required the incorporation of different decision makers, different time horizons, and different value functions. We direct interested readers elsewhere for detailed discussions of graphical representations of temporal medical decision modeling.[47–52]

Task Decomposition and Determination of Evaluation Criteria

We used a process called "task decomposition" to describe the characteristics that would be required for IT/DSSs to serve the information needs of clinicians and public officials as they make the key decisions presented in our schematic.[22] Task decomposition provides a framework for specifying, documenting, and evaluating what types of data an IT/DSS should contain to serve its purpose.[53–55] Task decomposition starts with the identification of an IT/DSS's main purpose (or target task). Typically, this target task is then hierarchically decomposed into 3 components: subtasks, the methods used for accomplishing those subtasks, and the necessary and sufficient information for completing those subtasks using those methods. We extended the hierarchy 1 step further to articulate a 4th component, the evaluation criteria for determining the competence of the IT/DSS to address the subtask. We decomposed the information needs of clinicians and public health officials into top-level tasks and subtasks. We then considered the methods for accomplishing each subtask, the data required for an IT/DSS to assist that subtask, and the evaluation criteria to determine the competence of an IT/DSS in assisting that subtask. Although the identification of the tasks, subtasks, information, and methods for completing the subtasks were derived directly from our task decomposition, we augmented our evaluation criteria with our review of evaluations of IT/DSSs designed for bioterrorism-relevant tasks (e.g., diagnostic DSSs, management systems, communication systems), advice from experts, and published evaluation criteria for diagnostic tests, IT/DSSs for purposes not related to bioterrorism, and surveillance systems.[12–16,19,26,55–62]

For example, performing syndromic surveillance is a target task of public health officials. Monitoring outpatient visits for the diagnosis codes associated with fever and rash (i.e., subtask) is one way to implement a syndromic surveillance system. One method for collecting these diagnosis codes would be a daily automated count of diagnosis codes associated with febrile

illness and dermatologic conditions determined from electronically recorded outpatient diagnosis codes (i.e., methods and data/information necessary to accomplish this subtask). An IT/DSS facilitating this subtask could be evaluated for its timeliness (e.g., ability to deliver recommendations quickly), sensitivity, specificity, cost of data collection, and the geographic distribution of patients under surveillance (i.e., evaluation criteria). After considering the evaluation criteria relevant to the surveillance subtasks delineated through the task decomposition process, we augmented our evaluation criteria for the surveillance task with published criteria for evaluating syndromic surveillance systems.[62]

Applying the Evaluation Criteria

We applied the evaluation criteria developed from the task decomposition to 341 reports of 217 existing IT/DSSs for bioterrorism. A complete description of the systematic review including literatures searches, data abstraction, and application of the evaluation criteria to reports of existing IT/DSSs is available elsewhere.[11]

RESULTS

After reviewing the descriptions of clinicians and public health officials responding to bioterrorism-related and naturally occurring infectious disease outbreaks, we determined that during a bioterrorism event, clinicians and public health officials would each have 4 major types of decisions and tasks. Clinicians would have to 1) correctly diagnose the clinical manifestations of biothreat agents, 2) rapidly manage the care of potentially exposed patients, 3) take effective action to prevent the further spread of disease, and 4) report suspicious or confirmed cases to local, regional, and national public health officials. Public health officials would have to 1) collect, manage, and interpret surveillance data; 2) determine when and how best to perform outbreak investigation; 3) determine the timing and scope of outbreak control measures, such as quarantine, to prevent the spread of disease; and 4) communicate with first responders (e.g., fire, police, and hazardous materials personnel), clinicians, other public health officials, and the public.

The Key Decisions Represented as a Schematic Using Influence Diagram Notation

We represented these 8 major decisions in a schematic using influence diagram notation (Figure 2). The schematic depicts 3 critical time periods as follows. Time period 1 refers to the interval in which decisions are made by clinicians regarding the events associated with the initial cases. Time period 2 refers to the interval in which decisions are made by public health officials regarding the events associated with the initial cases. Time period 3 refers to the interval in which decisions are made by clinicians regarding the events associated with the subsequent cases. We recognize that time periods 1 and 2 are likely to occur concurrently but have represented them as separate events to enable clear delineation of the decisions made by clinicians and public health officials. Because some IT/DSSs are user specific (e.g., only used by clinicians), the differentiation of time periods 1 and 2 facilitated the identification and evaluation of appropriate IT/DSSs.

In time period 1, after a bioterrorism event occurs, a population may be exposed to an infectious agent (denoted by the "exposure chance node), and those who have been exposed may become infected (Figure 2). Susceptibility to the infectious agent may be affected by prior immunization or other host factors such as immunosuppression (denoted by the "susceptible" chance node). The true infection status of any patient is unknown to the clinician. Therefore, the chance node "infection status" represents the clinician's pretest probability of disease. After an exposure, a single patient with an unusual clinical syndrome or a cluster of cases may present to a clinician for evaluation (denoted by the "clinical syndrome" chance node). During time period 1, clinicians are faced with 4 types of decisions: diagnostic decisions, management decisions, prevention decisions, and reporting decisions. Diagnostic decisions such as the selection and interpretation of diagnostic tests are affected by the clinician's pretest probability of disease. The interpretation of diagnostic test results depends on the sensitivity and specificity of the test and the clinician's pretest probability of disease. Management decisions include those regarding triage, treatment of acutely ill patients, and maintenance of personal safety. They are affected by the clinician's interpretation of diagnostic tests (denoted by the chance node "test result") and the patient's clinical syndrome. Prevention decisions include prophylaxis and vaccination of exposed individuals. They are affected by the clinician's interpretation of diagnostic tests and by the probability of exposure. Reporting decisions are affected by the clinician's interpretation of diagnostic tests (e.g., if a diagnostic test suggests anthrax, a clinician is likely to report this case to public health officials) and clinical syndrome (e.g., some highly atypical clinical syndromes or clusters of patients may also trigger the deci-

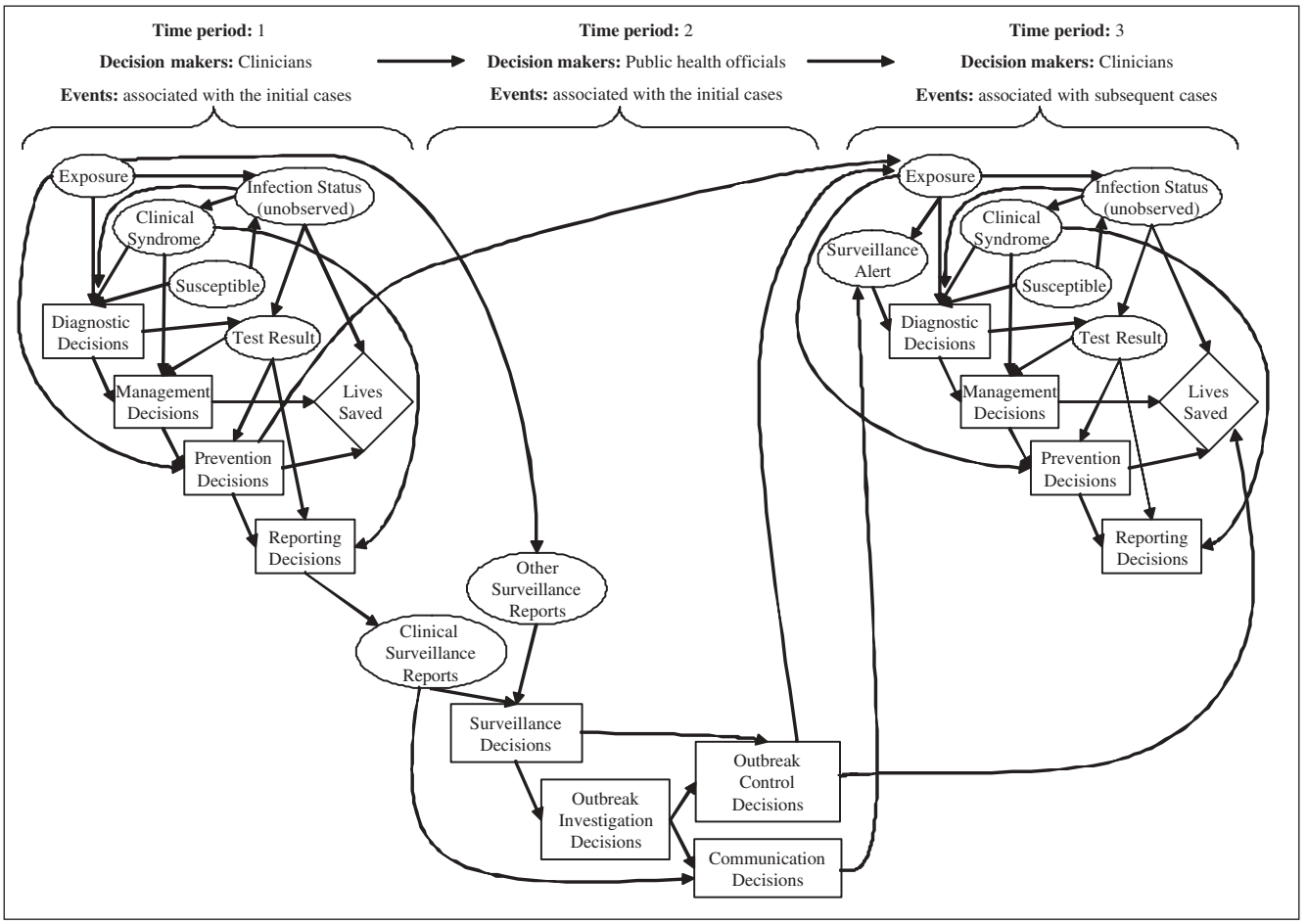

Figure 2 Schematic of decisions made by clinicians and public health officials during a bioterrorism response. This figure uses influence diagram notation to depict the key decisions of clinicians and public health officials responding to bioterrorism (rectangular decision nodes), to identify the uncertain events affecting these decisions (elliptical chance nodes), and to evaluate the information that is observable by the decision makers at the time they make their decisions. The schematic depicts 3 critical time periods as follows: time period 1 refers to the interval in which decisions are made by clinicians regarding the events associated with the initial cases, time period 2 refers to the interval in which decisions are made by public health officials regarding the events associated with the initial cases, and time period 3 refers to the interval in which decisions are made by clinicians regarding the events associated with the subsequent cases. The decisions and processes depicted in this figure could be supported by information technologies and decision support systems designed to facilitate bioterrorism preparedness and response.

sion to report). The desired outcome of this decision-making process (denoted by the diamond in Figure 2) could be lives saved, morbidity prevented, or dollars saved; it is affected by the patient's infection status and by management and prevention decisions.

In time period 2, public health officials are faced with 4 types of decisions: surveillance decisions, outbreak investigation decisions, outbreak control decisions, and communication decisions. In Figure 2, we denote the surveillance reports that could be received by public health officials by the 2 chance nodes "clinical surveillance reports" and "other surveillance reports." The node "clinical surveillance reports" includes any information from clinicians about potential bioterrorism-related illness (either from formal bioterrorism surveillance systems in which clinicians submit reports of patients meeting specific case or syndromic definitions or the isolated report from a clinician of a suspicious case). The node "other surveillance reports" includes the variety of bioterrorism surveillance data that could be collected by public health officials (e.g., from detection systems, pharmacy sales, veterinarians, zoos, clinical and microbiologic laboratory reports, ambulance/911 calls, hospital admissions and discharges, and school/work absenteeism). Surveillance decisions include selection of methods for determining the expected rate of each source of surveillance data, setting thresholds above which an outbreak will

be suggested (e.g., 2 standard deviations above the expected rate), and performing temporal and/or spatial analyses to determine when the threshold has been exceeded. These decisions are affected by the type of surveillance data and the computing and statistical resources available to the public health official.

If public health officials interpret surveillance reports as suggesting a possible bioterrorist event, they may then decide to initiate outbreak investigation. Decisions about initiating outbreak investigation will be affected by the type of information under surveillance (e.g., a few syndromic reports of patients presenting with fever and a rash might not be investigated but a report of a suspected case of smallpox would be), the methods used to calculate the expected rate of each type of data under surveillance, and the means by which thresholds are set to determine when outbreak investigation will be performed. If the investigation provides additional suggestion of an outbreak or exposure, public health officials will then have to determine the timing and scope of the appropriate outbreak control measures. Outbreak control measures include actions intended to prevent the spread of disease, such as quarantine, mass vaccination/antibiotic distribution, and requesting release of the National Pharmaceutical Stockpile. Decisions about the institution of outbreak control measures are based on the results of the outbreak investigations and interpretation of surveillance data. Decisions about whether and how to communicate the results of outbreak investigations to clinicians, first responders, other public health officials, the intelligence community, the media, and/or interested groups will also be based primarily on these results. The desired outcomes of this decision-making process could be lives saved, morbidity prevented, or dollars saved; it is affected by the population's infection status and by outbreak control measures.

In time period 3, clinicians are faced with subsequent cases (Figure 2). At this time, their estimation of the pretest probability of disease may be increased secondary to alerts from public health officials, thereby affecting subsequent testing, management, prevention, and reporting decisions. Similarly, after an outbreak has been established, public health officials' decisions about surveillance, outbreak investigation, outbreak control, and communication will be affected by the information that they receive from their public health colleagues.

The use of influence diagram notation facilitates the identification of the 8 key decisions and tasks that could be targets of DSSs designed to assist clinicians and public health officials responding to a bioterrorist attack. In addition, the schematic specifies 3 essential features of the decision-making process that could be the targets of IT/DSSs: the relationships between the decisions, the uncertain events that affect the decisions, and the information that is observable by the decision makers at the time they make their decisions. For example, IT/DSSs exist that use clinical information about a patient (e.g., temperature, peripheral white blood cell count, and chest radiograph findings) to suggest management alternatives (e.g., selection of antibiotics). From the schematic (Figure 2), it became apparent that for these systems to be maximally useful to clinicians, they should incorporate the results of diagnostic tests, provide recommendations in a timely manner (e.g., at the point of care), and be sufficiently flexible so that management algorithms and knowledge bases can be updated as the outbreak progresses.

Tasks of IT/DSS for Bioterrorism and Criteria for Evaluating Them

We used task decomposition to describe in detail the 8 top-level decisions and tasks and the associated subtasks that IT/DSSs would have to perform to assist clinicians and public health officials during a bioterrorism response. For each decision/task and associated subtasks, we considered the data requirements for an IT/DSS to assist in that subtask. This list of the necessary subtasks serves as the foundation of our evaluation system of the currently available IT/DSSs.

In Table 1, we present for each task examples of subtasks, information needs of the decision makers to perform that subtask, evaluation criteria, and IT/DSSs that could be used to perform that task. For example, interpretation of diagnostic tests is an important subtask of diagnostic decision making. To accurately interpret diagnostic test results, clinicians require information to determine the pretest probability of disease (e.g., history of exposure, signs, and symptoms), the diagnostic test results, and an understanding of the accuracy of the diagnostic test. Therefore, an evaluation criterion we applied to reports of diagnostic IT/DSSs for bioterrorism asked whether the reports described the systems' sensitivity and specificity.

In Table 2, we present the evaluation criteria for reports of IT/DSSs supporting a bioterrorism response. Several evaluation criteria for reports of IT/DSSs are relevant to all types of systems (e.g., the clear statement of the purpose of the system, descriptions of the system's hardware requirements, security measures, timeliness features, and costs of implementation and maintenance). Because of similarities in the design and functionality of some types of systems (e.g., reporting

Table 1 Key Decisions and Tasks with Examples from Task Decomposition of Subtasks, Information Needs, and Evaluation Criteria for Reports of Information Technologies and Decision Support Systems for Bioterrorism Preparedness and Response

Decisions/Tasks	Example Subtask	Example Information Need	Example Evaluation Criterion[a]	Example System
Diagnosis	Interpretation of diagnostic test results	Information about the pretest probability of disease given exposure history, patient's signs and symptoms, and diagnostic test results	Are sensitivity and specificity reported?	QMR[b]
Management	Treatment of acutely ill patients	Information regarding appropriate antibiotics and other therapies for suspected cases of bioterrorism-related illness	Is the inclusion of all bioterrorism-relevant agents and associated illnesses in the system's knowledge base described?	HELP[c]
Prevention	Prophylaxis of asymptomatic exposed persons	Information regarding the criteria for and effectiveness of prophylactic measures such as antibiotics, immune globulin, and vaccines	Is the ability to change recommendations as the epidemic progresses described?	Gideon[d]
Reporting	Clinicians' communication of information about suspicious cases to public health officials	Information regarding which diseases should be reported and how to perform such reporting	Is the timeliness of the system described?	GeoSentinel[e]
Surveillance	Analysis of surveillance data	Baseline information for each source of surveillance data including means and standard deviations over time accounting for seasonal and geographic variations	Are the methods used to determine baseline characteristics of surveillance data described?	ESSENCE[f]
Outbreak investigation	Verification that the cases identified from the surveillance data represent an outbreak	Information about the sensitivity and specificity of surveillance data on which the outbreak investigation is being based	Are sensitivity and specificity of the surveillance system reported?	CDC Wonder/PC[g]
Outbreak control	Institution of quarantine	Information regarding the criteria for and effectiveness of various quarantine and isolation procedures (e.g., mandates for a population to stay at home v. isolating patients in a designated facility)	Is the ability to change recommendations as the epidemic progresses described?	None found
Communication	Communication among national, state, and local public health officials	Information about ongoing outbreaks of naturally occurring or bioterrorism-related illnesses	Is the mode of transmission of information to the recipient described (e.g., email or pager alerts)?	RHEACTS[h]

a. These evaluation criteria focus on the information that should be collected regarding system performance from a report of a system but do not specify standards for each criterion (e.g., do not identify critical thresholds in sensitivity and specificity that individual systems must achieve to be useful during a bioterrorism response).

b. Quick Medical Reference (QMR) is a widely distributed general diagnostic decision support system (DSS) that uses rule-based logic to associate manually entered case findings with its knowledge base of more than 600 diseases.[63–75]

c. Health Evaluation through Logical Processing (HELP) was developed at LDS Hospital in Salt Lake City and applies clinical practice guidelines to the hospital's robust electronic medical record system to provide patient-specific recommendations to clinicians at the point of care.[76–82]

d. Global Infectious Disease and Epidemiology Network (Gideon) is a diagnostic DSS that provides a differential diagnoses of infectious diseases based on manually entered clinical information compared to its robust knowledge base of infectious diseases that includes all of the most bioterrorism-relevant agents.[90]

e. Global Emerging Infections Sentinel Network (GeoSentinel) monitors morbidity among international travelers through the receipt and analysis of faxed reports from 25 sentinel clinics worldwide.[91,92]

f. Electronic Surveillance System for the Early Notification of Community-based Epidemics (ESSENCE) was initially designed to perform syndromic surveillance using routinely collected outpatient diagnosis codes from military clinics in the Washington, D.C., area but has been expanded to include both military and civilian data sources from around the world.[86]

g. CDC Wonder/PC is an integrated information and communication service that allows users to search and download public health information from the Centers for Disease and Prevention (CDC) and facilitates communication among public health officials.[87–89]

h. Rapid Health Electronic Alert, Communication, and Training System (RHEACTS) provides a Web portal for alert notification, knowledge sharing, and training with security that is largely derived from a role-based identification system.[83–85]

Table 2 Evaluation Criteria for Reports of Information Technologies and Decision Support Systems (IT/DSSs) Supporting a Bioterrorism Response

Decision Being Supported	Evaluation Criteria for Reports of IT/DSSs Supporting a Bioterrorism Response[a]
Diagnosis	Is the purpose of the system stated?
	Are the hardware requirements described?
	Is the type of information required by the system described?
	Is the type of diagnostic information provided by the system described (e.g., a list of possible diagnoses)?
	Are sensitivity and specificity reported?
	Is the reference standard against which the system was compared described?
	Is the inclusion of all bioterrorism-relevant agents and associated illnesses in the system's knowledge base described?
	Is the ability to update the pretest probability of biothreat-related illness described?
	Is the method of reasoning used by inference engine described?
	Is the use of standard vocabulary described?
	Is the timeliness of diagnostic information described (e.g., information provided at the point of care)?
	Are the system's security measures described?
	Are the system's costs described?
Management and prevention	Is the purpose of the system stated?
	Are the hardware requirements described?
	Is the type of information required by the system described (e.g., data from the electronic medical record)?
	Is the manner in which recommendations are provided described?
	Is the accuracy of recommendations described?
	Is the inclusion of all bioterrorism-relevant agents and associated illnesses in the system's knowledge base described?
	Is the ability to change recommendations as the epidemic progresses described?
	Is the method of reasoning used by inference engine described?
	Is the use of standard vocabulary described?
	Is the timeliness of the recommendations described (e.g., information provided at the point of care)?
	Are the system's security measures described?
	Are the system's costs described?
Reporting and communication	Is the purpose of the system stated?
	Are the hardware requirements described?
	Is the information that the system is intended to communicate described?
	Are the intended provider(s) and recipient(s) of information described?
	Is the mode of transmission of information to recipient described (e.g., e-mail or pager alerts)?
	Is the timeliness of the system described?
	Are the system's security measures described?
	Are the system's costs described?
Surveillance	Is the purpose of the system stated?
	Are the hardware requirements described?
	Is the type of surveillance data collected by the system described?
	Are the methods used to collect surveillance data described?
	Is the geographic area under surveillance described?
	Is the acceptability of the system by data collectors described (i.e., their willing to use the system)?
	Are the methods used to determine baseline characteristics of surveillance data described (e.g., the expected rate of cases under surveillance on a given day in a particular geographic location)?
	Are the methods to perform analyses of data described (e.g., temporal-spatial)?
	Are the methods for determining when an outbreak has occurred described (e.g., setting thresholds)?
	Are the methods of presenting data to a decision maker described?

(continued)

Table 2 (continued)

Decision Being Supported	Evaluation Criteria for Reports of IT/DSSs Supporting a Bioterrorism Response[a]
	Is the flexibility of the system to change data collected and methods of analysis as the epidemic progresses described?
	Are sensitivity and specificity of the system reported?
	Is the reference standard against which the system was compared described?
	Is the timeliness of the system described?
	Are the system's security measures described?
	Are the system's costs described?
Outbreak investigation and control	Is the purpose of the system stated?
	Are the hardware requirements described?
	Are the types of actions recommended by the system described?
	Is the acceptability of the system by public health responders and data collectors described (i.e., their willing to use the system)?
	Is the ability to change information about available response resources (e.g., hospital beds and personnel) and relevant outbreak control recommendations described?
	Are sensitivity and specificity of the system reported?
	Is the timeliness of the system described?
	Are the system's security measures described?
	Are the system's costs described?

a. These evaluation criteria focus on the information that should be collected regarding system performance from a report of a system but do not specify standards for each criterion (e.g., do not identify critical thresholds in sensitivity and specificity that individual systems must achieve to be useful during a bioterrorism response).

and communication), we found that a single set of evaluation criteria could be used for both.

Diagnostic systems. The key evaluation criteria for diagnostic DSSs are the determination that all bioterrorism-relevant agents are included in the system's knowledge base, diagnostic sensitivity and specificity, timeliness, which is affected by the type of information required by the system (e.g., manually entered clinical information), and whether the recommendations are provided at the point of care. For example, Quick Medical Reference (QMR) is a widely distributed general diagnostic DSS that uses rule-based logic to associate patients' signs and symptoms with its knowledge base of more than 600 diseases.[63–75] The diagnostic accuracy of QMR compares favorably to that of other general diagnostic decision support systems and to physician experts; however (as is the case with all general diagnostic DSSs included in the systematic review), it has never been evaluated specifically for bioterrorism-related illness, we could not verify that all the bioterrorism-relevant agents were in its knowledge base, and its requirement for the manual entry of case findings would limit its timeliness. For a complete evaluation of the reports of QMR, we refer interested readers elsewhere.[11]

Management and prevention systems. Important evaluation criteria for IT/DSSs designed to support management and prevention subtasks include the determination that all bioterrorism-relevant agents are included in the system's knowledge base and that recommendations are accurate, timely, and can be updated as the outbreak proceeds. The management DSS that has been the topic of the most numerous clinical evaluations is the Health Evaluation through Logical Processing (HELP) system developed at LDS Hospital in Salt Lake City.[76–82] The HELP system, based on a robust electronic medical record, has numerous features with potential relevance to supporting clinicians' decision making during a bioterrorism response including implementing clinical practice guidelines for the diagnosis and management of community-acquired pneumonia, providing clinicians with alerts about specific laboratory and radiographic findings (including alerts for infections that are legally mandated to be reported to public health officials), and providing patient-specific antibiotic recommendations at the point

of care.[76–82] As with the general diagnostic DSSs, neither HELP nor any of the other management or prevention systems have been evaluated specifically for their ability to provide accurate, timely recommendations during a bioterrorism response, and we have no information as to whether the knowledge bases and inference engines of these systems include comprehensive information about bioterrorism-related illnesses. However, HELP has maximized timeliness of recommendations because its algorithms and alerts are generated continuously as the electronic medical record is updated. In addition, HELP's algorithms could be changed as an outbreak progresses.[11]

Reporting and communications systems. The key evaluation criteria for IT/DSSs for reporting and communication are that they are flexible (e.g., can update information/features as the epidemic progresses), timely, secure (e.g., provide for the confidentiality of patient information and the security of the data), and passive on the part of the data recipient (e.g., decision makers are automatically notified via page or e-mail of critical information rather than having to seek it out from a Web site or other source). Communication systems differ enormously in terms of their complexity, the type of information that they are designed to transmit, and the intended recipients of the information. Among the simplest and most widely used technologies for clinicians are alerting systems that automatically issue a page in the event that a patient has an abnormal laboratory result. For public health officials, there are systems such as the Rapid Health Electronic Alert, Communication, and Training System (RHEACTS) that have been designed to facilitate communication among local and state and federal public health decision makers. RHEACTS is a California initiative to provide a Web portal for alert notification, knowledge sharing, and training of public health officials with security that is largely derived from a role-based identification system.[83–85] It is likely that the usefulness of systems such as RHEACTS during a bioterrorism response may be limited unless their availability to more local public health officials and their use for routine public health communication increases.

Surveillance systems. Evaluations of bioterrorism surveillance systems require an understanding of the sensitivity, specificity, timeliness, and cost of collection of each source of surveillance data. In addition, evaluation necessitates an understanding of the methods used to determine when an outbreak has occurred. The earliest signs and symptoms caused by most biothreat agents are influenza-like illness, acute respiratory distress, febrile hemorrhagic syndromes, and febrile illness with dermatologic, neuorologic, or gastrointestinal symptoms. Therefore, patients with these syndromes are the targets of bioterrorism-related syndromic surveillance. These syndromic surveillance systems vary widely with respect to the syndromes under surveillance, data collected, methods of data analysis, and presentation to public health decision makers. One of the most extensive syndromic surveillance systems, the Electronic Surveillance System for the Early Notification of Community-based Epidemics (ESSENCE), was initially designed to perform syndromic surveillance using routinely collected outpatient diagnosis codes from military clinics in the Washington, D.C., area but has been expanded to include both military and civilian data sources from around the world.[86] More than 2700 syndrome- and location-specific graphs are prepared each day and automatically analyzed for patterns that suggest the need for outbreak investigation. Two evaluations of ESSENCE are currently ongoing: one to address data quality and the other to test the system's sensitivity and specificity over a range of outbreak scenarios.[86]

Outbreak investigation and control systems. The key evaluation criteria for an IT/DSS that facilitates outbreak investigation and control are that it is sensitive, specific, and acceptable to public health users (i.e., a system with a high false positive rate that alarms frequently and requires public health officials to investigate nonevents is not likely to be relied on during an actual bioterrorism event); matches the type of recommendation to the type of aberration detected in the surveillance data (e.g., a peak in acute respiratory distress cases might result in a call to the local hospital to determine the nature of the cases whereas a spike in sputum cultures growing *B. anthracis* might warrant a more intensive alarm and investigation); and has the flexibility to change recommendations as the outbreak progresses. Most of the IT/DSSs to facilitate outbreak investigation are communication systems that enhance communication among public health officials about suspected outbreaks in specific geographic areas or alert public health officials to peaks in surveillance data but do not actually provide decision support. For example, the Centers for Disease Control and Prevention's (CDC's) Wonder/PC is an integrated information and communication service that allows users to search and download public health information from the CDC and facilitates communication among public health officials.[87–89]

DISCUSSION

We developed a conceptual framework for the evaluation of IT/DSSs for bioterrorism preparedness and response based on formal approaches to identify the key decisions and tasks that clinicians and public health officials are likely to face while responding to bioterrorism. Clinicians must make decisions related to diagnosis and detection, management, prevention of further exposure or the spread of disease, and communication with public health officials. Public health officials must make decisions about surveillance, outbreak investigations, outbreak control measures, and communication with clinicians, other public health officials, and the public. Although clinicians and public health officials must make some decisions not captured in this general conceptual model, we specified the major decision areas affecting the important outcomes of lives saved and morbidity prevented.

Our conceptual framework addresses 3 limitations in the existing evaluation methods that could be applied to IT/DSSs for bioterrorism preparedness and response. First, the general methods for evaluating IT/DSSs assume a detailed knowledge of the information needs of users; however, an assessment of the information needs of clinicians and public health officials preparing for and responding to bioterrorism events has not previously been published. Thus, our use of task decomposition to systematically abstract the key tasks and information needs of these decision makers from responses to naturally occurring and bioterrorism-related outbreaks and other relevant literatures represents a significant contribution to efforts to develop bioterrorism-specific IT/DSSs and to evaluate them.

Second, none of the existing evaluation frameworks consider the effects of the IT/DSS on the relationships between multiple decision makers over time. Our conceptual framework used influence diagram notation to explore the relationships between the key decisions of clinicians and public health officials responding to bioterrorism—a method not typically part of the standard task decomposition approach. The advantages of using influence diagram notation to represent the complex and related decisions of clinicians and public health officials were that it facilitated the description of the uncertain events affecting the key decisions, highlighted the relationships between decisions made by different decision makers, and emphasized the critical steps in the decision-making process that could be influenced by IT/DSSs. The schematic presented in Figure 2 could be easily expanded to include additional decisions made by these 2 types of decision makers (e.g., to further delineate the tasks of emergency department clinicians from those of general practitioners or to describe the different tasks of local, state, and national public health officials), to add other decision makers (e.g., laboratory personnel, first responders, and hospital administrators), and to include more detail about specific diagnostic test characteristics, clinical syndromes, and the other key uncertainties (thereby evaluating the significance of these uncertainties on the decisions they affect).

Third, the published evaluation guidelines for diagnostic tests, information systems, and surveillance systems typically present broad system specifications or criteria without detailed information about how to apply these criteria to published evaluations of systems or tailor these criteria for a particular type of system.[26,56,57,60,61] Our use of task decomposition provided a formal method for developing the evaluation criteria specifically for bioterrorism response systems, which we then reviewed and augmented with advice from experts in bioterrorism preparedness and response. Having written the criteria in the form of a question facilitated our application of these criteria to the literature describing existing IT/DSSs. Despite the heterogeneity of the tasks and subtasks, common themes emerged in the criteria for most types of IT/DSSs: Evaluations require information about the system's timeliness, sensitivity, specificity, acceptability, flexibility, and security of the data collected. These could be considered the key evaluation criteria.

We found that most of the 217 IT/DSSs were designed for other uses and only subsequently adapted to facilitate a bioterrorism response. However, the timeliness needed for other purposes is often less stringent than that required for bioterrorism detection or response. We found that those systems designed primarily for nonbioterrorism purposes were most likely to be adaptable for bioterrorism preparedness or response if they were designed to be highly timely for their original purpose and could be modified for a bioterrorism response task. For example, rapid diagnostic tools for non-bioterrorism-related pathogens could be modified to detect biothreat agents. Other systems could be adapted for a bioterrorism response by making them more timely. For example, an influenza surveillance system that collected clinical data on a weekly basis could be changed to daily reporting of cases of influenza-like illness. In addition to this enhanced timeliness, systems designed for both delivery of routine health care and use during a bioterrorism response ("dual-use systems") may be more cost-effective or more acceptable to users than bioterrorism-only systems. We found that decision support was most effective when integrated into the normal flow of patient

care through clinical information systems[11]; however, we found no specific evidence linking multiple existing IT/DSSs (such as linking diagnostic systems with electronic medical records or using surveillance information to update pretest probabilities of disease when interpreting diagnostic information).

When applying the evaluation criteria to 217 currently available IT/DSSs that could potentially support the decisions of clinicians and public health officials, we found that the literature provides little information about the accuracy of these systems. As a group, the diagnostic DSSs have been subjected to the most comprehensive assessment of both sensitivity and specificity. In contrast, very little published data report the sensitivity and/or specificity of surveillance data or methods for analyzing them. Ongoing evaluations of these characteristics of syndromic surveillance systems will significantly improve the ability of public health decision makers to determine the meaning of a peak in the surveillance data. The sensitivity and specificity of the surveillance system is affected by the methods used to analyze the data. We found few reports describing the ability of a system to incorporate more than 1 source of surveillance data or to routinely perform temporal and spatial analyses.

Almost none of the reports of systems included in the systematic review provided a comprehensive description of its security measures. From our task decomposition and discussion with experts in bioterrorism preparedness, we determined that IT/DSSs for bioterrorism preparedness and response require measures to maintain patient confidentiality (e.g., typically by role-delimited access to patient information in a manner compliant with the Health Insurance Portability and Accountability Act of 1996), to resist cyber attack, and to maintain the security of clinical and laboratory specimens.

The conceptual framework described and then applied to more than 200 IT/DSSs focuses on decisions by clinicians and public health officials that are likely to be critical for preventing excess morbidity and mortality during a bioterrorism event. Our application of the evaluation provides insight into the elements of IT/DSSs that require additional evaluation to determine whether they will meet the complex information needs of decision makers involved in an effective bioterrorism response. Public health decision makers are currently making critical decisions regarding investments in systems for bioterrorism preparedness and response. Evaluations of existing systems and those under development according to the criteria described would significantly enhance their understanding of the likely costs and benefits of these systems for clinical and public health decision making.

REFERENCES

1. Jernigan JA, Stephens DS, Ashford DA, et al. Bioterrorism-related inhalational anthrax: the first 10 cases reported in the United States. Emerg Infect Dis. 2001;7:933–44.
2. Update: investigation of bioterrorism-related inhalational anthrax—Connecticut, 2001. MMWR Morb Mortal Wkly Rep. 2001;50:1049–51.
3. Update: investigation of bioterrorism-related anthrax and interim guidelines for clinical evaluation of persons with possible anthrax. MMWR Morb Mortal Wkly Rep. 2001;50:941–8.
4. Update: investigation of bioterrorism-related anthrax and interim guidelines for exposure management and antimicrobial therapy, October 2001. MMWR Morb Mortal Wkly Rep. 2001;50:909–19.
5. Recognition of illness associated with the intentional release of a biologic agent. MMWR Morb Mortal Wkly Rep. 2001;50:893–7.
6. Update: investigation of anthrax associated with intentional exposure and interim public health guidelines, October 2001. MMWR Morb Mortal Wkly Rep. 2001;50:889–93.
7. Becker C. 20/20 hindsight: months after anthrax claimed the lives of several Americans, hospitals review their reaction to the event—and plan for future crises. Mod Healthc. 2002;32:8–9, 12.
8. Borio L, Frank D, Mani V, et al. Death due to bioterrorism-related inhalational anthrax: report of 2 patients. JAMA. 2001;286:2554–9.
9. Josefson D. Toll of anthrax cases reaches 15. BMJ. 2001;323:1022.
10. Mayer TA, Bersoff-Matcha S, Murphy C, et al. Clinical presentation of inhalational anthrax following bioterrorism exposure: report of 2 surviving patients. JAMA. 2001;286:2549–53.
11. Bravata DM, McDonald K, Owens DK, et al. Bioterrorism Preparedness and Response: Use of Information Technologies and Decision Support Systems (Evidence Report/Technology Assessment No. 59). Rockville (MD): Prepared by the UCSF-Stanford Evidence-Based Practice Center under contract No. 290-97-0013 for the Agency for Healthcare Research and Quality; June 2002.
12. Anderson JG, Aydin CE, Jay SJ, eds. Evaluating Health Care Information Systems: Methods and Applications. Thousand Oaks (CA): Sage; 1994.
13. Friedman CP, Wyatt JC. Evaluation Methods in Medical Informatics. New York: Springer-Verlag; 1997.
14. Owens DK, Bravata DM. Computer-based decision support: wishing on a star? Eff Clin Pract. 2001;4:34–8.
15. Kaplan B. Evaluating informatics applications—clinical decision support systems literature review. Int J Med Inf. 2001;64:15–37.
16. Ammenwerth E, Graber S, Herrmann G, Burkle T, Konig J. Evaluation of health information systems—problems and challenges. Int J Med Inf. 2003;71:125–35.
17. Goldratt EM. Theory of Constraints. Great Barrington (MA): North River Press; 1990.
18. Hunink MGM. In search of tools to aid logical thinking and communicating about medical decision making. Med Decis Making. 2001;21:267–77.
19. Friedman CP, Owens DK, Wyatt JC. Evaluation and technology assessment. In: Shortliffe EH, Perreault LE, Wiederhold G, Fagan LM, eds. Medical Informatics: Computer Applications in Health Care and Biomedicine. New York: Springer-Verlag; 2000.
20. Donabedian A. Exporations in Quality Assessment and Monitoring. Volume 2. Ann Arbor (MI): Health Administration Press; 1982.
21. Donabedian A. The quality of care: how can it be assessed? JAMA. 1988;260:1743–8.

22. Sim I, Owens DK, Lavori PW, Rennels GD. Electronic trial banks: a complementary method for reporting randomized trials. Med Decis Making. 2000;20:440–50.
23. Nease RF Jr, Owens DK. Use of influence diagrams to structure medical decisions. Med Decis Making. 1997;17:263–75.
24. Owens DK, Shachter RD, Nease RF. Representation and analysis of medical decision problems with influence diagrams. Med Decis Making. 1997;17:241–62.
25. Callan K. Preparing for a decision support system. Top Health Inf Manage. 2000;21:84–90.
26. Shortliffe EH. Computer programs to support clinical decision making. JAMA. 1987;258:61–6.
27. Inglesby T, Grossman R, O'Toole T. A Plague on Your City: Observations from TOPOFF. Center for Civilian Biodefense Studies, Johns Hopkins University. Available from: http://www.hopkins-biodefense.org/pages/news/quarter.html#Anchor-8398. Accessed 20 December 2000.
28. Hoffman RE, Norton JE. Lessons learned from a full-scale bioterrorism exercise. Emerg Infect Dis. 2000;6:652–3.
29. Dark Winter. Johns Hopkins Center for Civilian Biodefense, Center for Strategic and International Studies, ANSER, and Memorial Institute for the Prevention of Terrorism. Available from: http://www.hopkins-biodefense.org/participants.html. Accessed 8 November 2001.
30. MacKenzie WR, Schell WL, Blair KA, et al. Massive outbreak of waterborne cryptosporidium infection in Milwaukee, Wisconsin: recurrence of illness and risk of secondary transmission. Clin Infect Dis. 1995;21:57–62.
31. Outbreak of West Nile-like viral encephalitis—New York, 1999. MMWR Morb Mortal Wkly Rep. 1999;48):845–9.
32. Dennis DT, Inglesby TV, Henderson DA, et al. Tularemia as a biological weapon: medical and public health management. JAMA. 2001;285:2763–73.
33. Arnon SS, Schechter R, Inglesby TV, et al. Botulinum toxin as a biological weapon: medical and public health management. JAMA. 2001;285:1059–70.
34. Inglesby TV, Dennis DT, Henderson DA, et al. Plague as a biological weapon: medical and public health management. JAMA. 2000;283:2281–90.
35. Henderson DA, Inglesby TV, Bartlett JG, et al. Smallpox as a biological weapon: medical and public health management. JAMA. 1999;281:2127–37.
36. Inglesby TV, Henderson DA, Bartlett JG, et al. Anthrax as a biological weapon: medical and public health management. JAMA. 1999;281:1735–45.
37. Bioterrorism readiness plan—a template for healthcare facilities. Association for Professionals in Infection Control and Epidemiology Inc. and Centers for Disease Control and Prevention. ED Manag. 1999;11 Suppl:1–16.
38. Proceedings of the National Symposium on Medical and Public Health Response to Bioterrorism. Arlington, Virginia, USA. February 16-17, 1999. Emerg Infect Dis. 1999;5:491–592.
39. Smithson AE, Levy L. Ataxia: The Chemical and Biological Terrorism Threat and the U.S. Response. Washington (DC): Henry L. Stimson Center; 1999.
40. ReddiNet information binder. Los Angeles (CA): Healthcare Association of Southern California; 2001.
41. Centers for Disease Control and Prevention. Health Level Seven Specifications for Electronic Laboratory-Based Reporting of Public Health Information. Atlanta (GA): Centers for Disease Control and Prevention; 1997.
42. Electronic reporting of laboratory information for public health. Paper presented at the Conference on Electronic Reporting of Laboratory Information for Public Health, Centers for Disease Control and Prevention; 7-8 January 1999.
43. US Department of Health and Human Services. Public Health Conceptual Data Model. Atlanta (GA): US Department of Health and Human Services, Public Health Service; 2000.
44. Centers for Disease Control and Prevention. Secure Data Network Standards And Procedures. Atlanta (GA): Centers for Disease Control and Prevention, Agency for Toxic Substances and Disease Registry; 1999.
45. Owens DK, Nease RF. A normative analytic framework for development of practice guidelines for specific clinical populations. Med Decis Making. 1997;17:409–26.
46. Owens DK, Nease RF. Development of outcome-based practice guidelines: a method for structuring problems and synthesizing evidence. Jt Comm J Qual Improv. 1993;19:248–63.
47. Xiang Y, Poh KL. Time-critical dynamic decision modeling in medicine. Comput Biol Med. 2002;32:85–97.
48. Aliferis CF, Cooper GF, Pollack ME, Buchanan BG, Wagner MM. Representing and developing temporally abstracted knowledge as a means towards facilitating time modeling in medical decision-support systems. Comput Biol Med. 1997;27:411–34.
49. Hazen GB. Stochastic trees and the StoTree modeling environment: models and software for medical decision analysis. J Med Syst. 2002;26:399–413.
50. Hazen GB. Factored stochastic trees: a tool for solving complex temporal medical decision models. Med Decis Making. 1993;13:227–36.
51. Hazen GB. Stochastic trees: a new technique for temporal medical decision modeling. Med Decis Making. 1992;12:163–78.
52. Magni P, Quaglini S, Marchetti M, Barosi G. Deciding when to intervene: a Markov decision process approach. Int J Med Inf. 2000;60:237–53.
53. Sim I, Owens D, Lavori P, Rennels G. Electronic trial banks: a complementary method for reporting randomized trials. Med Decis Making. 2000;20:440–50.
54. Chandrasekaran B, Johnson T. Generic tasks and task structure: history, critique and new directions. In: David J, Krivine J, Simmons R, eds. Second-Generation Expert Systems. New York: Springer-Verlag; 1993. p 232–72.
55. Gruninger M, Fox M. Methodology for the design and evaluation of ontologies. Toronto (Canada): Department of Industrial Engineering; 1995.
56. Guidelines for evaluating surveillance systems. MMWR Morb Mortal Wkly Rep. 1988;37 Suppl 5:1–18.
57. Hunt DL, Haynes RB, Hanna SE, Smith K. Effects of computer-based clinical decision support systems on physician performance and patient outcomes: a systematic review. JAMA. 1998; 280:1339–46.
58. Johnston ME, Langton KB, Haynes RB, Mathieu A. Effects of computer-based clinical decision support systems on clinician performance and patient outcome: a critical appraisal of research. Ann Intern Med. 1994;120:135–42.
59. Hornberger J, Goldstein MK. Clinical decision-support systems: evaluating the evaluation. Med Decis Making. 2000;20:130–1.
60. Sox HC, Blatt MA, Higgins MC, Marton KI. Medical Decision Making. Boston: Butterworth-Heinemann; 1988.
61. Adlassnig KP, Scheithauer W. Performance evaluation of medical expert systems using ROC curves. Comput Biomed Res. 1989; 22:297–313.
62. Sosin DM. Draft framework for evaluating syndromic surveillance systems. J Urban Health. 2003;80 Suppl 1:I8–I13.
63. Berner ES, Webster GD, Shugerman AA, et al. Performance of four computer-based diagnostic systems. N Engl J Med. 1994;330: 1792–6.
64. Bankowitz RA, Blumenfeld BH, Giuse BN. User variability in abstracting and entering printed case histories with Quick Medical Ref-

erence (QMR). Proceedings of the Annual Symposium on Computer Applications in Medical Care; 1987. p 68–73.
65. Bankowitz RA, Miller JK, Janosky J. A prospective analysis of inter-rater agreement between a physician and a physician's assistant in selecting QMR vocabulary terms. Proceedings of the Annual Symposium on Computer Applications in Medical Care; 1991. p 609–13.
66. Lemaire JB, Schaefer JP, Martin LA, Faris P, Ainslie MD, Hull RD. Effectiveness of the Quick Medical Reference as a diagnostic tool. CMAJ. 1999;161:725–8.
67. Bankowitz RA, McNeil MA, Challinor SM, Parker RC, Kapoor WN, Miller RA. A computer-assisted medical diagnostic consultation service. Implementation and prospective evaluation of a prototype. Ann Intern Med. 1989;110:824–32.
68. Bankowitz RA, McNeil MA, Challinor SM, Miller RA. Effect of a computer-assisted general medicine diagnostic consultation service on housestaff diagnostic strategy. Methods Inf Med. 1989;28:352–6.
69. Arene I, Ahmed W, Fox M, Barr CE, Fisher K. Evaluation of quick medical reference (QMR) as a teaching tool. MD Comput. 1998; 15:323–6.
70. Miller RA, McNeil MA, Challinor SM, Masarie FE Jr, Myers JD. The INTERNIST-1/Quick Medical Reference project—status report. West J Med. 1986;145:816–22.
71. Miller R, Masarie FE, Myers JD. Quick medical reference (QMR) for diagnostic assistance. MD Comput. 1986;3:34–48.
72. Bacchus CM, Quiston C, O'Rourke K, Detsky AS. A randomized crossover trial of QMR as a teaching tool for medical interns. J Gen Intern Med. 1994;9:616–21.
73. Berner ES, Maisiak RS. Influence of case and physician characteristics on perceptions of decision support systems. J Am Med Inform Assoc. 1999;6:428–34.
74. Berner ES, Maisiak RS, Cobbs CG, Taunton OD. Effects of a decision support system on physicians' diagnostic performance. J Am Med Inform Assoc. 1999;6:420–7.
75. Quick Medical Reference. First DataBank. Available from: http://www.firstdatabank.com. Accessed 14 November 2001.
76. Fiszman M, Haug PJ. Using medical language processing to support real-time evaluation of pneumonia guidelines. Proceedings of the AMIA Annual Symposium. 2000;27:235–9.
77. Aronsky D, Haug PJ. An integrated decision support system for diagnosing and managing patients with community-acquired pneumonia. Proceedings of the AMIA Annual Symposium; 1999. p 197–201.
78. Evans RS, Larsen RA, Burke JP, et al. Computer surveillance of hospital-acquired infections and antibiotic use. JAMA. 1986;256: 1007–11.
79. Evans RS, Classen DC, Pestotnik SL, Lundsgaarde HP, Burke JP. Improving empiric antibiotic selection using computer decision support. Arch Intern Med. 1994;154:878–84.
80. Evans RS, Pestotnik SL, Classen DC, et al. A computer-assisted management program for antibiotics and other antiinfective agents. N Engl J Med. 1998;338:232–8.
81. Pestotnik SL, Evans RS, Burke JP, Gardner RM, Classen DC. Therapeutic antibiotic monitoring: surveillance using a computerized expert system. Am J Med. 1990;88:43–8.
82. Pestotnik SL, Classen DC, Evans RS, Burke JP. Implementing antibiotic practice guidelines through computer-assisted decision support: clinical and financial outcomes. Ann Intern Med. 1996; 124:884–90.
83. Hall B. Director, Rapid Health Electronic Alert, Communications, and Training System (RHEACTS). In: Bravata DM, McDonald K, Owens DK, et al. Bioterrorism Preparedness and Response: Use of Information Technologies and Decision Support Systems (Evidence Report/Technology AssessmentNo. 59). Rockville (MD): Prepared by the UCSF-Stanford Evidence-Based Practice Center under contract No. 290-97-0013 for the Agency for Healthcare Research and Quality; June 2002.
84. Ascher MS. In: Bravata DM, McDonald K, Owens DK, et al. Bioterrorism Preparedness and Response: Use of Information Technologies and Decision Support Systems (Evidence Report/Technology AssessmentNo. 59). Rockville (MD): Prepared by the UCSF-Stanford Evidence-Based Practice Center under contract No. 290-97-0013 for the Agency for Healthcare Research and Quality; June 2002.
85. California State Senate Committee on Health and Human Services. Bioterrorism and public health: assessing California's preparedness: background. Available from: http://www.sen. ca.gov/ftp/SEN/COMMITTEE/STANDING/HEALTH/_home/BIOTERRORISM_BACKGROUND.DOC. Accessed 13 February 2002.
86. Pavlin JA, Kelley PW. ESSENCE: Electronic Surveillance System for the Early Notification of Community-Based Epidemics. Silver Spring (MD): US Department of Defense, Global Emerging Infections Surveillance and Response System; 2001.
87. Centers for Disease Control and Prevention. WONDER Logon. Available from: http://wonder.cdc.gov/. Accessed 5 October 2001.
88. Friede A, Reid JA, Ory HW. CDC WONDER: a comprehensive online public health information system of the Centers for Disease Control and Prevention. Am J Public Health. 1993;83:1289–94.
89. Friede A, Rosen DH, Reid JA. CDC WONDER: a cooperative processing architecture for public health. J Am Med Inform Assoc. 1994;1:303–12.
90. Ross JJ, Shapiro DS. Evaluation of the computer program GIDEON (Global Infectious Disease and Epidemiology Network) for the diagnosis of fever in patients admitted to a medical service. Clin Infect Dis. 1998;26:766–7.
91. International Society of Travel Medicine. GeoSentinel: surveillance strategy. Available from: http://www.istm.org/geosentinel/surveill.html. Accessed 21 September 2001.
92. International Society of Travel Medicine. GeoSentinel: objectives. Available from: http://www.istm.org/geosentinel/objectiv.html. Accessed 21 September 2001.