Current outbreaks of anthrax exposure and cases test our health care delivery and public health systems with threats of large spatial scope—the entire nation—that demand a very short temporal latency in our responses. Other potential bioterrorist attacks only increase the dimensions of this unprecedented challenge. The dimensions, however, are not unprecedented; rather, they are quite familiar to many researchers in biomedical informatics over the last 40 years. The task of comprehensive real-time monitoring on the regional and national scale has been the subject of full-fledged design and large-scale implementations led by biomedical informaticians.

Nonetheless, we run the risk that the knowledge gained in the decades of informatics research will not, in the appropriate haste to safeguard the population of the United States from the threats of bioterrorism, be reflected in the national public health information infrastructure. And that may result not only in wasteful expenditures but also in ineffective measures to prevent future attacks on the health of the U.S. population. This is, therefore, a timely juncture to review some of the most germane contributions from the biomedical informatics armamentarium to the tasks at hand, particularly data acquisition, threat detection, and response.

**Data Acquisition**

Among the necessary requisites for a national monitoring infrastructure is a set of standardized vocabularies with which to describe the events of interest. The National Library of Medicine and other societies have already supported the construction of several important vocabularies and, furthermore, have created a framework—the Unified Medical Language System—to share descriptions across vocabularies and even link a new bioterrorism-monitoring vocabulary to other terminologies (such as the billing codes generated by most U.S. health care institutions). Furthermore, the development of a sound and sufficient terminology itself requires an understanding of the design choices implicit in pre-coordinated and post-coordinated vocabularies and the requirements entailed by cataloging vs. indexing of events.

Sharing reporting of clinical events across multiple institution requires a standardized means for describing the organization of that data; that is, a shared data model. Poorly designed data models lead to difficulty in deployment across institutions, errors in the collation of events, and problems in adapting the data model to new requirements and will not help prevent inconsistencies in the reports. In
the course of the last three decades, standardized models for describing clinical events in general and emergency department information in particular have been developed, and the general guidelines for a safe and efficient approach to such modeling has been articulated. Ignorance of such efforts is wasteful and risks rediscovery of all the mistakes already perpetrated by informaticians during the development of the discipline.

Electronic medical record systems are the specific hardware and software implementations through which primary care health care providers and hospital systems gather, store, and report clinical information. To do so, they have been engineered with user interfaces matched to clinical tasks and clinical workflow and built on top of very high availability systems with redundant and secure storage.

The particulars of clinical data entry have proved refractory to most naïve attempts to use interfaces borrowed simplistically from other application domains and have required judicious application of ethnography to the workflow and the mandates of safe and effective health care. The synergism between standardized clinical data models and electronic medical record systems has allowed informaticians to leverage the advent of a widely available networking infrastructure, the Internet, to rapidly implement large-scale multi-institutional clinical data gathering and integration.

An underused component of the public health system is the general population. Individuals at risk can provide the most rapid and comprehensive reporting of exposures, symptomatology, and compliance with and side effects of therapies, particularly when treated individuals number in the tens of thousands, as they do today. Biomedical informaticians have studied since the 1960s how best to enable patients to effectively communicate their symptoms and medical histories in their own terms and in a timely fashion.

In the Internet age, the study of consumer informatics has demonstrated that a wide swathe of our population can effectively use technologic means (developed by informaticians) to report a wide range of clinically relevant information. The application of these techniques with the same breadth and energy as those expended for far more mundane financial applications can help provide even earlier and more sensitive warnings than any solely institution-based activities.

Broad monitoring of health status and delivery presents well-described risks to the privacy of individuals, particularly when it involves regional or nationwide reporting. Consequently, biomedical informaticians have developed a range of technologic solutions like name matching that minimize disclosure while preserving the intended health service and health monitoring functionality.

**Threat Detection**

Once raw clinical data are acquired, the detection of signatures of bioterrorism requires sophisticated and prompt interpretation of monitored health care data across time and geography—this in the context of many diseases with early clinical presentations overlapping those of the bioterrorist infectious agents. The uncertainty associated with this overlap and the variation of the degree of the overlap require the probabilistic inference techniques developed by informaticians for distinguishing subtle signals or diseases from the background of events or findings of lesser import.

The costs of missing the detection of a bioterrorist incident are obviously great, as are the costs and risks of misdiagnosing and treating thousands of unaffected individuals. The interactions between the sensitivity and specificity of the detection algorithms and these various costs are of the same type that have been the subject of clinical decision support systems grounded in a formal decision-theoretic framework. Naïve bioterrorism detection implementations that have suboptimal specificity and sensitivity and that ride roughshod over the complex tradeoffs of competing utilities will result in surprising and unacceptable outcomes. Furthermore, the explicit nature of these decision models makes the implications of any detection strategy much clearer to the decision makers in our public health and law enforcement agencies.

**Response**

Even when the correct treatments, isolation methods, and testing protocols are known by experts, it is clear that, as in so many other clinical disciplines, the knowledge and implementation of the normative, prescribed responses to exposure and disease from bioterrorist attack are uneven at best. Clinicians throughout the country have only partial and often out-of-date knowledge of appropriate procedures. This is all the more problematic because of our rapidly changing understanding of what constitutes an effective (and an age- and health-status-specific) response to each of the infectious agents that could
potentially be used against our populations. To this end, the large complement of methodologies and implemented systems engineered by biomedical informaticians to effectively design guidelines, directly relevant to ensuring that all clinicians are able to deliver state-of-the-art diagnostic and treatments to potential and actual bioterrorist victims.

In summary, the challenges that bioterrorism brings to our health care system are not novel from the perspectives of the biomedical informatics research community. Swift and judicious deployments of the existing biomedical informatics tools and implementations will rapidly improve the readiness and responsiveness of our health care and public health system to acts of bioterrorism. Sustained development of the more advanced medical informatics techniques will result in our populations’ receiving the best possible and most timely protection.

References

32. Masys DR, Baker DB. Patient-centered Access to Secure Systems Online (PCASSO): a secure approach to clinical data access via