Medical Informatics and Preparedness

The terrorist attacks of September 2001 and the subsequent deliberate dissemination of anthrax have stimulated public awareness of the need in both the public health and clinical health care systems to quickly detect and respond to altered patterns of disease in communities across the nation. Debate over the capacity of the existing systems to fully respond to these demands has created a sense of urgency for immediate action to improve these functions. Public health resources were taxed to provide early detection and rapid response. The clinical care delivery system faced challenges of emergency response to urban casualties, highlighting the value of clinical information systems that facilitate information management in crisis situations.

The effective application of informatics to these data collection, analysis, and dissemination tasks could allow the rapid deployment of systems that would greatly enhance our preparedness. Much of the informatics experience gained in health information system implementation efforts over the past several decades is directly applicable to the new challenges of bioterrorism and emergency response. By utilizing this collective knowledge in areas such as architecture, infrastructure, standards, and knowledge representation, newly created systems are more likely to yield maximum benefits. As an organization, AMIA is already focused on issues of public health informatics, having developed a national consensus agenda for the field at its 2001 Spring Congress.1

The AMIA 2001 Annual Symposium provided an additional opportunity to bring together clinicians, medical informatics professionals, researchers, and policy makers in a concerted effort to document current informatics approaches that support rapid detection and response to crises. Key to the Association’s mission is a working group program that enables interested professionals who share a common clinical theme to advance the unique perspectives of their groups.

JAMIA is pleased to present a set of papers based on presentations and discussions at the Annual Symposium that can serve as an anchor in developing the informatics response to war, bioterrorism, and disaster. These papers provide a conceptual overview of the clinical and public health challenges and summaries of the ways in which biomedical informatics can support the health care system response to these challenges.

The special section begins with two reports of current activities. Teich et al.2 provide a summary of the special plenary session on the informatics response to bioterrorism, disaster, and war that was a last-minute addition to the AMIA meeting, including specific recommendations from the speakers. Lober et al.3 describe the design and preliminary results of six emerging community-based bioterrorism surveillance systems designed to provide enhanced early detection.

Next, two different perspectives on needed actions are presented. Kohane4 reviews the biomedical informatics literature relevant to bioterrorism data collection, detection, and response, suggesting that both policy makers and system developers should avail themselves of this extensive compendium of lessons learned over many years. Wagner5 invokes the term “biodefense” to describe the current needs and draws lessons from the early U.S. space program to advocate a vision for action in the creation of new informatics tools to address bioterrorism.

Finally, the special section concludes with an official policy statement from AMIA6 articulating a vision of the national health information infrastructure need-
ed to address emergent concerns using a scalable architecture that can also be applied to issues of broad-based health information management.

These papers form the "early call to action" for the medical informatics community. They identify needs and direction and highlight areas in which basic research and practical solutions are needed. In the coming months, *JAMIA* will publish additional papers that begin to build the basic biomedical informatics science and prototypical solutions needed to ensure that the health care system is able to manage emerging crises.

While the papers provide an apt starting point, it is important to identify topics and issues that still must be addressed. As a group, the papers identify actions needed and informatics support for institutions providing traditional health care. Full preparedness requires creative vision that will capitalize on how community- and home-level surveillance of symptoms and health problems will complement institutionally-based information systems.

Inherent in the massive collection of data for which many of the papers argue are the ever-present issues of confidentiality and security. Awaiting attention are thoughtful treatments of the trade-offs between personal privacy and public good that arise with mass surveillance systems. In addition, to ensure accurate interpretation of collected data, advances must be made in the development of decision logic and other mathematical and heuristic models that facilitate detection and avoid false alarms. Finally, large-scale, continuous surveillance approaches must of necessity address issues related to data storage, oversight protections to ensure proper use of data, and policy-level action to maintain the balance between private rights and public good.

Also, as we consider the issues related to bioterrorism, we must be cognizant of the more generic informatics problems related to the medical response to any large-scale disaster, whether due to natural events or to weapons of mass destruction. In such situations, existing medical records must be immediately available to emergency personnel, and information about care given must be captured to become part of the lifetime medical record of each individual treated. Facilitating the organization, management, and communication of emergency medical personnel is another important challenge that transcends the specific nature of the triggering event.

Finally, the energy, creativity, and resources devoted to creating informatics responses to bioterrorism will best serve society if the approaches are conducted in a manner that is mindful of the more mundane, but potentially more significant, health care problems and public health information needs that currently and continually face our society. Investments in surveillance, early detection, and rapid response systems must be complemented with and extended by attention to the needs of day-to-day management of health information to ensure the health of the public; effective, coordinated response to disease and injury; and efficient management of clinical and research information.

Much more remains to be done to ensure that we are fully prepared for possible future terrorism events. It is hoped that the information in this special section will both contribute to the ultimate solutions and highlight the key role of informatics in improving public health and health care in response to the current crisis.—PATRICIA FLATLEY BRENNAN, RN, PhD, WILLIAM A. YASNOFF, MD, PhD

References


Affiliations of the authors: University of Wisconsin–Madison, Madison, Wisconsin (PFB); Centers for Disease Control and Prevention, Atlanta, Georgia (WAY).

Correspondence and reprints: William Yasnoff, MD, PhD, Associate Director for Science, Public Health Practice Program Office, Centers for Disease Control and Prevention, 4770 Buford Highway NE, MS K36, Atlanta, GA 30341-3724; e-mail: <wyasnoff@cdc.gov>

Received for publication: 11/19/01; accepted for publication: 11/21/01.