Chapter XXXIX
Bioterrorism Response and IT Strategies

David A. Bray
Emory University, Goizueta Business School, USA

INTRODUCTION

Most analyses of possible future bioterrorism events predict they may be similar to the anthrax events of 2001. Specifically, a limited population of individuals may experience morbidity or mortality, but the concern, panic, and worry stirred up by the threat will catch the attention of the entire nation. If public health IT is to help with bioterrorism preparedness, it needs to not only address the mitigation of civilian illnesses and deaths, but also help to manage individual and societal fears springing from the real or threatened occurrence of such an event.

BACKGROUND

In order to understand how public health information technology can aid public health preparedness in terms of bioterrorism preparedness and associated emergency response, it is apt to start with a definition of bioterrorism. In 1998, the U.S. Department of Health and Human Services (DHHS) appointed the Centers for Disease Control and Prevention (CDC) to coordinate and lead the overall planning effort to upgrade national public health capabilities to respond to biological and chemical terrorism. This action complemented the CDC's established mission, specifically, to promote health and quality of life by preventing and controlling disease, injury, and disability (Gerberding, 2005).

In establishing the Bioterrorism Preparedness and Response Program (BPRP) within the CDC, DHHS framed the context of bioterrorism as the use or threatened use of biological agents or toxins against civilians, with the objective of causing fear, illness, or death. The CDC was charged by DHHS to coordinate and assist local and state public health and medical officials with the detection, identification, and response to a bioterrorism event. BPRP has developed several public health IT solutions to support these objectives (Kun & Bray, 2003; RAND Science and Technology Policy Institute, 2001).

Moreover, the CDC has distributed federal funds to support the Laboratory Response Network (LRN). The LRN serves as a network of labs prepared to respond to biological and chemical terrorism, and includes state and local public health, veterinary, military, and international labs. LRN labs are designated as either national, reference, or sentinel labs depending on the types of tests they

can perform and their containment facilities (i.e., lab capability). Since its launch, the LRN specifically has been involved with the anthrax events of 2001, the severe acute respiratory syndrome (SARS) events of 2003, and the ricin events of 2003 to 2004. The LRN represents a partnership that includes the Association of Public Health Laboratories (APHL), the CDC, the Department of Defense (DoD), the Federal Bureau of Investigation, and other collaborating entities. There are several key public health IT components to the LRN (Bray, 2003; Morse et al., 2003).
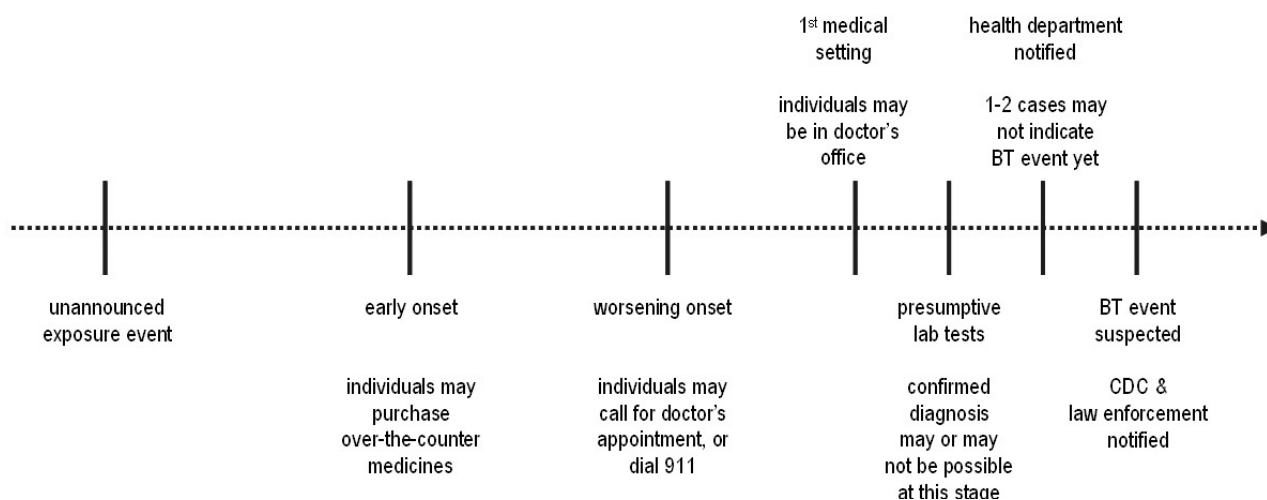
IT APPROACHES USED IN RESPONSE TO BIOTERRORISM

Public health IT can help with the detection and investigation of a bioterrorism event by advocating standards in the electronic reporting of collected epidemiological data and results at the local, state, and federal levels. Furthermore, public health IT can advocate standards in the routing and security of data. Routing and security differ as they represent how data are transported semantically from one location to another, as well as how data are made available to authorized users only. Currently, while there are several efforts to standardize

hospital and public health data, several areas key to public health surveillance efforts lack definitive standards for electronic collection, routing, and security of data (Devadoss, Pan, & Singh, 2005; U.S. General Accounting Office [GAO], 2003).

BPRP has invested public health IT resources into an aberration detection solution known as the Early Aberration Reporting System (EARS). The EARS tool was developed to facilitate the analysis of public health surveillance data. The primary purpose of the EARS tool was to provide state and local health departments with the ability to apply aberration detection methods of proven degrees of sensitivity to either collected count or rate data. As the EARS tool is neutral when it comes to the specific data type or format being collected, public health professionals can analyze different types of data (e.g., 911 calls, ER [emergency room] data, school absenteeism data) using the same system (CDC, 2002; Kun & Bray, 2003).

In addition to providing the code for the EARS tool freely to state and local public health departments, BPRP also has provided drop-in surveillance assistance for high-profile events, chiefly via site-specific implementations of the EARS tool and other tools. Such events included the 1999 World Trade Organization Meeting in Seattle, the 2001 Democratic National Convention, and the 2001

Figure 1. Timeline of a hypothetical bioterrorism response

| | | | 1st medical setting | health department notified | |
| | | | individuals may be in doctor's office | 1-2 cases may not indicate BT event yet | |

unannounced exposure event | early onset | worsening onset | presumptive lab tests | BT event suspected

individuals may purchase over-the-counter medicines | individuals may call for doctor's appointment, or dial 911 | confirmed diagnosis may or may not be possible at this stage | CDC & law enforcement notified

Related Content

Supporting Policy-Makers with Social Media Analysis Tools to Get Aware of Citizens' Opinions
Timo Wandhöfer, Steve Taylor, Miriam Fernandez, Beccy Allen, Harith Alani, Somya Joshi, Paul Walland, Sergej Sizov, Catherine van Eeckhaute, Mark Thamm, Arnim Bleier, Peter Mutschkeand Vasilis Koulolias (2014). *IT in the Public Sphere: Applications in Administration, Government, Politics, and Planning (pp. 121-156).*
www.irma-international.org/chapter/supporting-policy-makers-with-social-media-analysis-tools-to-get-aware-of-citizens-opinions/104014

Wrestling with Contradictions in Government Social Media Practices
Lars Haahr (2014). *International Journal of Electronic Government Research (pp. 35-45).*
www.irma-international.org/article/wrestling-with-contradictions-in-government-social-media-practices/110955

The Politics of Social Media: Mediating Ambivalences in the Era of Political Populism
Joseph L. Flores (2020). *Examining the Roles of IT and Social Media in Democratic Development and Social Change (pp. 22-54).*
www.irma-international.org/chapter/the-politics-of-social-media/248397

Information Networks, Internet Governance and Innovation in World Politics
Claudia Padovaniand Elena Pavan (2009). *Electronic Constitution: Social, Cultural, and Political Implications (pp. 154-173).*
www.irma-international.org/chapter/information-networks-internet-governance-innovation/9656

Institutionalisation, Framing, and Diffusion: The Logic of Openness in eGovernment and Implementation Decisions - A Lesson for Developing Countries
Bongani Ngwenya, Sam Lubbeand Rembrandt Klopper (2012). *Digital Democracy: Concepts, Methodologies, Tools, and Applications (pp. 1212-1232).*
www.irma-international.org/chapter/institutionalisation-framing-diffusion/67658