Chapter 13
Public Health Surveillance for Bioterrorism

Peter N. Wenger, William Halperin, and Edward Ziga

To paraphrase D. A. Henderson, if the public health infrastructure were a living organism, public health surveillance would be its sensory organ system. It receives and processes data from its environment that subsequently impacts on the organism's resulting actions. The appropriateness of those actions is dependent on the "health" of the sensory organs. More formally, public health surveillance is defined as "the ongoing, systematic collection, analysis, and interpretation of health data essential to the planning, implementation, and evaluation of public health practice, closely integrated with the timely dissemination of these data to those who need to know [1]."

Surveillance activities provide evidence-based information vital to subsequent investigative, research, or prevention and control efforts but do not include those efforts [2]. Surveillance is the component of public health practice that provides the information assisting in directing the appropriate response. This applies to any public health surveillance system regardless of its purpose. This chapter will focus the discussion on public health surveillance issues relevant to bioterrorism. For those readers interested in pursuing more information on public health surveillance in general, the authors suggest Teutsch and Churchill's [3] and Halperin and Baker's [4] excellent texts on public health surveillance.

13.1 Consequences of Bioterrorism

Incidents involving bacterial pathogens [5, 6], chemical agents [7], and the September 11, 2001, attack on the World Trade Center in New York City clearly demonstrate the overt vulnerability of civilian populations to terrorist acts. The resulting morbidity and mortality and subsequent psychosocial and

P.N. Wenger
Associate Professor, Departments of Preventive Medicine and Community Health/
Pediatrics, University of Medicine and Dentistry of New Jersey/New Jersey Medical
School, NJ, USA
e-mail: wengerpn@umdnj.edu

L.I. Lutwick, S.M. Lutwick (eds.), *Beyond Anthrax*,
DOI: 10.1007/978-1-59745-326-4_13, © Springer Science+Business Media, LLC 2008

economic impact on communities can be devastating. Bioterrorism can differ in several significant aspects from other modes of terrorism. Terrorist activities involving chemical agents, small arms, explosive or incendiary devices, or nuclear or radiological weapons are likely to be recognized by first responders such as the police, fire department, emergency medical service (EMS) or Hazardous Material (Hazmat) personnel at the point of attack. The morbidity and mortality caused by these agents are essentially limited to the area in which they are dispersed with secondary effects expected among first responders and in healthcare facilities to which victims are transported.

The covert intentional release of a biological agent, on the other hand, may not have an immediate impact due to the delay between exposure and onset of disease (incubation period). Initial recognition of disease caused by bioterrorist activity will most likely be by medical personnel in emergency departments, clinics, or private practices some days or weeks after release of the agent. Outbreaks of disease caused by bioterrorist activity [8] may initially present similar to many common and naturally occurring outbreaks such as influenza, resulting in further delay in the recognition of the event for what it is. Properties of certain biological agents of terrorism (e.g., smallpox, pneumonic plague, and viral hemorrhagic fevers) include person-to-person transmission. The potential for a sustained outbreak with widespread cases can be great, therefore, unless appropriate interventions that contain the outbreak are implemented. The potential for delayed recognition and response with subsequent dire consequences is substantial. There are many biological agents considered potential bioweapons. The Centers for Disease Control and Prevention (CDC) has developed three categories of biological agents, prioritized as to their potential of bioterrorist use and the severity of disease they may produce (Box 1).

13.2 Surveillance

The response to a bioterrorist incident, including medical, public health, law enforcement, and political interventions are predicated on initial detection of disease associated with the intentional release of the biological agent. Recognition of disease and outbreaks due to either naturally occurring or intentional release of infectious pathogens has depended on astute healthcare providers contacting the appropriate public health agency at the point of initial recognition of cases [1, 2, 9]. For example, if the astute physician in Florida who recognized and reported the initial inhalational anthrax case in the 2001 anthrax outbreak [6] had not either identified or reported the case, it may have delayed recognition of the outbreak for several weeks. This would have delayed implementation of infection control interventions in the affected mail facilities, United States Senate office building, and other contaminated buildings resulting in possible increased morbidity and mortality due to anthrax.

The existence of organized surveillance efforts in a public health agency (e.g., health department) provides the infrastructure for conveying information to facilitate a timely and appropriate response [2]. The threat of bioterrorism has emphasized the need to improve and augment existing surveillance methods and systems to facilitate early detection of disease activity as well as integrate surveillance activity on all levels.

There are over 100 surveillance and public health information systems maintained by different programs at the CDC and hundreds more at the local and state level. Surveillance systems are developed to monitor and disseminate information on many different health-related events involving infectious diseases, chronic diseases, environmental and occupational health, birth defects and injury control. Surveillance for bioterrorist-related disease outbreaks is a component of surveillance for infectious diseases. Fundamental infectious diseases surveillance in the United States has been well established for years, however, surveillance for disease and injury associated with other terrorist-related activity, such as the intentional release of toxic chemical agents and detonation of radiological devices, has not received the same attention. While some disease related to other terrorist activity may be captured in surveillance for bioterrorist activity (e.g., toxic injury due to ricin), systems will have to be designed with these events in mind. Surveillance systems maintained for infectious diseases of public health importance include communicable diseases with epidemic potential, vaccine-preventable diseases, emerging infectious diseases, HIV/AIDS, hospital-acquired infections, tuberculosis, foodborne infectious diseases, antimicrobial-resistant organisms among others. While methods for conducting public health surveillance may differ considerably by program and disease, the general flow of data and information through a surveillance system is schematically represented in Fig. 13.1.

13.2.1 Fundamental Surveillance

The most fundamental surveillance for infectious diseases in the United States is maintained by the National Notifiable Disease Surveillance System (NNDSS). It has been functioning in some form since 1878 [10]. NNDSS seeks reports on diseases caused by many different organisms (Box 2). It is a passive surveillance system in which a healthcare practitioner or a clinical laboratory will report a suspected or confirmed case of a notifiable infectious disease. Reporting is to the local and/or state health department that then passes the information, usually stripped of personal identifiers, on to federal authorities, in this case, the CDC.

Traditionally, data are reviewed on a case-by-case basis at the local level to determine action required on any individual case or local outbreak. A more complete analysis is performed at the state and national levels to detect any unusual patterns that may indicate spread of disease outside the local

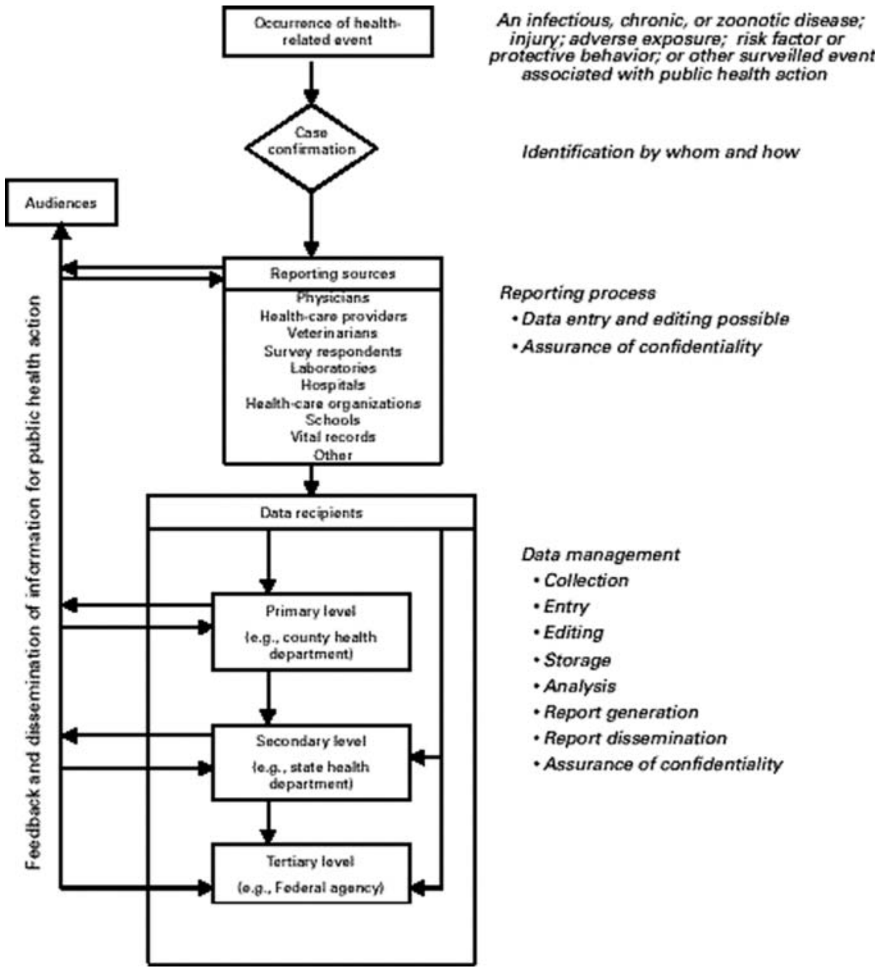
Occurrence of health-related event
An infectious, chronic, or zoonotic disease; injury; adverse exposure; risk factor or protective behavior; or other surveilled event associated with public health action
Case confirmation
Identification by whom and how
Audiences
Reporting sources
Physicians
Health-care providers
Veterinarians
Survey respondents
Laboratories
Hospitals
Health-care organizations
Schools
Vital records
Other
Reporting process
• Data entry and editing possible
• Assurance of confidentiality
Data recipients
Primary level (e.g., county health department)
Secondary level (e.g., state health department)
Tertiary level (e.g., Federal agency)
Data management
• Collection
• Entry
• Editing
• Storage
• Analysis
• Report generation
• Report dissemination
• Assurance of confidentiality
Feedback and dissemination of information for public health action

Fig. 13.1 Simplified flow chart for a generic surveillance system
Centers for Disease Control and Prevention. Updated Guidelines for Evaluating Public Health Surveillance Systems: Recommendations from the Guidelines Working Group. MMWR 2001;50(RR-13):8

jurisdiction [11]. The data collected is published as cumulative provisional cases weekly in the *Morbidity and Mortality Weekly Report*(MMWR) and as final corrected data at the end of the year in the annual *Summary of Notifiable Diseases, United States*. Notifiable disease statistics are also available from CDC's National Center for Health statistics in its publication, National Vital Statistics Reports and on the Internet at http://www.cdc.gov/nchswww/.

The Council of State and Territorial Epidemiologists (CSTE), in collaboration with the CDC, recommends the health conditions to be notifiable through the NNDSS. Each state, however, determines whether and how these conditions should be made reportable except for the quarantinable diseases (cholera, diphtheria, infectious tuberculosis, plague, potential pandemic influenza viruses, SARS, smallpox, yellow fever, viral hemorrhagic fevers). Reporting of these infections is required by international regulation [2, 11]. The legal basis requiring reporting of notifiable diseases varies by state, as does the authority for determining which cases are reportable [2, 11]. Depending on the state, reporting of notifiable diseases may be mandated by the legislature, state health officer or epidemiologist, the board of health or some combination thereof [2, 12, 13]. Most states require reporting of all notifiable conditions recommended by CSTE and many have included diseases not included in the NNDSS. For instance, smallpox was removed from the NNDSS list of notifiable diseases in 1988 due to the declared eradication of the disease by the World Health Assembly in 1980; however, most states have reinstituted mandatory reporting of smallpox because of concerns of its use as a bioweapon. The Infectious Disease Committee of the CSTE has since recommended that smallpox be placed under surveillance by all states, territories, and the CDC as part of NNDSS [14]. In addition, many states mandate the reporting of outbreaks due to any pathogen regardless of inclusion in the NNDSS list of notifiable infectious diseases.

13.2.2 Information Technology Impact

Advances in communication and information technology over the past half century have revolutionized the practice of public health surveillance. Notifiable disease reporting was traditionally performing using paper-based data collection forms. In 1984, the CDC in collaboration with the CSTE began testing the Epidemiologic Surveillance Project [15], with a goal to demonstrate the effectiveness of computer transmission of public health surveillance data between state health departments and the CDC. The project developed computer programs using existing disease surveillance systems to transmit data to the CDC on all nationally notifiable diseases. In 1985, the system became a fully interactive computer-based reporting system. By 1989, all 50 states were participating and the project was renamed the National Electronic Telecommunications System for Surveillance (NETSS) [15, 16]. De-identified data is transmitted weekly from all 50 state health departments as well as from New York City, Washington D.C., and five US Territories.

Though the NETSS initiative facilitated disease notification from the state to the federal level, it was clear that the myriad systems that comprise the US public health infrastructure from the local to the federal levels often were not integrated, interfering with the timely flow of information [17]. In 1993, the CDC/Agency for Toxic Substances and Disease Registry (ATSDR) Steering Committee on Public Health Information and Surveillance System convened to implement a major initiative for the creation of integrated public health surveillance and health information systems. Their recommendations are documented in the 1995 report, *Integrating Public Health Information and Surveillance Systems* [18]. Subsequently, the National Electronic Disease Surveillance System (NEDSS) initiative was developed and is currently in the process of being implemented. While NETSS addressed the issue of electronic data transfer from the state level to the CDC, NEDSS has expanded the scope of the initial initiative to include the integration of all related surveillance systems at the local, state and federal level through innovative electronic and information technology. NEDSS "promotes the use of data and information system standards to advance the development of efficient, integrated, and interoperable surveillance systems at federal, state and local levels [19]." The long-term objective of NEDSS [20] is to facilitate development of complementary electronic information systems that automatically gather health data from a variety of sources on a real-time basis as well as facilitate the monitoring of the health of communities. NEDSS will also assist in the ongoing analysis of trends and detection of emerging public health problems and provide information for setting public health policy. The NEDSS architecture will eventually replace the NETSS reporting format. NEDSS currently resides within the Public Health Information Network (PHIN) [21] initiative and serves as its public health surveillance component.

An incarnation of NEDSS, the NEDSS Base System (NBS), is actual surveillance software that may be deployed by state health departments in collaboration with the CDC. As of June 2007 it is deployed to 16 states including Alabama, Arizona, Idaho, Maryland, Maine, Montana, Nebraska, New Mexico, Nevada, Rhode Island, South Carolina, Tennessee, Texas, Virginia, Vermont, and Wyoming [22]. Other states have or are in the process of developing computer-based surveillance data collection and processing systems that are NEDSS-compatible. These systems will eventually be incorporated into a fully integrated surveillance system from the local to national level. The New Jersey Communicable Diseases Reporting and Surveillance System (CDRSS) is an example of a state developed NEDSS-compatible web-based surveillance data collection and processing system that will be discussed subsequently.

13.2.3 Surveillance and the Public Health Infrastructure

A major purpose of surveillance for bioterrorist events is detection at the earliest possible time of infectious diseases occurrences due to the intentional release of bioagents and to disseminate the information promptly to those who will affect appropriate public health, medical, law enforcement, and sociopolitical interventions. Sustainability of a surveillance system wholly dedicated to very rare events such as bioterrorist-related disease outbreaks would be expensive and difficult to maintain. Episodes of naturally occurring infectious diseases of great public health importance are not uncommon and pose many of the same surveillance problems as detecting the intentional release of bioagents.

Severe acute respiratory syndrome (SARS), HIV/AIDS, multidrug-resistant tuberculosis, foodborne disease outbreaks, pandemic influenza, and West Nile virus show the necessity of vigilant and sustained surveillance systems. Surveillance activities require time, money, and most importantly and vastly underappreciated, human resources. Development of new surveillance systems and improvements in existing systems to better detect bioterrorist-related disease activity should include the capacity to monitor for other infectious diseases of public health importance including emerging infectious diseases and vaccine-preventable diseases among others. These systems must have routine surveillance capabilities in order that they survive the extended periods of bioterrorist activity dormancy.

After years of political and financial neglect, our current public health infrastructure is currently under tremendous stress to meet the myriad public health problems posed daily regardless of the demands of bioterrorism security. For example, the authors of this chapter work with the Communicable Diseases Division (CDD) of the Department of Health and Human Services of Newark, New Jersey (NDHHS). Newark is a city of approximately 250,000 residents in a metropolitan area of several million people located about 15 miles from downtown New York City. The residents of Newark are ethnically diverse with a substantial immigrant population. A significant portion of the population exists under the poverty level. All the public health problems found in urban areas are experienced by the city. There are tens of thousands commuters in the city throughout the week including 40,000 students attending the colleges, universities, and graduate schools. In addition, Newark Liberty Airport that services 32 million passengers a year, including 8 million international travelers, and the Port of Newark, one of the largest ports for container ships in the United States, are located within city boundaries. In addition, many vital roadways essential for the nation's commercial transport pass through the city. The potential for bioterrorist activity is great. The CDD of NDHHS manages infectious disease surveillance activities, including surveillance for bioterrorism. Despite funding for biodefense activities, the CDD remains understaffed and financially stressed to meet its' routine, non-terrorist-related public health responsibilities. A case can be made that the advent of substantial funding sources dedicated to bioterrorist-related activity has extended the preexisting public health resources and divided attention from foundation public health issues. For example, during the smallpox vaccination campaign in early 2003, much of the public health workforce were furloughed from their usual duties to meet the demands required from the campaign leaving their usual responsibilities unfulfilled. The challenge is to develop and maintain surveillance capabilities that meet the daily needs of the community (e.g., vaccine-preventable infectious diseases, foodborne disease outbreaks, etc.) and are flexible enough to detect bioterrorist events. To meet this challenge the CDD/

NDHHS formed an Office of Surveillance and Prevention (OSP) under the direction of the local Health Officer located at the NDHHS. Using state biodefense funding, a fulltime epidemiologist was hired for the OSP and a cooperative consultative arrangement was reached with the Department of Preventive Medicine and Community Health (DPMCH)/University of Medicine and Dentistry of New Jersey (UMDNJ)/New Jersey Medical School (NJMS) and UMDNJ School of Public Health (SPH). This arrangement provides the CDD/NDHSS with additional expertise in surveillance, epidemiology, infectious diseases, and chemical toxins that it was not able to afford to directly employ. Examples of OSP surveillance activities will follow in this chapter.

13.2.4 Indirect Benefits

Most of the discussion of surveillance for bioterrorism involves early detection of disease due to bioterrorist activity; however, surveillance activities can serve other purposes in the face of bioterrorism. Estimating the magnitude of morbidity and mortality in the population due to the bioagent once it has been released and assessing the effectiveness of interventions in limiting the diseases. Surveillance can be used to monitor adverse health events associated with bioterrorism [23] or other major public health events, such as those associated with long-term antimicrobial prophylaxis for specific agents (anthrax) [24] or vaccination campaigns (smallpox [25, 26], influenza [27]). In addition, surveillance information can be used to help focus response assets and assist in efforts to manage community concerns [28].

13.3 Reporting and Collection of Data

13.3.1 Reporting

It is one objective of a public health department to contain an outbreak of infectious disease within a single incubation period of the responsible agent to prevent transmission within the community, limiting unnecessary morbidity and mortality [29]. Early detection of bioterrorist-related activity not only has vital medical and public health implications but also offers the best opportunity for prevention of additional episodes through successful law enforcement intervention. Early detection is crucial in gaining control of any outbreak and early detection is dependent on timely reporting.

Biosensor technology detecting the presence of infectious agents in the environment prior to host infection offers the possibility of very early detection of the intentional release of bioagents. This technology, however, is currently very expensive, uncommon, and not well field tested. At this time, the earliest detection of disease due to infectious diseases, whether naturally occurring or intentionally released, depends on astute frontline healthcare providers and microbiology laboratory personnel.

All US states and territories have laws or regulations mandating the reporting of particular health conditions, including infectious diseases. New Jersey Administrative Code 8:57-1 requires *immediate* telephone reporting by healthcare providers, laboratory directors, and others in positions of authority (e.g., school principals, prison superintendents, etc.) to local public health authorities (if they cannot be located then state authorities) of *suspected* or confirmed cases of 19 different conditions including anthrax, botulism, brucellosis, plague, smallpox, tularemia, viral hemorrhagic fevers, and any outbreak or *suspected* outbreak, including but not limited to, a suspected act of bioterrorism. Recognition of suspected specific diagnosis (e.g., anthrax, plague, or smallpox), however, by frontline providers is difficult due to unfamiliarity with the syndromes associated with these agents or their similarity with the prodromal presentation of other naturally occurring infections. In addition, differential diagnoses are predicated by a physician's index of suspicion, usually determined by commonly occurring diseases and not rare entities.

13.3.2 Confirmation

Definitive diagnoses of infectious diseases require laboratory confirmation, usually by culture or serology, and it is at this point that diagnoses, especially of rare diseases, and reporting commonly takes place by laboratory personnel. Laboratory confirmation of infection involving culture of the agent from affected tissue usually takes several days after obtaining appropriate samples. Serologic evidence is usually not present at initial presentation. Other molecular diagnostic tools, such as polymerase chain reaction (PCR), can significantly shorten the turnaround time in obtaining microbiologic confirmation of a diagnosis. These testing modalities, however, are often not available at a local level, especially for uncommon pathogens and may not be ordered if available due to their expense if a common pathogen is the suspected etiologic agent. The situation is more difficult for laboratory identification of disease due to chemical toxins for which laboratory access is even more difficult and less widely used than for identification of infectious agents. Furthermore, outbreaks are often difficult to appreciate on the provider level and require a greater perspective (e.g., local community, city, regional, state(s), and nation) for recognition. For example, the extent of a recent outbreak of hepatitis A in western Pennsylvania was not recognized until review on a state level [30, 31]. Lack of awareness of reporting responsibilities by those required to report, including the what, when, whom, and how to report, as well as the ease of contact (availability of contact numbers, computer access, or forms) further exacerbate delay in reporting.

13.3.3 Adequacy of Collection

Doyle, et al [32], in an analytical literature review evaluating completeness of notifiable infectious disease reporting in the United States between 1970 and 1999, found that reporting completeness was most strongly associated with the reporter's perception of the seriousness of the disease being reported. This suggests that educational programs for providers and laboratory personnel stressing their public health duties in the effort versus bioterrorism as well as development of diagnostic aids in identifying disease associated with bioterrorist-related agents may be effective in improving conventional provider- and laboratory-based reporting.

13.3.4 Passive versus Active Systems

Reportable disease data is most often collected through a passive reporting system, that is one dependent on the initiative of the reporter and thus prone to under-reporting [1, 32]. Healthcare providers have numerous immediate responsibilities with respect to patient care so it is not surprising that reporting of diseases to public health agencies is often not prioritized. Even though required, the lack or perceived lack of resultant activity by health departments subsequent to case reporting discourages reporter participation. Active surveillance, the collection of data is elicited by the agency operating the surveillance system, is more likely to provide more complete reporting but is much more labor intensive and costlier than its passive cousin. One study [33] evaluated passive versus active surveillance in identifying cases of hepatitis A in Kentucky over a 22-week period. The report demonstrated that nine more cases were identified through the active surveillance system. This resulted in the prevention of an estimated additional seven cases through administration of prophylaxis to the contacts of the nine case-patients. The added benefit of active surveillance does not come without a price. The estimated cost of operating the active surveillance system was approximately six times that of the passive system [33].

While active surveillance may not be sustainable over long periods of time, it can be used over the short term for acute critical issues. This is often referred to as drop-in surveillance. The New York City Department of Health and Mental Hygiene (NYCDOHMH) and CDC performed active syndromic (see below) surveillance in sentinel emergency departments to identify bioterrorist activity in the aftermath of the September 11th terrorist attacks [23]. In Newark, an annual ethnic festival, usually attracting approximately 400,000 people, was scheduled late spring of 2003. Festival organizers expected a sizable contingent from Toronto, at that time experiencing a SARS outbreak. The NDHHS, which maintains passive emergency room surveillance in all five hospitals located in Newark, activated enhanced (collecting data for a specific condition or syndrome, in this case SARS), active surveillance in those same hospitals.

This active enhanced surveillance activity persisted for a period of 3 days prior to the festival (baseline), during the festival, and for 10 days following the festival (one incubation period).

A paper-based data collection tool based on the CDC case definition for SARS at that time was developed by the NDHHS OSP epidemiologist and distributed to appropriate emergency department personnel at each hospital. The form was used for every patient presenting with fever and/or respiratory symptoms during the described period. Health inspectors from the NDHHS visited each emergency department daily and collected the forms and reviewed emergency department logs for any missed possible suspects. The OSP epidemiologist reviewed all data. In addition, EMS personnel assigned to health stations at the festival site received training on evaluating festival attendees for SARS who present with suspicious symptoms. No cases of suspect or probable SARS were identified. At the end of the enhanced active SARS surveillance period, the OSP epidemiologist presented the information obtained to appropriate personnel in participating emergency departments. This surveillance activity not only served its expressed purpose but also fostered increased communication and cooperation between the NDHHS and the area's hospitals.

13.3.5 Personnel and Electronics

It is important for health departments to recognize who is responsible for notifiable disease reporting in their locale and develop close, mutually beneficial relationships with them. In Newark, a significant portion of the community receives initial medical care for acute conditions at local emergency departments. The NDHHS felt, therefore, it would be appropriate to focus initial bioterrorist-related surveillance activities in local emergency departments. The local hospital infection control practitioners (ICPs) are assigned the task of reporting notifiable infectious diseases to the health department in emergency departments and hospitals. One of the NDHHS initiatives was to organize monthly meetings for all the hospitals ICPs, attended by staff from the NDHHS OSP, in which issues of mutual interest are discussed. These meetings have greatly contributed to developing strategies to simplify reporting procedures and increase communication.

Many states have introduced electronic data collection and reporting to increase the completeness and timeliness of reporting. A NNDSS survey conducted by the CSTE in 2001 revealed that 24 of 45 (53.3%) states responding to the survey utilized some form of electronic data transfer in reporting notifiable disease data to state health departments [13]. The number has increased since then. The New Jersey Department of Health and Senior Services (NJDHSS) has developed the CDRSS, a web-based application used to enter, update and track notifiable communicable disease data for the purpose of aggregating and reporting the information to CDRSS system users, as well as the CDC.

CDRSS has been built to conform to NEDSS standards. Users will include ICPs, physicians, laboratories, and local, regional and state public health professionals. CDRSS allows real-time case reporting as well as case retrieval and filtration by various parameters. Summary information is available to all users. An ICP may access summary data on all reportable diseases reported through CDRSS but can retrieve personalized detailed data only on those cases reported from their institution, while a local health officer may retrieve detailed data on all cases reported in their jurisdiction. Data is easily exported to many different programs for the purpose of analysis or presentation. The application has been deployed to the provider level (hospitals [ICPs]) and some microbiology laboratories utilized by New Jersey healthcare providers and is in various stages of deployment to other reporting sources throughout the state. While no formal studies on system effectiveness have been completed at this date, most users have reported a much greater preference for CDRSS over paper-based reporting.

There is great interest in utilizing automated electronic data collection and transmission systems to facilitate early detection of bioterrorist activity. Capturing automated routinely collected data (e.g., billing, electronic medical records or charting, laboratory reports) from emergency departments [34], hospitals, ambulatory-care settings [28, 35, 36], and clinical laboratories for reporting notifiable diseases would complement, not supplant, existing provider- and laboratory-based reporting. In addition, automated electronic data collection would allow sustained data collection from multiple data sources that would ordinarily not be readily available if dependent upon manual data collection. Additional sources to consider include poison control centers, nurse and physician emergency hotlines, over-the-counter pharmacy sales, school and employer absenteeism records, and intensive care unit (ICU) medical records (*see* Table 13.1).

Automated electronic data collection has the potential to augment conventional reporting without additional de novo public health reporting responsibilities to frontline personnel. These systems can be designed to operate in real-time (transfer of data on entering into the system) or batch transfer of data at specified times. Studies of electronic laboratory-based reporting conducted at the University of Pittsburgh Medical Center [37] and the State of Hawaii Department of Health [38] revealed that electronic reports were received, on average, in a more timely manner and were at least as complete as conventional laboratory reporting. A review of five automated electronic laboratory systems, however, revealed problems with data transmission, sensitivity, specificity, and user interpretation [39]. Problems identified included lapses in reporting due to failure or adjustments in data extraction software and lack of uniformity of coding standards between clinical laboratories. Specificity was adversely affected due to automated data extraction errors in extracting culture results if entered in free text, for example, reporting as positive a negative culture result due to the organism's name appearing in free text. In addition, accumulation of duplicate reports, unnecessary reports

Table 13.1 Possible sources of health indicator surveillance data

Data source	Pros	Cons and confounders
Outpatient and emergency department visits	Reflects incidence of disease in the general population	Nonspecific – may be difficult to document definitive information
Intensive care unit diagnoses	Best indicator of rare events like west Nile virus or Hantavirus pulmonary syndrome	Will not capture milder cases
Over-the-counter pharmacy sales	Reflects symptomatology most broadly	Subject to promotions/sales
Clinical lab submissions	Ordered by clinicians	May not be ordered for all (most) patients
Medicare or medicaid claims	Ease of capture data	Problems with timeliness and accuracy
Nursing homes	Reported by medical personnel; immobile population with limited exposure possibilities	Immobility reduces exposure potential; not broadly representative
Systematic testing for specific disease agents in specimens submitted to public health lab	Specificity of diagnoses	Broad screening not likely to capture meaningful data; difficulty getting information on positive samples; not timely
School and work absenteeism	May occur earlier than clinician visits	Nonspecific; delays in obtaining data
Ambulance call chief complaints	Many communities with timely access to data	Nonspecific
Poison information center calls	Ability to access in real-time	Many not be related to infectious diseases
HMO/nurse hotline calls	Occur very early in outbreak	May be difficult to categorize

Reprinted with permission from Biological Threats and Terrorism: Assessing the Science and Response Capabilities: Workshop Summary © 2002 by the National Academy of Sciences, courtesy of the National Academies Press, Washington, D.C.

(e.g., screening rubella serology in pregnant women), and identification of unreportable conditions increased the number of false positives.

The ultimate identification of bioterrorist activity will be realized by investigation of reported diseases through surveillance by local and state health departments. Poor specificity in surveillance reporting will result in unnecessary investigations thus placing undue burden on an already overtaxed public health system. Many local health departments, additionally, do not possess the sophisticated information technology or expertise required to fully participate in automated electronic surveillance. Automated electronic surveillance systems will undoubtedly make important contributions in refining timely surveillance activity, however, there remain many development and implementation issues before its fundamental value will be realized.

13.4 Syndromic Surveillance Methodology

The inherent delays in conventional disease reporting have led to the exploration and development of alternative methods of early detection surveillance systems. Broadly speaking, syndromic surveillance involves monitoring disease or health-related event data that does not require specific medical diagnoses. A syndromic surveillance system collects and interprets data on clinical signs and symptoms that precede formal diagnosis in a way that would identify with sufficient probability an outbreak of public health interest, i.e., bioterrorist event. Data collected for syndromic surveillance could not be used in establishing a specific diagnosis in an individual; however, it may detect patterns of disease in a population that would indicate occurrence of an outbreak earlier than a surveillance system that requires a more definitive diagnosis. Reporting of routinely collected data such as ICD-9-coded chief complaints or initial diagnosis in emergency departments or ambulatory clinic settings may serve as data sources for syndromic surveillance.

13.4.1 Syndrome Classifications

Syndromic surveillance requires the classification of signs and symptoms such as fever, cough or dyspnea or ICD-9 codes into syndromic groups or clusters (detectors) that would be recognized by data extraction programs or personnel. For instance, a syndromic group for lower respiratory tract infections (LRTIs) may include all ICD-9 codes for pneumonia and bronchitis or descriptive terms such as fever, cough, difficulty breathing or combinations of terms such as fever and cough. Since significant variability in assigning diagnostic terms or ICD-9-coding to similar patients exists between providers and clinics, syndromic surveillance can reduce variability in reporting when collecting data from different providers. For instance, one provider may code a patient who initially presents with clinical signs and symptoms of a LRTI with the ICD-9 codes for cough and fever, while another may code it as an unspecified pneumonia and a third may give that patient a more specific diagnosis of viral pneumonia. If all those initial diagnostic ICD-9 codes were included in a syndromic cluster for LRTI that case would be captured while it may have been missed in a surveillance system requiring a more defined diagnosis depending on the patient's provider. In addition, it would allow capture of the suspected diagnosis earlier in the patient encounter.

This methodology, however, would have a corresponding decrease in specificity and thus positive predictive value in identifying an outbreak of LRTI due to any specific pathogen. For example, syndromic surveillance for cutaneous anthrax is more likely to detect cases of cutaneous anthrax in contrast to surveillance for the specific diagnosis. Given the large baseline number of cases of general cutaneous infection that would be identified by syndromic surveillance, however, the number of actual cutaneous anthrax cases that would have to occur for an outbreak to be identified would have to be large. A parallel example would be the detection of bioterrorist-related pulmonary disease during influenza season. The developers and users of any surveillance system will have to decide at what point specificity may be sacrificed to improve timeliness of reporting.

13.4.2 Evaluation of Syndromic Surveillance

It is important to periodically evaluate the sensitivity, specificity, and positive predictive value of these syndromic groups in identifying diseases or outbreaks of public health interest. This can be accomplished by comparison with a "gold standard" such as discharge diagnosis, emergency department or hospital chart review or final microbiology or serology laboratory results. Espino and Wagner at the Center for Biomedical Informatics at the University of Pittsburgh compared two syndromic groups to detect acute respiratory illness [40]. One group was constructed of ICD-9-coded chief complaints and the other of ICD-9-coded diagnoses obtained at a later point in the patient encounter. Performance was measured against review of emergency department records. No difference in sensitivity or specificity was found between the two syndromic groups in identifying actual acute respiratory disease. This suggests that syndromic groups constructed of ICD-9-coded chief complaints, which can be reported early on in the patient encounter, have a role in public health surveillance.

A comparison of syndromic categorization of chief complaint and discharge diagnosis for emergency department visits in US National Capitol Region revealed good overall agreement between the two ($\kappa = 0.639$), however, neurologic ($\kappa = 0.085$) and sepsis ($\kappa = 0.105$) syndrome categories had markedly lower agreement than other syndromes [41].

13.4.3 Electronically-Based Syndromic Surveillance

Data extraction for syndromic surveillance can be done manually as was done by the CDC and NYCDOHMH in the aftermath of September 11th [23]. The procedure, however, is much too labor intensive and expensive to be sustainable over long periods of time. Sustainability of syndromic surveillance depends on the development of automated electronic data transmission systems. An example of a syndromic surveillance system based on real-time automated electronic data collection and transmission is the Real-Time Outbreak and Disease Surveillance (RODS) system developed at the Center for Biomedical Informatics at the University of Pittsburgh [34].

The RODS system adheres to NEDSS specifications and currently operates in multiple cities, states, and countries. It was used during the 2002 Winter Olympics in Utah. In December 2002, RODS software was made available at no cost to health departments and academic institutions; however, it requires the technical resources to maintain real-time electronic disease surveillance systems. The RODS software has been open-sourced since September 2003 and those interested are directed to The RODS Open Source Project website at http://openrods.sourceforge.net/.

13.4.4 Role of Syndromic Surveillance

Syndromic surveillance is not meant to supplant existing provider- and laboratory-based surveillance but to augment these systems. Developing independent but complimentary surveillance systems can serve to confirm and validate information derived from existing systems as well as hopefully improve the sensitivity, specificity, and positive predictive value of overall surveillance in the detection of public health threats. Whether syndromic surveillance is more likely to detect the consequences of bioterrorist activity earlier than astute frontline clinicians or current surveillance systems remains unknown at this time. There is much to be done in exploring this approach to find its ultimate utility in public health surveillance. For those readers interested in pursuing more information concerning syndromic surveillance the authors recommend reviewing the numerous sources found on the CDC website (www.cdc.gov: search under syndromic surveillance).

13.5 Data Analysis and Interpretation

Surveillance system data are observational in nature and distributed over time and space thus allowing public health epidemiologists to describe patterns of disease in the community. It is the analysis and interpretation of the collected surveillance data that enables detection of unusual disease events or trends in the population. Analysis is the application of appropriate methods in aggregating the collected surveillance data and interpretation is the creative assessment of the analysis to detect emerging data patterns [1, 42]. While computer software programs are readily available for automated data analysis choosing the appropriate analytic method as well as the interpretation of analyzed data is wholly dependent on human reasoning. It is vital that epidemiologists involved with the analysis and interpretation of surveillance data understand and be intimately involved with the entire surveillance process. They must know the inherent idiosyncrasies of the data set and its analysis if the interpretation is to be meaningful.

13.5.1 Sentinel Health Events

Analysis and interpretation may be very simple and straightforward. The natural occurrence in the US of most the agents considered most likely to be used in bioterrorism-related activity (Box 1) is so uncommon [43] that one case report is enough to raise a high index of suspicion. These are in essence sentinel health events [44, 45] that signify failure of prevention, in this case, occurrence of a bioterrorist event. The anthrax assault through the US postal system in 2001 is a case in point. Public health authorities recognized quickly after the initial report from Florida that this was not a case of naturally occurring infection and disease.

Even if the agent is not initially recognized, sudden appearance of similar severe disease presentation in unexpected populations should alert authorities to suspicious circumstances and initiate appropriate action. Examples are adult respiratory distress syndrome with fever occurring in healthy young adults or children or in groups of people who work, study, or attended an event in the same location. It cannot, however, be anticipated that bioterrorist-related disease outbreaks will be so obvious. As mentioned earlier, prodromal illness due to many likely bioagents often present like other, naturally occurring pathogens. The episode may, therefore, be difficult to recognize as being a potential bioterrorist-related event, especially if initial numbers are small or occur over a widespread area.

Pathogens commonly causing disease in a community may be used as terrorist episode as was the case in the 1984 outbreak in central Oregon due to intentional contamination of salad bars with *Salmonella typhimurium* [5]. Advances in biotechnology have allowed the genetic manipulation of bacteria and viruses to increase their pathogenicity, virulence, and induce vaccine and antimicrobial resistance. Bioterrorists have the potential to acquire or develop formerly mildly or non-pathogenic microorganisms, which would not be immediately suspected, into bioweapons [46–48]. It is important, therefore, to have surveillance in place with the ability to promptly recognize the early onset of more subtle disease trends that suggest bioterrorist-related activity. In addition, it is essential to have infectious disease and emergency department physicians, ICPs, and clinical toxicologists in place throughout the medical system who are well trained and sensitive to the occurrence of unusual clinical presentations that may indicate terrorist activity or other public health emergencies.

13.5.2 Aberration Detection in Surveillance Data

Detection of bioterrorist-related disease through surveillance activities is often discussed in terms of outbreak or epidemic recognition. Epidemicity is defined as being "relative to the usual frequency of the disease in the same area, among the specified population, at the same season of the year [49]." The terms epidemic and outbreak are often used synonymously although outbreak contains less emotional content to the public.

In syndromic surveillance, an epidemic may be suggested by increases in the number of cases meeting the criteria for a syndromic cluster. This definition of epidemicity demands a comparison between an observed number of cases or health events in a specified population, time and place to what is expected or considered normal. An epidemic may require the presence of an aberration in disease trends. An aberration is defined as the occurrence of health events that are statistically significant when compared to the normal history [42]. Early detection of bioterrorist-related disease through syndromic surveillance requires development of analytic modeling techniques that will reliably detect aberrant signals over time and space using data collected and analyzed in real time or near real time (i.e., data batched and analyzed every 8, 16, or 24 h). The models use historical data over prescribed time intervals in specified populations and locations to predict the expected number of cases or rates of disease that then is compared with the observed number of cases or rates.

There are numerous methodological issues to consider and any method developed or chosen has its own particular advantages and disadvantages. It is vitally important that whatever model is used, it be tested periodically to confirm that it is reliably detecting what it was designed to detect, in this case early evidence of disease trends that may suggest bioterrorist activity. Obviously, this is difficult given the exceedingly low incidence of bioterrorist-related events but it can be accomplished by comparing it versus independent, reliable surveillance systems in early detection of naturally occurring events that may resemble onset of bioterrorist-related disease activity (i.e., historical or real-time seasonal influenza trends) [50].

It is important to remember that while the existence of an aberration may be considered necessary; it is not sufficient for the occurrence of an epidemic [51]. False positive case reports may give rise to aberrant signals in surveillance data. For instance, statistically significant increases in influenza-like illness may not indicate an increase in influenza infection but reflect other non-influenzal respiratory tract viral infections that will be captured as cases of influenza-like illnesses. In this case, laboratory evidence of influenza infection would be required to confirm an influenza epidemic.

While much of the analysis of surveillance data is designed to detect aberrations in disease trends, statistical significance is not a necessary perquisite for detection of bioterrorist activity. The small number of cases (18 definitive cases, 11 of them inhalational, over four states and the District of Columbia over 3 months) associated with the 2001 anthrax attack would not have triggered an alert (statistically significant increase, in this case, in a flu-like prodromal illness) in a local, state, or even national syndromic surveillance system attempting to capture anthrax.

There is no analytic or aberrant detection model that, in and of itself, is capable of identifying an epidemic or bioterrorist-related disease activity. It is the public health personnel responsible for surveillance activities that will ultimately decide on whether or not there is sufficient surveillance evidence suggesting unusual disease activity. One may speculate that improved surveillance may be best accomplished by the proliferation of highly trained, epidemiologically sophisticated infectious disease, toxicology, and other related professionals throughout the medical and public health landscape. This is, in fact, the rationale for the creation of the Epidemic Intelligence Service (EIS) at the CDC. EIS is an on-the-job training program in epidemiology for a cadre of health professionals who then populate medical and public health settings throughout the United States, improving the nations epidemiologic and surveillance capabilities [52].

Advances in molecular biology technology have made important contributions to infectious disease public health surveillance and can assist in rapidly confirming a suspected event. Technologies such as pulsed-field gel electrophoresis (PFGE), restriction fragment length polymorphism analysis, and nucleic acid sequencing have allowed the recognition of related disease outbreaks over widespread geographic, temporal, and convoluted social terrain that would have been difficult to identify on epidemiologic evidence and analysis alone. This has been demonstrated in the recognition of common source multi-state and international foodborne disease outbreaks [53], tuberculosis outbreaks [54, 55], and in the surveillance of nosocomial infections [56, 57].

13.6 Information Dissemination and Communication

13.6.1 Appropriate Reporting of Information

Immediate notification of the proper authorities (“those who need to know”) of surveillance information that indicates suspected bioterrorist-related disease is a principal function of the public health surveillance process. Notification and standard operating procedure (SOP) protocols must be clearly established and immediately available to not only those responsible for disseminating surveillance information but to backup personnel in the event regular personnel are unavailable. The protocols should clearly describe who is to be contacted and how for any given situation as well as a hierarchy of contacts if the main contact is inaccessible. Means for emergency and routine communication should be maintained and routinely tested to insure reliability. Recent advancements in communication technology, including the Internet, allow the instantaneous transfer of information, however this technology relies on communication systems that may be vulnerable to interference. Alternative communication channels should be established in lieu of disruption of regular channels during an emergency.

Surveillance information must be presented in a clear, understandable format developed for the recipient of that information. Surveillance information may be distributed to many different recipients with different functions and levels of understanding. Recipients may include physicians, hospital infection control or emergency departments, Office of Emergency Management (OEM) agencies, public health authorities, law enforcement agencies or mass media organizations. The surveillance information should be pertinent to the needs of the recipient so that they may better act on that information without confusion. Distilling data into charts and graphs can simplify and help clarify surveillance information; however, if done improperly the risk of transmission of misinformation is greatly increased. It is recommended that the public health agencies operating surveillance systems work closely with system users to develop methods of information transfer and presentation that are timely, consistent, clear and useful.

13.6.2 Feedback to Surveillance Participants

While prompt dissemination of surveillance information is imperative in any system designed to detect bioterrorist-related disease, the consistent delivery of surveillance information in a context that is useful to the participants and users of the surveillance system(s) is essential for sustainability. Participation in a surveillance system depends on consistent feedback of information to the system's users and the perception that the information is useful. A surveillance system in which data flows in one direction (e.g., little to no feedback to the systems reporters) will undoubtedly experience lack of reporter enthusiasm with resulting reporting delay as well as under-reporting. Timely feedback of information generated by the surveillance system to the reporting entities enhances the chances of reporter participation in the system. In Newark, the OSP epidemiologist in the NDHHS not only forwards the daily emergency department census and admission data to the NJDHSS but distributes the results of the local data analysis to the ICPs at the five participating local hospitals in individual and aggregate format on a weekly basis. The NJDHSS distributes aggregated data on a state and county level collected via the CDRSS through an e-mail list-serve to the state regional epidemiologists who then share the information with interested local parties.

13.6.3 Interorganizational Communications

Close personal communication between representatives of different entities or organizations that are involved in preparedness activities for terrorist events yields great benefits for public health surveillance performance. Within a month of September 11, 2001, the CDD of the NDHHS and the Department of Preventive Medicine and Community Health of the New Jersey Medical School (NJMS) began hosting what initially were Thursday evening sessions of interested public health parties discussing local and regional issues of public health preparedness and response to terrorist activities. Discussions have since included diverse topics of significant public health interest. Participants have included representatives from local hospitals, the New Jersey Medical School and UMDNJ School of Public Health, local Emergency Medical Services (EMS), the New Jersey Poison Information and Education System (NJPIES), healthcare payer organizations, the Port Authority of New Jersey and New York (PANJNY), and the Public Health Service Quarantine Service, among others. Topics have included exercises in specific scenarios (e.g., arrival of a passenger with suspected smallpox infection to Newark Liberty Airport), local public health SARS preparedness, and discussion of specific surveillance issues with respect to agents of bioterrorism, influenza, SARS, and vaccine-preventable diseases. The familiarity engendered during these serial sessions between the representatives of the various agencies has resulted in increased interorganizational cooperation in developing and maintaining improved surveillance communication.

As mentioned earlier, there is currently an effort to integrate the multiple public health data streams on the local, state, and national levels to facilitate early detection of public health issues and emergencies [21]. The Public Health Information Network is the framework in which this initiative is being developed. The alerts and communication component of PHIN is the Health Alert Network (HAN). The purpose of HAN is to ensure that all communities have 24/7 access to timely emergent public health information; the services of highly trained public health professionals; and evidence-based practices and procedures for effective public health preparedness, response, and service [21]. The objective is a seamless rapid alerts and communication system that connects the entire US public health infrastructure; from the local to the national. In New Jersey, HAN is accessed through the New Jersey Local Information and Communications System (NJLINCS) at the password-protected NJ HAN website [58]. Statewide information management resides in the NJDHSS while local management is governed by NJLINCS coordinators located at the county and selected city health departments. Access to the system requires registration through the local NJLINCS coordinators.

13.7 Confidentiality

Surveillance activity, especially on the local and state levels, often requires collection of personal identifying data. Subsequent investigation of infectious disease outbreaks cannot be carried out without person, place, and time data. In the event of bioterrorist activity, information sharing with law enforcement agencies will become necessary. Public health activities, including surveillance, are dependent on the public's acceptance and protecting the confidentiality of personal health information forms the basis of that trust between the public and the public health establishment.

The standard operating procedure (SOP) for surveillance systems must include provisions for maintaining confidentiality of personal health information and consideration of potential uses of data that contain personal identifiers [59], including sharing surveillance data with law enforcement agencies in the event of suspected bioterrorist activities. Protocols must be established restricting access to personal information as well as providing secure storage of data, whether electronic or paper based. Electronic and more traditional data transfer must be made secure and protected from saboteurs and computer hackers. Public health agencies should review the confidentiality and security provisions with all organizations or institutions they may share data with.

The Health Insurance Portability and Accountability Act (HIPAA) of 1996, which took affect April 14, 2003, provides the legal basis addressing the privacy and security of health information. The HIPAA Privacy Rule [60] continues to allow for the existing practice of sharing protected health information (PHI) with public health authorities authorized by law to collect or receive such information to aid them in their activities to protect the public's health. HIPAA requires the development and implementation of policies and procedures to protect the confidentiality and secure the security of personal health information as discussed in the previous paragraph.

13.8 Conclusion

Public health surveillance is an ongoing system of data collection, analysis and interpretation, and then dissemination of that information to those who will act upon it accordingly. It is within this framework, in close harmony with astute healthcare workers in clinical practice and laboratory personnel, that the consequences of an intentional release of a bioweapon will be recognized. This will occur either by direct observation (e.g., a report of a case of anthrax) or through detection of aberrant events (e.g., greater than expected occurrence of severe lower respiratory tract infections). Advances in information technology and the development of innovative surveillance methodology will augment their efforts. It is essential that adequate numbers of people are dedicated to these tasks and they receive the proper training to develop expertise in developing and maintaining surveillance systems with the flexibility to meet the dynamic demands of public health in an ever-changing society. This will only be accomplished through sustained public, political and financial commitment to rebuilding the public health infrastructure.

Information and communication technology has the potential of revolutionizing the practice of public health. They allow the development of novel methods of data reporting and collection, analysis, and dissemination. However the information technology industry has the potential of creating a huge financial drain on public health that may actually impede public health programs. As new methods are developed it is necessary they undergo critical evaluation as to their effectiveness. This can only be accomplished through a public health infrastructure populated with people who understand and are familiar with the intricacies of surveillance. The Institute of Medicine has identified the fragmentation of surveillance systems and lack of integration of public health data and information systems as a critical barrier to the timely flow of information in times of crisis [17]. These technologies provide the tools in which to integrate multiple programmatic public health surveillance and information systems from the local to federal level through the NEDSS initiative. However it is important to remember that those who use them will determine the ultimate value of these tools.

References

1. Thacker, S. B. and Berkelman, R. L. Public health surveillance in the United States. *Epidemiol. Rev.* 10, 164–190, 1988.
2. Thacker, S. B. Historical development. In: Teutsch, S. M. and Churchill, R. E. (eds) Principles and Practices of Public Health Surveillance, 2nd edition. New York: Oxford University Press, 1–18, 2000.
3. Teutsch, S. M. and Churchill, R. E. (eds). Principles and Practices of Public Health Surveillance, 2nd edition. New York: Oxford University Press, 2000.
4. Halperin, H. and Baker Jr., E. L. (eds). Public Health Surveillance. New York: Van Nostrand Reinhold, 1992.
5. Török, T. J., Tauxe, R. V., Wise, R. P., et al. A large community outbreak of salmonellosis caused by intentional contamination of restaurant salad bars. *J. Amer. Med. Assoc.* 278, 389–395, 1997.
6. Brachman, P. S. The public health response to the anthrax epidemic. In: Levy, B. S. and Sidel, V. W. (eds) Terrorism and the Public Health. New York: Oxford University Press, 101–117, 2003.
7. Okumura, T., Suzuki, K., Fukuda, A., et al. Tokyo subway sarin attack; disaster management, part 1: Community emergency response. *Acad. Emerg. Med.* 5, 613–617, 1998.
8. Centers for Disease Control and Prevention. Recognition of illness associated with the intentional release of a biologic agent. *Centers for Disease Control and Prevention*50, 893–897, 2001.
9. Institute of Medicine National Research Council. Intelligence, detection, surveillance, and diagnosis. In: Countering Bioterrorism: The Role of Science and Technology. Washington DC: The National Academies Press, 1–18, 2002.
10. Centers for Disease Control and Prevention. National notifiable disease surveillance system. Available at <http://www.cdc.gov/ncphi/disss/nndss/nndsshis.htm>. Accessed on January 22, 2008.
11. Teutsch, S. M. Considerations in planning a surveillance system. Appendix 2A. In: Teutsch, S. M. and Churchill, R. E. (eds) Principles and Practice of Public Health Surveillance, 2nd edition. New York: Oxford University Press, 27–29, 2000.
12. Chorba, T. L., Berkelman, R., Safford, S. K., et al. Mandatory reporting of infectious diseases by clinicians. *J. Amer. Med. Assoc.* 262, 3018–3026, 1989.
13. Council of State and Territorial Epidemiologists. Nationally notifiable disease surveillance system queriable database: NDSS assessment 2005: State and territorial reporting profiles. Available at <http://www.cste.org>. Accessed on January 22, 2008.
14. Council of State and Territorial Epidemiologists. Position statements 2003: smallpox surveillance (03-ID-03). Available at <http://www.cste.org>. Accessed on January 22, 2008.

15. Centers for Disease Control and Prevention. National electronic telecommunications system for surveillance. Available at <http://www.cdc.gov/ncphi/disss/nndss/netss.htm>. Accessed on January 23, 2008.
16. Centers for Disease Control and Prevention. National electronic telecommunications systems for surveillance-United States, 1990-1991. *MMWR – Morbid. Mortal. Week. Rep.* 40, 502–503, 1991.
17. Committee on Assuring the Health of the Public in the 21st Century. The governmental public health infrastructure. In: Institute of Medicine. The Future of the Public Health in the 21st Century. Washington DC, The National Academies Press, 96–177, 2003.
18. Centers for Disease Control and Prevention. Integrating public health information and surveillance systems. Available at <http://www.cdc.gov/nedss/Archive/katz.htm>. Assessed on January 23, 2008.
19. Centers for Disease Control and Prevention. National electronic disease surveillance system. Available at <http://ww.cdc.gov/nedss/>. Assessed on January 23, 2008.
20. Centers for Disease Control and Prevention. Supporting public health surveillance through the national electronic disease surveillance system. Available at <http://www.cdc.gov/nedss/Archive/Supporting_Public_health_Surv.pdf>. Accessed on January 23, 2008.
21. Centers for Disease Control and Prevention. Public health information network. Available at <http://www.cdc.gov/phin>. Accessed on January 23, 2008.
22. Centers for Disease Control and Prevention. National electronic disease surveillance system base system. Available at <http://www.cdc.gov/phin/activities/applications-services/nedess/nbs.html>. Accessed on January 21, 2008.
23. Centers for Disease Control and Prevention. Syndromic surveillance for bioterrorism following the attacks on the World Trade Center-New York City 2001. *MMWR – Morbid. Mortal. Week. Rep.* 52, 13–15, 2002.
24. Centers for Disease Control and Prevention. Update: Investigation of bioterrorism-related anthrax and adverse affects from antimicrobial prophylaxis. *MMWR – Morbid. Mortal. Week. Rep.* 50, 973–976, 2001.
25. Centers for Disease Control and Prevention. Notice to readers: Smallpox vaccine adverse events monitoring and response system for the first stage of the smallpox vaccination program. *MMWR – Morbid. Mortal. Week. Rep.* 52, 88–89, 99, 2003.
26. Centers for Disease Control and Prevention. Update: Adverse events following civilian smallpox vaccination-United States 2003. *MMWR – Morbid. Mortal. Week. Rep.* 52, 819–820, 2003.
27. Retailliau, H. F., Curtis, A. C., Starr, G., et al. Illness after influenza vaccination reported through a nationwide surveillance system, 1976–1977. *Am. J. Epidemiol.* 111, 270–278, 1980.
28. Pavlin, J. A., Kelley, P., Mostashari, F., et al. Innovative surveillance methods for monitoring dangerous pathogens. In: Knobler, S. L., Mahmoud, A. A. F. and Pray, L. A. (eds) Biological Threats and Terrorism: Assessing the Science and Response Capabilities: Workshop Summary. Washington DC: The National Academies Press, 185–196, 2002.
29. Conrad, J. L. and Pearson, J. L. Improving epidemiology, surveillance, and laboratory capabilities. In: Levy, B. S. and Sidel, V. W. (eds) Terrorism and the Public Health. New York: Oxford University Press, 270–285, 2003.
30. Centers for Disease Control and Prevention. Hepatitis A outbreak associated with green onions at a restaurant – Monaca, Pennsylvania, 2003. *MMWR – Morbid. Mortal. Week. Rep.* 52, 1155–1157, 2003.
31. Walsh, T. Pennsylvania reporting system speeds fight against hepatitis A, November 18, 2003. In: Government Computer News. Available at <http://www.gcn.com/Vol1_no1/daily-updates/24189-1.html>. Accessed on January 23, 2008.

32. Doyle, T. J., Glynn, K. M. and Groseclose, S. L. Completeness of notifiable disease reporting in the United States: An analytical literature review. *Am. J. Epidemiol*. 155, 866–874, 2002.
33. Hinds, M. W., Skaggs, J. W. and Bergeisen, G. H. Benefit-cost analysis of active surveillance of primary care physicians for hepatitis A. *Am. J. Public Health* 75, 176–177, 1985.
34. Tsui, F. -C., Espino, J. U., Dato, V. M., et al. Technical description of RODS: A real-time public health surveillance system. *J. Am. Med. Inform. Assoc*. 10, 399–408, 2003.
35. Lazarus, R., Kleinman, K., Dashevsky, I., et al. Use of automated ambulatory-care encounter records for detection of acute illness clusters, including potential bioterrorism events. *Emerg. Infect. Dis*. 8, 753–760, 2002.
36. US Department of Defense. Annual report, fiscal year 1999, Silver Spring (MD): Walter Reed Army Institute of Research; 1999.
37. Panackal, A. A., M'ikanatha, N. M., Tsui, F. -C., et al. Automatic electronic laboratory-based reporting of notifiable infectious diseases at a large health system. *Emerg. Infect. Dis*. 8, 685–691, 2002.
38. Effler, P., Ching-Lee, M., Bogard, A., et al. Statewide system of electronic notifiable disease reporting from clinical laboratories: comparing automated reporting with conventional methods. *JAMA – J. Amer. Med. Assoc*. 282, 845–850, 1999.
39. M'ikanatha, N. M., Southwell, B. and Lautenbach, E. Automated laboratory reporting of infectious diseases in a climate of bioterrorism. *Emerg. Infect. Dis*. 9, 1053–1057, 2003.
40. Espino, J. U. and Wagner, M. M. Accuracy of ICD-9-coded chief complaints and diagnoses for the detection of acute respiratory disease. *Proc. AMIA Symp*. PMIDI 11833477, 164–168, 2001. www.amia.org/pabs/proceedings/symposia/start.hmtl
41. Begier, E. M., Sockwell, D., Branch, L. M., et al. The national capitol region's emergency department syndromic surveillance system: do chief complaint and discharge diagnosis yield different results? *Emerg. Infect. Dis*. 9, 393–396, 2003.
42. Janes, G. R., Hutwanger, L., Cates Jr., W., et al. Descriptive epidemiology: Analyzing and interpreting surveillance data. In: Teutsch, S. M. and Churchill, R. E. (eds) Principles and Practice of Public Health Surveillance. 2nd edition. New York: Oxford University Press, 112–167, 2000.
43. Chang, M., Glynn, M. K. and Groseclose, S. L. Endemic, notifiable bioterrorism-related diseases, United States, 1992–1999. *Emerg. Infect. Dis*. 9, 556–564, 2001.
44. Rutstein, D. D., Berenberg, W., Chalmers, T. C., et al. Measuring the quality of medical care: A clinical method. *N. Engl. J. Med*. 294, 582–588, 1976.
45. Rutstein, D. D., Mullan, R. J., Frazier, T. M., et al. Sentinel health events (occupational): A basis for physician recognition and public health surveillance. *Am. J. Public Health*. 73, 1054–1062, 1983.
46. Alibek, K. and Handelman, S. Biohazard. New York: Random House, 1999.
47. Garrett, L. Betrayal of Trust: The Collapse of Global Public Health. New York: Hyperion Press, 2000.
48. Miller, J., Engelberg, S. and Broad, W. Germs: Biological Weapons and America's Secret War. New York: Simon and Schuster, 2001.
49. Last, J. M. A Dictionary of Epidemiology. 4th edition. Oxford: Oxford University Press, 2001.
50. Lewis, M. D., Pavlin, J. A., Mansfield, J. L., et al. Disease outbreak detection system using syndromic surveillance data in the greater Washington DC area. *Am. J. Prev. Med*. 23, 180–186, 2002.
51. Stroup, D. F., Wharton, M., Kafadar, K., et al. Evaluation of a method for detecting aberrations in public health surveillance. *Am. J. Epidemiol*. 137, 373–380, 1993.
52. Mullan, F. Plagues and Politics: The Story of the United States Public Health Service. New York: Basic Books, Inc., 1989

53. Mahon, B. E., Pönkä, A., Hall, W. N., et al. An international outbreak of *Salmonella* infections caused by alfalfa sprouts grown from contaminated seeds. *J. Infect. Dis*. 175, 876–882, 1997.
54. Bifani, P. J., Mathema, B., Liu, Z., et al. Identification of a W variant outbreak of *Mycobacterium tuberculosis* via population-based molecular epidemiology. *J. Amer. Med. Assoc*. 282, 2321–2327, 1999.
55. Small, P. M., Hopewell, P. C., Singh, S. P., et al. The epidemiology of tuberculosis in San Francisco – a population-based study using conventional and molecular methods. *N. Engl. J. Med.* 330, 1703–1709, 1994.
56. Roberts, R. B., de Lencastre, A., Eisner, W., et al. Molecular epidemiology of methicillin-resistant *Staphylococcus aureus* in 12 New York hospitals. MRSA Collaborative Study Group. *J. Infect. Dis*. 178, 164–171, 1998.
57. de Lencastre, H., Severina, E. P., Roberts, R. B., et al. Testing the efficacy of a molecular surveillance network: Methicillin-resistant *Staphylococcus aureus*(MRSA) and vancomycin-resistant *Enterococcus faecium* (VREF) genotypes in six hospitals in the metropolitan New York City area. The BARG Initiative Pilot Study Group. Bacterial Antibiotic Resistance Group. *Microb. Drug Resist*. 2, 343–351, 1996.
58. New Jersey Health Alert Network. Available at <http://njlincs.net>. Accessed on January 23, 2008.
59. Snider, D. E. and Stroup, D. Ethical issues. In: Teutsch, S. M. and Churchill, R. E. (eds) Principles and Practices of Public Health Surveillance. 2nd edition. New York: Oxford University Press, 194–214, 2000.
60. Centers for Disease Control and Prevention. HIPAA Privacy Rule and Public Health. *MMWR – Morbid. Mortal. Week. Rep*. 52, 1–12, 2003.