



American Association of
HEALTH PLANS

Testimony

Homeland Security: Improving Public Health Surveillance

**Karen Ignagni
President and CEO
The American Association of Health Plans**

**Submitted to the
U.S. House of Representatives
Committee on Government Reform
Subcommittee on National Security, Emerging Threats,
and International Relations**

May 5, 2003

Good afternoon, Mr. Chairman and members of the Subcommittee. I am Karen Ignagni, President and CEO of the American Association of Health Plans (AAHP). Thank you for the opportunity to be here today to discuss the role of private health plans in the development and operation of regional and national bioterrorism and acute illness surveillance systems. AAHP is the principal national organization representing more than 1,000 health plans which provide coverage for more than 170 million Americans nationwide.

We are excited about the role that health plans can play in national and local efforts to improve America's overall emergency preparedness and response, and protect our homeland from health-related terrorist threats. The Congress, the Department of Health and Human Services, the Department of Homeland Security and other federal, state and local government agencies, as well as the medical and scientific communities, state and local policymakers, and public and private organizations, have been working together to address homeland security issues. A key element of these collective efforts is the integration of all resources that can contribute to the early identification of a bioterrorist event and improve coordination and communication with federal, state, and local public health organizations. Coordination and mobilization of all resources is essential if we are to create and maintain an effective public health infrastructure responsive to potential catastrophic events.

America's health plans are positioned to help advance this coordination of resources because they have unique capabilities to provide real-time data and other relevant information that can be an important part of the development of a national and state emergency preparedness and readiness strategy. These capabilities include:

- Large well-defined populations that allow public health officials to know where illnesses are concentrated (and also where they are not);
- Real-time de-identified data for the early detection of disease clusters, infections or potential biological and chemical exposure;
- Real-time symptom data from health plan nurse call centers;
- Nurse case managers who log valuable information from follow-up medical care, post-hospitalization, health care visits, and home care visits; and

- Rapid-response outbound call technology that can deliver customized public health messages to health plan members, network providers and employers.

My testimony today will highlight the critical importance of strengthening our nation's ability to respond to bioterrorist attacks through effective surveillance systems. I will also review questions that have been raised about passive surveillance systems being prone to chronic underreporting and delays in the receipt of data by public health authorities. Finally, I will discuss the experiences of private health plans that are working with CDC to contribute to the development of early warning health surveillance systems.

The opportunity to strengthen public health surveillance programs

The events of September 11, 2001 and the subsequent anthrax contamination have made the nation keenly aware of the need to be better prepared and responsive to potential future terrorist attacks. The Institute of Medicine's (IOM) Forum on Emerging Infections' 2002 report, *Biological Threats and Terrorism- Assessing the Science and Response Capabilities*, emphasizes the importance of countering bioterrorism with effective surveillance and early detection. Surveillance mechanisms are seen as critical elements in strengthening our ability to respond to a bioterrorist attack. Delays in detection would further spread communicable diseases and prevent or delay the introduction of effective treatment, increase morbidity and mortality, and heighten public fear.

The IOM report stresses that comprehensive surveillance for bioterrorism will require integrating human resources, laboratory resources, and information management in innovative, legal, and acceptable ways that allow for early detection and characterization of threats.

In addition, the Department of Defense identified four key elements of surveillance systems that are needed to maximize patient survival:

1. Facilitating the rapid recognition of a bioterrorist attack;
2. Assisting in determining the site of exposure;
3. Maximizing efficient delivery of targeted (and perhaps scarce) medical countermeasures to the infected population; and
4. Assessing containment and mitigation.

The expansion and improvement of early warning systems for bioterrorism will likely have the additional benefit of strengthening the public health infrastructure for detection of naturally occurring infectious disease outbreaks as well as new emerging diseases. The advantages of this improved public health surveillance is a theme heard throughout the public health community and reinforced by the Director of the Centers for Disease Control and Prevention (CDC), Julie Gerberding, MD, MPH, who commented last year on the demonstrated benefits of bioterrorist planning and funding in improving the surveillance and public health response to West Nile Virus. Such systems can be utilized or easily modified to track and alert public health officials about other infectious disease outbreaks such as Severe Acute Respiratory Syndrome (SARS).

While we know the importance of early warning systems to our nation's domestic readiness effort, there are significant challenges ahead. The General Accounting Office's (GAO) recent report, *Infectious Disease Outbreaks-Bioterrorism Preparedness Efforts Have Improved Public Health Capacity, but Gaps Remain*, suggests that public health surveillance programs, especially those capable of detecting possible bioterrorism attacks, are "inadequate." The GAO's report emphasized that state and local public health authorities rely primarily on passive surveillance systems that are prone to chronic underreporting and significant time lags between diagnosis and receipt of the data by public health authorities. Initiatives underway by public health authorities to develop active electronic surveillance systems have largely focused on hospital and emergency rooms where access to data has been challenging, the number of institutions that must develop customized surveillance procedures is large, and the uncertainties about which hospitals serve specific communities are problematic.

The GAO found that the level of preparedness in states and cities was varied, and generally lacking in terms of regional planning. States and metropolitan areas are focused on their specific populations, but there is little coordination across regional areas or state lines. Since infectious disease (naturally occurring or deliberately spread) knows no jurisdictional boundaries, the lack of regional and/or national surveillance capacity represents a significant gap in our current level of homeland security.

Challenges to improving local, state, federal, and international health data collection and reporting

Infectious disease is mobile, and prior to an onset of symptoms, *invisible*. The recent Severe Acute Respiratory Syndrome (SARS) and West Nile virus epidemics have illustrated the advantage of uniform cross-border and cross-region health data reporting and analysis, and the danger of restricting or limiting that flow. Collaborations on a variety of fronts will be needed to establish “best practices in real-time surveillance” that can be integrated and applied in a myriad of settings required for effective detection of possible bioterrorism events. None of the systems currently being developed are likely to be adequate in and of themselves. The best solution will probably be a “system of systems” that is sensitive enough to detect specific conditions and even small outbreaks.

Collaborations among various levels of government (federal, state and local) and the private sector will help to prevent and provide earlier detection of potential bioterrorist attacks. Active public health surveillance systems designed by the private sector utilizing sophisticated data collection and computerized modeling programs are currently being developed for specific diagnosis and symptoms (e.g., influenza-like illness) and are being rapidly adapted to meet the challenge posed by the threat of bioterrorism. This work can be leveraged to meet the needs of homeland security. There is a necessary tension between the desire for a “uniform” system and the advantages of developing a variety of approaches that will lead to effective options that meet the wide-ranging needs of the international public health community and homeland security, as well as the local public health authority.

Private health plans are working with the CDC to contribute to the development of early warning health surveillance systems

Soon after the tragic events of September 11, we began discussions with our member plans about their skills and experience and how we could leverage that to contribute to public health preparedness. In our fact finding process, it became clear that health plans had a unique set of skills and competencies based on their integrated care coordination systems, large defined populations and comprehensive data sets that could provide a substantial public health benefit. Our community

realized that we should be an important component of an early warning health surveillance system. Much of this information includes coded diagnoses in automated medical records, information collected by telephone assistance/triage centers, and other data (automated vital signs, encounter clinician notes, laboratory data, etc.). This type of information is sufficient to identify, within a day, at least some new clusters of respiratory, gastrointestinal, neurological, and other illnesses experienced by health plan members.

Once our community identified its potential contribution to homeland readiness, we began discussing how we could help support the work of the CDC. This resulted in the collaboration of several health plans and AAHP with CDC to create a national bioterrorism syndromic surveillance demonstration program that utilizes existing automated data maintained by health plans covering more than 20 million people in 50 states. The primary goal of the program is to develop and implement standards, protocols, infrastructure, and analytic tools for detecting and reporting unusual geographic and temporal clusters of symptoms or complaints of acute illness that might represent the initial warnings of a bioterrorism event. The initial work to develop and evaluate the effectiveness of an early warning health surveillance system is being funded through a grant from CDC.

The national demonstration program involves AAHP, and four health plans or physician groups – Harvard Pilgrim Health Care/Harvard Vanguard Medical Associates (Massachusetts), HealthPartners (Minnesota), Kaiser Permanente Colorado, and UnitedHealthcare’s nurse call center, Optum. Through additional funding from the Texas League of Health Departments, Scott and White Healthcare System (Texas), and the Austin Regional Clinic (Texas) are participating in the demonstration project and are included as additional sites providing data to the project.

The demonstration program includes a rapid response capability to identify unusual clusters of symptoms or illness from daily encounters, to notify the right public health officials of these clusters, and to facilitate the ability of public health officials to obtain detailed clinical information about specific cases when needed. Health plans report only aggregate de-identified data to the surveillance system – counts of episodes of illness or symptoms within specific geographic areas – thus providing maximum protection of patient confidentiality. In cases where unusual clusters are identified, the state or local public health team will decide if additional information is needed. This

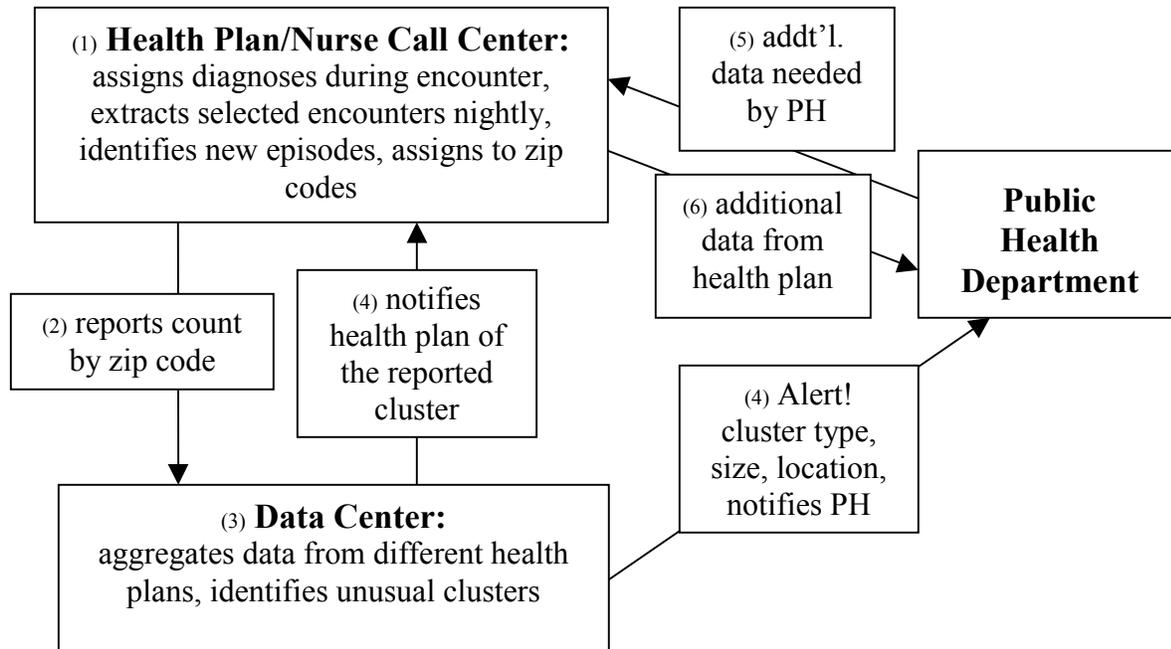
system is being developed in a manner that will facilitate the participation by other health plans and medical groups that possess real-time encounter level information.

Diagnoses recorded during routine ambulatory care, including office visits and nurse telephone triage calls, may provide important information on disease outbreaks before their occurrence is detected through emergency room visits, or hospitalizations. For instance, evidence suggests the increase in winter respiratory illness in a community can be detected two weeks earlier in the ambulatory setting than through hospital admissions. The operation and use of nurse telephone call centers may dramatically improve the early detection of bioterrorism and infectious diseases. Professionally staffed call centers provide symptom triage, health information, case management, and care coordination for health plan enrollees. These call centers are local, statewide and national in scope and operate extended hours – many operating twenty-four hours a day, seven days a week. By utilizing the available ambulatory care and nurse call center data, health plans are in a unique position to identify the earliest indicators of sentinel bioterrorism events or emerging infectious diseases.

Health plans participating in the study disclose health information to a research data center which in turn analyzes the information and identifies unusual clusters of medical events, such as a concentration of a specific disease or illness in a geographic area. This system is based on one created by investigators who have dual appointments at Harvard Pilgrim Health Care/Harvard Vanguard Medical Associates and Harvard Medical School, in collaboration with the Massachusetts Department of Health through an earlier bioterrorism preparedness grant from the CDC. This demonstration initiative takes advantage of the health plans' ability to use their existing automated data systems to rapidly identify health plan members that may be part of an important disease cluster. Typically, each night, a computer program at the participating health plan extracts the clinical encounters for the preceding 24 hours that meet any of more than a thousand specified criteria, such as cough, fever, or a rash. These criteria and their associated disease groupings (syndromes) were developed in collaboration with the CDC and the DOD. The system then eliminates visits for illnesses that had previously been identified, and links the relevant information about the new illnesses to the individual's zip code. The health plan's information system then sends a daily report to the data center using secure Internet communications.

The disclosure of information to the data base is pursuant to research waivers obtained from health plan Institutional Review Boards (IRBs) or privacy boards. The privacy rule allows disclosure of health information for research projects either by written authorization or by a waiver of the authorization requirement approved by an IRB or privacy board. This daily report lists only the aggregate count of new illnesses or symptoms in each zip code, thereby affording important privacy protections. The data center combines reports from different health plans and searches for unusual clusters of different syndromes (respiratory, gastrointestinal, etc.). The system takes into account factors such as seasonal occurrences, day of the week, and other factors that influence the number of complaints and cases cared for on a particular day. It also takes into account past information about patterns of illness and health care delivery in each zip code. Because the number of health plan members in each area is known, it is possible to adjust the observed counts of the new illnesses and consider the number of people who are at risk for being affected. Because this work is automated, many thousands of possibilities are analyzed. It would not be possible to do this cluster detection work manually because the numerous mathematical computations would be too difficult.

The decision rules built into the automated system allow the data center, a research unit of Harvard Medical School in the Brigham and Women's Hospital, to determine whether the number of cases is sufficient to warrant notifying the relevant health department about the type, size and location of the cluster. The data center uses aggregate information to inform public health departments that, for example, there are four people with pneumonia in a particular zip code. In general, the disclosure of aggregated health information by zip code is not identifiable information subject to the privacy rule. The public health department is informed about who to contact at the health plan to obtain additional information about individuals who are part of the cluster, and their illness. The data center will also notify the health plan about the information reported to the public health department and direct it to review the relevant clinical records, which are always stored and maintained at the health plan.



These communications between the public health departments and the health plans are covered by existing public health reporting laws and are consistent with the confidentiality protections of the HIPAA privacy rule. This enhanced collaboration between health plans and public health organizations builds on existing relationships and a long history of reporting information to public officials when a public health problem is identified. Because of this new early warning health surveillance system, we have the ability to identify illnesses that otherwise would have been missed and report them much earlier.

In summary, the new system has several valuable features from a public health perspective:

- health plans provide coverage to over 170 million Americans; many have some electronic information, e.g. nurse call centers, that could be useful for this type of surveillance;
- the source population will be known, which allows greater flexibility for detecting illness clusters than is possible when only the affected individuals are known, as is the case for most systems based on emergency room visits or hospitalizations;
- it is relatively simple to modify the syndrome definitions or to create new syndromes when new potential threats may arise, because the health plans retain diagnosis-level data and other information that may easily be added (for example, we are now working with CDC to modify the system to help identify SARS outbreaks);

- it will use electronic information that is already collected by the medical practices, health plans and call centers as part of routine operations, which is important for any system to be functional long term;
- because the information is available electronically, the incremental costs to extract data of interest, and make it available to public health agencies, will be small;
- because the system uses medical record information, it will be more detailed and informative than other types of automated data, such as billing records; and
- importantly, the system conforms to members' expectations and to the HIPAA requirements protecting confidential personal health information – using information as sparingly as possible to accomplish the public health mission.

Health plans have been at the forefront of population-based health care and are taking a leadership role, working with public health agencies to construct an effective early warning, detection system that – when coupled with the state and local public health departments – will help protect our country from emerging infectious diseases and potential bioterrorism agents.