September 19, 2003

Pattern Recognition

By Katherine McIntire Peters
kpeters@govexec.com

Detecting a bioterror attack may be almost as difficult as responding to one.

In 1999, a medical resident at the Walter Reed Army Institute of Research in Silver Spring, Md., wanted to find a way to detect an outbreak of disease before the disease was actually diagnosed in a laboratory. If public health officials learned about a surge in health complaints—for instance, if a lot of people who worked in a particular ZIP code started developing coughs or fevers—they would have a head start in containing an outbreak, even before a disease was definitively diagnosed.

To test his theory, the resident began collecting and analyzing the billing codes reported to insurance companies when a person visits a doctor. The Defense Department had begun using the codes (called ICD-9 codes for International Classification of Diseases, 9th Revision) two years earlier throughout the military medical system. ICD-9 codes, of which there are tens of thousands, had never been used for disease surveillance, says Lt. Col. Julie Pavlin, who oversaw the project as chief of the Department of Field Studies at Walter Reed. They were used mostly for record keeping and billing purposes.

"This database already exists, and it does have this diagnostic information in it. The question was, 'Can we get that information and use it for surveillance?'" Pavlin says. The resident found he could pull the data from a central server at the Defense Department, so they began by looking at the Washington area, since it was considered a high-threat area for bioterrorism, as well as a data-rich area with its high percentage of military personnel and retirees.

The Electronic Surveillance System for the Early Notification of Community-Based Epidemics, or ESSENCE, pulled preliminary medical assessment data from more than 100 Defense Department primary care clinics and facilities within 50 miles of the White House.

"This information is supposed to be entered at the time of the patient visit," says Pavlin. "It's safe to imagine that if you've got two minutes to see a patient and they come in and they've got a cough, you don't know why they're coughing. They could have tuberculosis, they could have pneumonia, they could have any number of things—it could be from smoking."

To make the data useful, they grouped the ICD-9 codes into broad categories reflecting particular symptoms, such as those for respiratory illness or gastrointestinal illness.

The results were mixed, she says. Nonetheless, the results were promising enough that in 2000, the Walter Reed researchers joined forces with researchers at the Johns Hopkins Applied Physics Laboratory in Laurel, Md., who were working on a similar project for the Maryland Health Department. The two groups established data-sharing agreements and started examining the ICD-9 codes in the Washington metropolitan area.

In 2001, the team received funding from the Defense Advanced Research Projects Agency to expand its analysis to other existing data sources, such as pharmacy records and school absentee records, in a joint military-civilian program called ESSENCE II. The goal of the program, says Pavlin, is to create a database that integrates information from disparate sources across the region

into a composite picture that detects meaningful changes in health status as those changes occur.

LOSING THE PAPER TRAIL

Historically, public health surveillance has been a slow, deliberate, paper-intensive business. Patients seek care from physicians in private practice, clinics or hospitals, where tests are ordered and specimens are drawn and sent to laboratories for analysis. Laboratory personnel analyze the specimens and report their findings back to physicians; in those cases where public health may be affected, such as when communicable diseases are diagnosed, public health departments are notified. Records are kept in paper files and are difficult to share.

One of the many drawbacks to the system is that microbes can move far more quickly than most health care bureaucracies. Although physicians routinely report suspected cases of communicable diseases, such as tuberculosis, or more recently, Severe Acute Respiratory Syndrome (SARS), directly to public health officials without waiting for diagnoses, the system is hardly foolproof.

"Of course that's a terrible system," says Dr. Claire Broome, senior adviser to the director of the Centers for Disease Control and Prevention. "Doctors don't get paid to do [surveillance]; they don't have time to do it. We've done studies that show how incomplete that is. But it is important to recognize that at least for the urgent notifications—a clinician thinks something is going on and phones the health department—that's still a critical system, and it works and it's important," she says.

By the mid-1990s, concerns about the public health threats posed by emerging infections, both those occurring naturally and those engineered by humans, was growing. Fear of bioterrorism grew with the accumulation of evidence from former Soviet military scientists and U.N. weapons inspectors in Iraq. While the military has a long history of tracking disease and working to mitigate its effects on troops, civilian health officials also were growing increasingly concerned about the potential threat.

At the same time, states—the primary collectors and purveyors of public health data—were having a tougher time tracking and reporting information on infectious disease to federal authorities.

"Every time we applied for a grant and got federal money, if [the CDC] had software that went with it, you then were obligated to use it. So then you had a separate software program for tuberculosis, another one for sexually transmitted diseases, a third one for HIV/AIDS, a fourth one for just generic reportable diseases," says Joel Hersh, director of the Pennsylvania Bureau of Epidemiology.

In late 1998, the CDC developed what it called a public health conceptual data model—essentially a blueprint for integrating the various data collected in the public health arena. The CDC then invited states to apply for grants to help fund their adoption of the new model. The idea was that states would be able to develop technical solutions that fit their unique circumstances. At the same time, states would gain the ability to integrate their data collection with a National Electronic Disease Surveillance System (NEDSS).

Like those in most other states, Pennsylvania health officials applied for and received federal grants to begin bringing their disease-reporting systems into compliance with the new, integrated model established by the CDC.

Pennsylvania health officials were able to supplement the CDC grants with state funds, which

the health department used to hire Deloitte Consulting to build a Web-based application of the CDC model. PA-NEDSS, as the state's system is called, allows health care providers and clinicians to report diseases, and suspected cases of disease, as soon as they are discovered. "Physicians, hospitals and laboratories are able to go in through the Web, in a secure application, and report what they used to report on paper," says Hersh.

SECURITY AND PRIVACY

Pennsylvania took PA-NEDSS live in July 2002. Since then, the state health department has received more than 100,000 electronic reports through the system. Debbie Sills, a partner with Deloitte Consulting, the prime contractor responsible for the system's design and implementation, says that after the Sept. 11 terrorist attacks and subsequent anthrax attacks, state leaders increased both the pace and the scope of disease surveillance.

"They quickly realized this was a vital element of their bioterrorism plan, and they asked us to be more aggressive about implementation and rollout, training staff and getting hospitals online," says Sills.

The biggest challenge was designing a system that could accommodate a broad range of users, including physicians in emergency rooms, doctors in practices, laboratory technicians, public health investigators in the field and epidemiologists. "There's literally thousands of users and they have lots of levels of capability as relates to their understanding of disease reporting and also to their understanding of the use of technology," Sills says.

Another factor complicating implementation was security. "We're talking about millions of medical records in this database, and the security and privacy are paramount," Sills says.

"There is a very elaborate security system that covers roles and responsibilities of various users—what data they can and cannot see, what data they can update, what they can view only, and so on. In addition to that, there is a very tight security system to provide access."

The new reporting system represents a revolution in disease surveillance, says Pennsylvania's Hersh. Before laboratory technicians and physicians began providing electronic reports under PA-NEDSS, they filed paper reports by mail with the state health department in Harrisburg. The reports were sorted by hand and then re-mailed to disease investigators across the state for follow-up reporting.

"From the point the doctor drew the specimen and sent it to the lab, it might be three to four weeks before our investigator would receive it in the field. By the time it gets to the poor investigator, other people may have become infected unknowingly," says Hersh.

"Because [PA-NEDSS] operates in real time, as soon as we get the report, it's immediately available to the investigator, so there's never more than an overnight delay," Hersh says. The NEDSS system hasn't been fully embraced by all users, however. For laboratories, the transition away from paper records has probably been easiest.

But for physicians and hospitals, the reporting requirements are more complex and time-consuming and, consequently, they have been less enthusiastic, Hersh says.

While he agrees there is a long road ahead in fully integrating the entire healthcare community into the online system, he believes Pennsylvania's experience can serve as a model for other states. "Part of what we've been hacking away at in terms of the iceberg is that this has been a paper system for a hundred years," he says.

NEDSS is a particularly effective tool for laboratory reporting, says the CDC's Broome, which is important because laboratories are the source of a large portion of communicable disease diagnosis and reporting.

"We've developed a set of standard messages that [enable] the big clinical laboratories to transmit electronic messages to state health departments when they have a case of hepatitis or meningitis or other conditions of public health importance. NEDSS basically is the message format, the message security, and it also provides an in-box in public health to receive the information and analyze it and track follow-up," Broome says.

TRANSFORMING SURVEILLANCE

As much of an improvement as NEDSS is over manual reporting, it doesn't change the fact that doctors, nurses and other clinicians must initiate a report in the first place. Because many of these people are already overwhelmed by the demands of an over- burdened health care system, this is a significant drawback to the way diseases are reported.

"The thing that really we think is transforming the process is having information, which is stored electronically in a hospital or a clinical laboratory, automatically generate a notification via standard electronic message when a laboratory test identifies a condition of public health importance," says Broome.

Under a program called the Healthcare Collaborative Network, health officials are trying to expand the range of clinical data sources from which public health data might be automatically captured, such as hospital pharmacy records and patient discharge files. This is particularly important for reporting conditions that wouldn't necessarily be identified by a clinical laboratory, and for surveillance aimed at assessing the quality of care being provided.

The Healthcare Collaborative Network is a demonstration program being implemented by IBM at three hospitals, the CDC, the Food and Drug Administration and the Centers for Medicare and Medicaid Services. "This complements NEDSS in the sense that it lays the foundation for how information flows," says Bruno Nardone, the IBM program executive responsible for implementing the network.

The network is designed to turn the collection of health data into an automatic, electronically updated endeavor that places no new burdens on health care workers. By sharing data automatically among network participants, the opportunities for health monitoring, quality assurance and disease surveillance grow enormously. Thus far, the greatest challenges in implementing the network have been not been technical, but legal—ensuring that privacy of patient records is maintained, says Nardone.

Dr. Marc Overhage, a physician at Wishard Hospital in Indianapolis, one of the participating hospitals in the demonstration, says the promise of the network far outweighs the challenges of developing it. Because data is captured automatically, it doesn't present an additional reporting burden for doctors and nurses. By collecting and analyzing data related to patient treatment and outcomes, hospitals and physicians can significantly improve the quality of care they provide.

In July, the National Library of Medicine, part of the Health and Human Services Department, took a significant step in establishing a common electronic medical records system in the United States, much like the electronic data system banks use to transmit financial data between institutions. The library signed a $32.4 million, five-year contract with the College of American Pathologists to permanently license the college's standardized medical vocabulary and offer it

free of charge to health care providers across the country.

“It’s hard to overstate the significance of this,” says Dr. John Mattison, assistant medical director for clinical systems with the Southern California division of Kaiser Permanente, one of the largest health care networks in the country. The contract ultimately will affect everything related to medical record keeping, from bioterrorism-surveillance programs to the quality of care patients receive, Mattison says.

The standardized vocabulary, the Systematized Nomenclature of Medicine-Clinical Terms, known as SNOMED CT, is considered to be the world’s most comprehensive clinical terminology database, with terms for more than 340,000 medical concepts. The licensing agreement will allow health care providers, hospitals, insurance companies, public health departments, medical research facilities and others to incorporate the highly specific terminology into their electronic information systems.

The Institute of Medicine also is designing a standardized model of an electronic health record, which, once approved by the health care standards development organization known as HL7, would be shared, free of charge, with all components of the U.S. health care system. The model is expected to be ready next year, and will provide a crucial mechanism by which physicians’ offices, insurance companies, hospitals and others can all communicate electronically.

“We will see much more rapid advances in the knowledge base of medicine, we will see much more effective care delivered. If the patient elects to have that information shared—this doesn’t violate any security at all—then the information can be translated from one system to another, from one country to another, in a way that it’s understandable and reproducible so that it’s very accurate and very reliable, and that today is very difficult to achieve. It allows for real portability of records, but still within the framework of confidentiality,” Kaiser Permanente’s Mattison says.

Mattison anticipates that the licensing agreement will result in important advances in public health and even the early detection of bioterrorist attacks.

“When it comes to something like detecting bioterrorism, for example, if there’s two cases that show up in one emergency room with a set of symptoms, and another one 100 miles away, and five more in the Midwest, and six in the South scattered around different hospitals, nobody’s going to be able to identity that those in fact represent a cluster, and perhaps represent some bioterrorist event,” Mattison says.

“Whereas, if that information is coded in SNOMED, and rolled up into a surveillance [program], then early detection is not only plausible but likely.”