How Bioterrorism Became an HIM Issue

Save to myBoK

by Dan Rode, MBA, FHFMA

Bioterrorism is not a subject that people would normally relate to HIM. Yet, since the first anthrax letter was discovered on October 4, 2001, there have been discussions around the country that will directly affect HIM for many years to come.

Bioterrorism spotlighted public health and public health data. While the debate on the public health response to bioterrorism is probably more pertinent to those in Florida, New York, New Jersey, and Washington, DC, the relevance of this discussion will affect all US citizens and certainly raise the profile of public health in the context of our healthcare information infrastructure and readiness.

The anthrax events revealed our lack of a public health communication system as many people asked, "Who do you report an incident to?" When the letters were found, there was a variety of organizations to contact, including police, postal authorities, security offices, and more. However, when individuals presented themselves to healthcare facilities with common symptoms, whom to query was unclear. As media coverage of the letter incidents and anthrax cases increased, much of the query process was directed to the Centers for Disease Control and Prevention (CDC). It was the media coverage itself that alerted many healthcare providers to the threat and description of this biological agent. Now the questions are: will there be another bioterrorism event? What should healthcare providers do when it happens?

This is not a new story in public health. There have been other diseases and outbreaks that have needed skilled resources directed to various populations. However, because the recent public health communication problems were associated with bioterrorism and thus in a media spotlight, they have drawn attention to the need for a professional response to similar diseases or outbreaks, such as Legionnaire's disease, the West Nile virus, or AIDS.

As information professionals addressed this issue, they focused on what could be done immediately. Three main needs were identified:

- a standardized communications mechanism that will allow healthcare providers to report and query public health resources
- a way to use technology to both alert and educate healthcare professionals about a threat
- a method of reviewing certain aspects of collective health information on individuals to determine if there is a public health threat that warrants follow-up and reaction

It's Time to Connect the Healthcare Community

As information technology professionals reviewed these issues, they immediately considered the Internet a possible solution. The IT community was surprised to learn that there is still a very large number of healthcare facilities and professionals that do not have access to the Internet or e-mail. This deficiency will have to be addressed by both the government and healthcare providers. The IT community will also need to address who is in this network and where messages should be sent to direct resources in the most appropriate manner.

As HIM professionals know, communication is most effective when it is uniform and standardized. But experience has also taught us that uniformity and standardization take time. To circumvent this delay, many IT and healthcare professionals have suggested using a form in intake areas of healthcare facilities that could be e-mailed to designated public health authorities when a questionable encounter occurs. This is a short-term solution.

For the long term, the healthcare industry must address uniformity and standardization. The value of consistent and uniform coding is very apparent, as is the value of a coding system that is uniform across sites of service such as emergency rooms, clinics, physician offices, and more. Additionally, it's clear that when such information is collected, its value is increased when it

can be compared nationally and internationally. This insight has spotlighted the variance between ICD-9-CM and ICD-10 coding systems, when data in the US needs to be compared with data in the rest of the world.

Similarly, signs and symptoms and other values in coding systems that have been ignored for reimbursement purposes take on new importance. Initially, the discussions surrounding such communication focused on a physician-public health exchange. Now, they are recognizing the value of using information professionals to collect and code all the encounter information for transmission to the public health authority.

The October anthrax outbreaks raised concerns about the identification of disease when it first presents itself, especially in this era of interstate and international travel. Obviously, alerts can be issued through the media. However, linking all providers to the Internet improves the situation because the sender can uniformly communicate to providers without a third-party interruption. E-mail presents a means of pushing a message to the healthcare provider community and additional details, signs and symptoms, education, and instruction can be either communicated or available on an appropriate Web site.

Some IT professionals also suggest sending an electronic data set that could be immediately added to the provider's intake "electronic form." Then, notable signs and symptoms would raise a red flag at the provider site indicating a potential case or encounter should receive additional follow-up. Through the use of coding, such data sets could be sent out consistently.

Facilitating Ongoing Data Collection

The first two approaches presume that there is an encounter with a patient that dictates communication with public health authorities, or an outbreak or activity that dictates that public health authorities contact healthcare providers. But what happens before that? How do public health authorities determine that a situation needs their attention? If the first case of anthrax had not followed September 11th's tragic events, would it have been identified?

IT and public health professionals are now looking at ways to take the public health pulse. One solution is the ongoing collection of certain healthcare signs, symptoms, and diagnoses, along with certain demographic data, that are uploaded onto a public health network. Such information would be collected and analyzed electronically to trigger an alert that a public health event that needs attention might be happening in one or more locations. For example, a particular area might suddenly have a significant increase in the number of respiratory cases or rashes appearing at healthcare provider sites. Analysis at a state level might alert authorities to some local outbreak, or at a national level, there might be notice that the same symptoms are mysteriously appearing in New York, Florida, and the District of Columbia. The system might then request that some additional information might be collected, such as occupation, recent travel, or other data.

Another alternative is that such signs and symptoms might even be entered by individuals as part of a daily exercise that includes entering and sending (via the Internet) daily physiological data and complaints, by laboratories sending summaries of test outputs, by pharmacies sending inventory turnover levels, and by mechanical devices sending environmental data from various communities.

Always Essential: Uniformity and Standardization

A considerable amount of the discussion on bioterrorism has been very similar to the dialogue on medical errors: medical data must be collected in a uniform manner using standards to ensure consistency and provide the ability to compare data and recognize trends. These conversations have highlighted the need for improving diagnostic coding by adopting ICD-10-CM standards and the need for standardized vocabulary for the collection of other data. These are issues that AHIMA has stressed consistently over time.

The bioterrorism discussions have also examined issues raised under HIPAA for uniform transactions and the need for a common healthcare individual identifier. The uniform transaction model in HIPAA could lead the way for either using the HIPAA transactions to collect data or for a new transaction that would collect the initial diagnostic information discussed above. The uniform ID is the only way to trace individuals from location to location, which provides more privacy than if an individual's name, address, and other data are sent. This latter recommendation will be debated for some time and requires considerable education of the public and policy makers.

These discussions have not been undertaken to condemn the existing public health agencies but rather to strengthen the information infrastructure by responding to two main questions. First, what type of public health infrastructure should be built and who should pay for it? Obviously, there are local, state, and national needs for such an infrastructure that will also include all healthcare providers and will include the attributes discussed above. Second, where in the structure are decisions to be made?

Where HIM Is Needed

In the end, it boils down to data—in this case, healthcare data. Some of this data currently exists but how it is collected and communicated is yet to be determined. Some of the non-standard data is yet to be agreed on and may need the interpretation of HIM professionals. Clearly, HIM involvement will be necessary for the system and infrastructure to agree on nomenclature and to facilitate education and adoption of a new diagnostic coding system. HIM professionals will need to be involved with how data is collected, interpreted, stored, and communicated. As such, HIM professionals also need to be involved in local and national discussions on how this infrastructure will be built and how data integrity, quality, and privacy will be maintained.

HIPAA: Another Data Standard Debate

At press time, Congress is discussing a potential delay in the implementation of the HIPAA administrative simplification regulations. Whether the privacy regulations will be part of the delay has yet to be determined. Whether the currently anticipated regulations will need to be in place is also under consideration.

Most of those groups seeking delay are concentrating on the transaction and code sets regulation. If Congress acts, the delay will probably be limited to one year. Or Congress may continue with the current deadline of October 16, 2002, for the transactions and code sets, or simply put the issue aside in favor of more pressing business. Part of the problem is that congressional representatives are getting mixed messages from their constituencies regarding HIPAA readiness, which leaves them at the mercy of a few very powerful lobbying groups.

There are alternative pieces of legislation in circulation that suggest if a delay is given, it will be the final delay. Otherwise, covered entities, especially providers, will be penalized. This is an interesting twist because health plans are supposed to be primarily responsible for transactions. No matter what happens, two messages to healthcare providers are clear: do not delay implementation of the transaction and code set rules. If there is no extension, the due date for providers essentially remains October 16, 2002. If there is a delay, there is still a limited time for implementation and lack of a strategic plan for implementation could mean that deadlines will not be met. Additionally, the longer the rule takes to implement, the longer the advantages of HIPAA will kept at bay.

The second message is also clear: Congress needs to be kept current on these and many similar issues if they are to make wise decisions. Communication from healthcare professionals is as important as communication from healthcare professional associations. If the AHIMA Policy and Government Relations team can help, let us know.

Dan Rode *(dan.rode@ahima.org) is AHIMA's vice president of policy and government relations.*

Article citation:
Rode, Dan. "How Bioterrorism Became an HIM Issue." *Journal of AHIMA* 73, no.1 (2002): 14-17.