Biosurveillance
Background Briefing
Privacy and Security of Biosurveillance Data

Office of the National Coordinator for Health Information Technology

February 24, 2006

The following information has been provided to you by the Office of the National Coordinator and is a synthesis of data collected from collaboration with the co-chairs, expert members of the community, and other workgroup members. This information should be reviewed and factored into the decision-making process at the February 24, 2006 Biosurveillance workgroup meeting. The meeting should focus on deciding upon recommendations that must be made to the Secretary and the American Health Information Community at the March 7, 2006 meeting.

Charges for the Biosurveillance Workgroup

- **Broad Charge for the Workgroup:** Make recommendations to the Community to implement the informational tools and business operation to support real-time nationwide public health event monitoring and rapid response management across public health and care delivery communities and other authorized government agencies.
- **Specific Charge for the Workgroup:** Make recommendations to the Community so that within one year, essential ambulatory care and emergency department visit, utilization, and lab result data from electronically enabled health care delivery and public health systems can be transmitted in standardized and anonymized format to authorized public health agencies within 24 hours.

Background Information

Data from clinician encounters is very important to public health authorities for the purposes of biosurveillance. Critical in the use of these data are the needs for protecting patient privacy and supporting authorized public health investigation of critical health events. This options document describes an approach and some related issues regarding both patient privacy and public health needs.

Although HIPAA allows for named reporting of appropriate public health data, many are concerned about protecting the needs of protecting patient privacy. HIPAA "de-identification" relates to protecting patient privacy in data used for public release and other purposes such as scientific research. Some of these data, such as general localizing information, are critical for public health to establish that an event is occurring and how it may threaten the general population. So while full HIPAA de-identification, may provide maximum protection from a privacy and security prospective, it makes it virtually impossible for public health authorities to have information needed to identify, monitor and respond to public health emergencies.

At the other end of the spectrum, public health authorities, at times, get named data as required by state law to ensure to allow follow-up on notifiable diseases. In the context of biosurveillance use of health care data, a significant amount of public health value can be derived from data that do not include patient names or medical record numbers and since many are concerned about the use of named data in this type of monitoring, most do not use named data for these broader biosurveillance purposes

Since the specific charge endorsed by AHIC (the full Committee) already specifies that data from electronically enabled health care delivery and public health systems can be transmitted in standardized and anonymized format to authorized public health agencies, the work group needs to consider an acceptable approach to provide anonymized data in developing recommendations to the Full Committee.

Use of a Randomized Data Linker

An approach that is now used to balance the privacy and public health needs, is to not include direct patient identifiers in the data reported for these biosurveillance, but to include a randomized data linker that is meaningless to recipients of the data, but can be used to go back to the original data provider to support appropriate, authorized public health follow-up. Advantages of this approach included that public health does not need direct patient identifiers to carry out a number of public health functions, privacy issues are largely addressed, and the ability for appropriate public health investigation is largely preserved. Issues with the data linker approach include adding a step for public health organizations that must have access to named data (they need to present themselves as an appropriately authorized public health agency and request that additional information from the original data provider).

Issues associated with the use of a randomized data linker include specification of the level at which the data linker is consistently used in data reporting: is the same data linker used for all data concerning a patient coming from a data providing organization, just data related to one particular patient encounter, or even just one lab result or data element.