Emergency Response Data Exchange

April 22, 2002

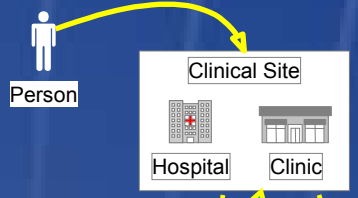
Tim Morris

Centers for Disease Control and Prevention

Information Exchange

- Who can send and receive information?
- What information is exchanged?
- When is information exchange between specific partners appropriate or required?
- How is information formatted and transported?

Anthrax: Clinical Case



Patient presents with Anthrax symptoms at clinical site

Federal response entities notified

notified

State and Local Public Health Departments

Centers For Disease Control and Prevention (CDC)

Federal response entities

Case data sent to State Health Dept. and forwarded to CDC with request for assistance

d to

state and CDC

Specimen sent to Laboratory Response Network lab for confirmation

Field Investigation Team

Field team reports findings back to state or local health dept.

Lab

Exposure cohort identified and intervention begins

Environmental specimens sent to lab with report back to field team

Response teams identify source of exposure

Response Partners

- State and local health departments
- CDC
- FDA, USDA, FEMA, EPA, other federal agencies and local counterparts
- Department of Homeland Security
- Department of Health and Human Services
- Federal and local law enforcement
- Hospitals, clinics and other local care delivery facilities
- Commercial vendors and contractors

Information Types

- Cases, contacts and exposure cohorts
- Laboratory orders and results
- Interventions
- Environmental data
- Spatial data
- Health alerts
- Recommendations

Emergency Response Laboratory Routing Example

Routing Requirements

- Public Health entities might exchange data with any Laboratory Response Network lab
- Public Health entities might exchange data with entities outside their jurisdiction
- Default routes must be supported
- Temporary routes should be easily configurable for creation during events

Routing Infrastructure

- Information flow in emergencies must be close to real time
- Emergency data exchange partners may not be the same as routine partners
- Same network should be used for routine and emergency data exchange
- Collaboration agreements may not always be in place for emergency data exchange
- Network must support dynamic registration of new nodes
- Clients must support dynamic discovery of new nodes and services
- Network must support authentication across multiple security boundaries with single set of credentials

Interoperability

- Physical
  - Transport – ebXML
  - Security/encryption – PKI
  - Directory services – LDAP
  - Service repository
- Semantic
  - Terminology – LOINC, SNOMED etc.
  - Formatting – HL7 version 2.x, 3
  - Parsing

Open Issues

- Routing
  - State and local laws governing data
- Authentication
  - Central authority for credentials
  - Standard interfaces for authorizations
- Infrastructure
  - Broad implementation of standard transport protocols
  - Implementation at state and local level
  - Vocabulary maintenance
- Identifier namespaces
  - Laboratory specimen accessioning
  - Case identifiers
  - Maintaining context across multiple clients

Keys to Success

- Implementation of standards
- Discovery and implementation of routing policy and procedures
- Local infrastructure expansion
- Available expertise for state and local support
- Use of central authority for authentication credentials and identity binding