NEDSS SYSTEMS ARCHITECTURE
Version 2.0, April 15, 2001

The NEDSS Systems Architecture is built around recognized national standards, *de facto* commercial standards that are not tied to particular vendors, and the use of Internet technologies for information interchange. Standardized modular elements are being emphasized in order to facilitate the use of commercial software platforms, to minimize proprietary commercial applications that cross element boundaries, to prepare for module by module element exchange as new technologies are developed, to facilitate technology sharing, and to strive for the rapid exchange of high quality, comparable data.

Fully developed systems will have all of the NEDSS systems elements, and in addition, will have the elements functioning well as an integrated whole.

NEDSS Systems Elements:

a. Conduct and support web browser-based data entry and data management

Functional description: This element will involve developing secure, web browser-based data entry and management capacity for use inside and outside of health departments. Browser-based data entry will be used for data input and results reporting inside of health departments, between local health departments and state health departments, for reporting from and to other sources (e.g., infection control practitioners, small laboratories) and for case management. Sites will have the ability to develop and refine their own systems, but will also be able to incorporate into their web systems web forms and application server code representing public health reports developed by the CDC and others as part of coordinated surveillance systems (e.g., national notifiable diseases reporting, selected EIP activities, and others). Case management tools will be used across categorical program data to develop an integrated, patient-centered design.

Technical description: Web browser-based data entry will be developed using commercial application server technology as part of a multi-tiered web development system using open-platform web servers (e.g., Apache, Microsoft's IIS, Netscape) running on Windows NT / 2000, LINUX or UNIX and supporting generic web browsers (HTML 3.0+ / Java). The web server, the application server and the database server will be separate tiers of this system. Web application servers (e.g. those made by Silver Stream, BEA, IBM and Microsoft) can speed the development and upkeep of web input and management systems. JavaScript for field-based data validation in the browser and EJB, CORBA, or DNA (DCOM) components on the

server can be implemented for application logic (please see element #e). Application servers, regardless of physical platform will be able to run shared JAVA code. Data delivery to an associated database will use ANSI standard SQL and ODBC or JDBC connectivity. Security over the Internet will be implemented using a Secure Sockets Layer (SSL) capable server and industry standard client certificates or token-based for authentication and selective authorizations. Firewalls will be necessary to protect accumulated data (please see element #h).

b. Accept, route and process electronic HL7 messages containing laboratory, clinical and public health content.

Functional description: This element involves developing the capacity to dynamically accept, import, route to other recipients, and process incoming electronic messages in HL7 format which use the LOINC and SNOMED coding standards. These messages will come, for example, as result reports from local clinical laboratories or emergency departments, from HMO's, from CDC laboratories, or as pertinent information from other public health jurisdictions (e.g., in the setting of multijurisdictional outbreaks). Efforts to initiate public health electronic laboratory reporting with clinical care sites and labs will be encouraged. NEDSS Charter sites and some NEDSS Element Development sites will also develop infrastructure to support XML data exchange, which will provide the message infrastructure for HL7 Reference Information Model (RIM) content.

Technical description: Many laboratory and clinical systems now transmit HL7 version messages. Messages will be dynamically received, processed and, as appropriate, routed to other organizations or stored with either a dedicated interface engine or HL7 message and translation software components running on Windows NT / 2000, LINUX or UNIX servers. The ability to translate and manipulate LOINC and SNOMED codes and to map local lab codes into these standards will be important. Application logic to perform data validation, to queue data reports for completion and to initiate the completion and submission of full case reports will be performed using EJB, CORBA, or DNA (DCOM) components (please see element #e).

c. Implement an integrated data repository.

Functional description: The developed data repository will be integrated (i.e., contain data from multiple state-based and CDC categorical programs), patient-centered where appropriate (i.e., where reporting information is about a person, such as in surveillance case reports), will implement the Public Health Conceptual Data Model / HL7 Reference Information Model structure as appropriate, will include the ability to associate incoming data with appropriate existing data (e.g., a report of a disease in a person who had another condition previously reported), will have the capacity to support data accumulated through various means (e.g., through web-based and thick client systems as well as electronic messages), and will function so that data can be accessed by standards-based interaction with commercial products for reporting,

statistical analysis, geographic mapping and automated outbreak detection algorithms as well as the processing of queued data from and for electronic messages.

Technical description: The integrated data repository will implement common database technology (e.g., Sybase, Oracle or SQL Server) running on servers using Windows NT / 2000, LINUX or UNIX and supporting ODBC, ANSI standard SQL and JDBC access for data input from web based systems, reporting and analysis tools. The repository will also be able to house stored procedures that can initiate EJB, CORBA and DNA (DCOM) objects. Appropriate security for the repository will include firewall protection, restricted access, selective authorizations and the encryption of some sensitive patient data (please see element #h).

d. Develop active data translation and exchange (integration broker) functionality.

Functional description: This element supports data translation, data import and export, queuing and messaging for the dynamic bi-directional interchange of data using Extensible Mark-up Language (XML) to and from the integrated data repository, other associated databases and, in some cases, the within health departments and with other public health agencies. Data integration functionality will be deployed with the ability to rapidly develop ad hoc data exchange interfaces without programming. XML messaging will also provide the messaging infrastructure for future versions of HL7 and X12 content and for some environments may be best achieved with interface engine technology such as in element #b.

Technical description: Integration broker functionality may be fulfilled by an integration broker server, by software components running on shared servers or by some application server technologies. Bi-directional data transmission will occur using XML transfer over HTTP or HTTPS as appropriate. Secure communication with recipient servers will be performed with virtual private network capacity or certificate-based SSL server to server communication. Application logic to perform data validation, to queue data reports for completion or to initiate the completion and submission of full messages will be performed using EJB, CORBA, or DNA (DCOM) components (please see element #e). XML messages and associated application logic for program specific reporting will be derived from the Public Health Data Model / HL7 Reference Information Model and will be jointly developed by the CDC and the funding recipients.

e. Contemporary application programming practices - component based, object oriented and cross platform where possible. (formerly - Develop transportable business logic capability).

Functional description: Data validation, business rules for data accumulation, data processing, workflow implementation, data coding and decoding, registry mapping, and case management capabilities will be developed on the application server around the data repository using contemporary programming practices including one of several component development approaches, object oriented code development and,

where possible, a cross platform implementation. Application logic for data accumulated via the web, via thick client software, via messaged XML and HL7 will need to be consistently applied to ensure that data quality is good and shared data is comparable.

Technical description: Component development will involve EJB, CORBA or DNA (DCOM). Database access will use SQL and ODBC or JDBC connectivity. Application server development surrounding the data repository will apply business rules and initiate integration broker activity. Data repository stored procedures will need to initiate application server functions.

f. Develop data reporting and visualization capability.

Functional description: Selective data reporting according to user need-to-know, statistical analysis, Geographic Information Systems (GIS) use and other visualization, display and mapping functions will be implemented using COTS (commercial off of the shelf software) solutions through industry standards for access to the data repository.

Technical description: Commercial reporting systems (e.g., Crystal Reports or Actuate, statistical analyses software such as SAS, SPSS or EPI Info 2000 and GIS software (e.g., ArcView or MapInfo) will be integrated using ODBC and JDBC data access. Security and access control will be applied for remote access over public networks using SSL and Certificate or Token-based authentication with appropriate authentication and authorization.

g. Implement a shareable directory of public health personnel.

Functional description: Select information about pertinent public health personnel within state health departments and select local health jurisdictions will be listed in a standards-based information directory. The directory will be shareable and merge-able with directories from other state and local health departments and the CDC to create a directory of public health personnel. The directory will capture information about the roles and expertise of personnel for the use by public health communication and notification systems. Eventual use for authentication and authorization to resources is also anticipated. The directory of public health personnel will be used to guide the flow of information within and among public health agencies for emergent and non-emergent purposes.

Technical description: Directories will be maintained using the Light Weight Directory Access Protocol (LDAP) services. Data fields in the directory will use X.500 standards for field type and length. Public and non-public field division, standard Object Classes and their attributes and definitions as well as methodologies for replication will be defined in conjunction with CDC and DHHS directories.

h. Implement a security system and appropriate security policies.

Functional description: To develop standards, operating procedures and infrastructure for the secure transmission, processing and storage of sensitive or critical data and the support of sensitive or critical systems. This will include the secure Internet exchange of information based on the creation and operation of a secure Internet connection and gateway facility that can work in concert with the CDC's Secure Data Network (SDN).

Technical description: Security policies will be implemented with authentication based on industry standard X.509 certificates, secure tokens, and other applicable means as identified; access and control of data via selective integrated repository authorization; an encryption engine and appropriate use of encrypted data; and access control through a firewall by data routing to programs and other organizations.

NEDSS Systems Architecture for State and Large Local Health Departments