Public Health Information Network
Functions and Specifications
Version 1.2 – December 18, 2002

Introduction and Chronology

Through several efforts over the past few years, CDC, together with our partners, has been working toward the adoption and implementation of standards-based, integrated, and interoperable information technology (IT) systems to support public health work. Now the CDC, in cooperation with its public health partners, is advancing a group of coordinated standards and specifications to ensure a consistent and coherent public health information network can be built to serve the nation's public health information needs.

The events surrounding last fall's anthrax bioterrorism made rapid progress toward achieving these goals more urgent than ever. HHS Secretary Tommy Thompson's announcement on January 31, 2002, of $1.1 billion in funding to states for bioterrorism (BT) preparedness, to be provided mainly through CDC bioterrorism cooperative agreements created an unprecedented opportunity for developing public health capacity. This announcement resulted in a tremendous amount of effort in a short time - at CDC to prepare the guidance for the Bioterrorism Preparedness and Response cooperative agreement supplements, and subsequently, in health departments around the country to prepare work plans and submit applications. Important challenges remain.

CDC's Office of the Director recognized that a substantial amount of these resources would probably be spent on information technology, and that accelerating progress toward defining and implementing IT standards for public health (building on and harmonizing prior efforts through Health Alert Network [HAN], National Electronic Disease Surveillance System [NEDSS], and Epi-X) could improve the likelihood that these expenditures would result in effective information flow through interoperable systems; but absence of guidance now for standards-based development could work against us. Consequently, CDC decided to incorporate the "Public Health Information Technology Functions and Specifications (for Emergency Preparedness and Bioterrorism)" into the BT guidance as an attachment. A benefit of this urgency and compressed time frame is that CDC now has this first version of public health IT functions and specifications, as published with the BT guidance.

The CDC Information Council (CIC) took an important first step at its April 2002 meeting by deciding that CDC would work to adopt IT standards and specifications that would apply to all CDC cooperative agreement programs. While the urgency and compressed time frame required for the BT cooperative agreement did not permit a full process for evaluation and review of these functions and specifications as potential CDC enterprise standards, their heavy reliance on well evaluated NEDSS and HAN standards and their presence in the BT guidance make them a reasonable starting point for CDC enterprise standards. At the same time, a process for review and evolution is needed to promote the PHIN functions and specifications from a starting point toward full-fledged implementation.

Background and Association with Other Standards Initiatives

These PHIN functions and specifications are consistent and compatible with standards promoted by the National Health Information Infrastructure and other work of the National Committee on Vital and Health Statistics, the Health Insurance Portability and Accountability Act (HIPAA), and other government initiatives (such as the CHI eGovernment project) that are based on the use of leading industry standards.

The PHIN functions and specifications are almost exclusively based on the NEDSS Systems Architecture Version 2.0, the NEDSS conceptual and logical data models, NEDSS identified standard vocabularies, and the HAN technical specifications version 2, which, in turn, are specific implementations of relevant industry standards. Data standards are derived from, and compatible with the Health Level 7 Reference Information Model (RIM). Vocabulary standards not associated with the RIM are associated with the well established LOINC and SNOMED terminologies. These associations are well founded for the areas that are currently included in the logical data model. As is described below in "Scope", the logical data model is not currently inclusive of some public health data domains, e.g. environmental data, which may better derive their specifications from other industry standards.

Technical specifications from the NEDSS Systems Architecture and HAN are based on well established industry standards for interoperable technical systems (please see the attached standard reference glossary). The PHIN Functions and Specifications do introduce one additional technical standard, ebXML, which is proposed for establishing a secure Internet-based, bidirectional data brokering network (the live exchange and acknowledgment of data messages between partners) for BT preparedness.

The formulation of the functions in the PHIN Functions and Specifications is based on basic IT building blocks that support many different public health functions.

Scope and Implications

These PHIN Functions and Specifications apply to systems implemented on Intranets at Internet connected health departments. At this time, this does not principally include international cooperative agreements in places where Internet connectivity is limited. The data specifications should apply to laptop and handheld systems, but currently the technical specifications do not cover these technologies. The PHIN Functions and Specifications apply to those who send data to public health in the context of the identified message standards for lab and clinical data and the transport mechanisms for moving data securely to public health across the Internet. Health Resources and Services Administrations (HRSA) has also endorsed these Functions and Specifications and has referenced them in their preparedness funding.

These PHIN functions and specifications are intended to be incorporated into program guidance for CDC cooperative agreements with public health agencies, and to guide IT systems development in the context of those cooperative agreements. They are also intended to provide guidance for relevant IT enhancements for existing systems, particularly with respect to data standards. For example, health departments currently exchanging electronic data with laboratories would use the PHIN functions and specifications as a guide for development of standard-based information exchange.

The CDC will be providing assistance to partners to facilitate implementation of these PHIN functions and specifications in their IT systems. In addition, the CDC plans to support the evolution and further development of these functions and specifications, as well as the technical infrastructure to support their implementation in public health. This support will take the form of technical assistance, direct assistance with contracted resources and, at times the provision of software components that support standards-based software implementations wherever in public health that they are developed.

Process and Evolution

The technical and data standards and specifications included herein will be regularly updated and refined by the Centers for Disease Control and Prevention and its public health partners.

The CIC, which includes representatives from CDC and its public health partners, is developing a process for the evolution and development of the data specifications, technical standards, and for the evaluation of CDC and non-CDC systems for their compatibility with these standards. This process will inform development of the PHIN functions and specifications. In addition, to gain additional perspectives on these functions and specifications, directions for their evolution, and to gain a better understanding of issues in their implementation, CDC plans a review of these PHIN functions and specifications by a panel consisting of CDC technical and program personnel, partner organization technical and program personnel, and external experts.

Public Health Information Technology
Functions and Specifications

These Functions and Specifications will be updated regularly to represent completion of data specifications and architecture refinements. Updates can be found at:
www.cdc.gov/cic/functions-specs

Public health is practiced by an array of local, state and federal organizations that are further divided into functionally organized units around clinical, health department, laboratory, disease program and other operational divisions. The complex responsibilities and interactions between these public health partners necessitate significant coordination of information technology and information sharing methodologies to meet bioterrorism and public health preparedness objectives. This document contains partner and CDC functions, industry standards and detailed specifications necessary to have a secure, coordinated public health IT system capable of acquiring, managing, analyzing and disseminating public health information to meet these challenges. The specifications included herein are based on industry data and systems standards, most of which have been identified in related national initiatives like the National Electronic Disease Surveillance System (NEDSS) and the Health Alert Network (HAN). As such, these standards and specifications represent a part of a broader public health systems and data architecture.

This document identifies bioterrorism and public health preparedness functions and describes how these functions should be implemented using identified standards and standards-based specifications to build a coordinated system. The system will enable the secure, immediate exchange of critical health data (surveillance, possible cases, contacts, lab, clinical, personnel, etc.) between clinical partners, public health agencies and labs and, as appropriate, federal agencies. It will support the appropriate management and presentation of information to public health decision makers at a variety of levels. To achieve the sharing of software and systems and to be able to reliably exchange data, adherence to specific data and systems specifications (which in turn adhere to appropriate national standards), is required and will be evaluated.

Each IT function may be referenced in several places in cooperative agreement guidance. A reference to a specific function requires full compliance with the stated functions, standards and specifications. The IT function describes general functional capabilities specifications for how those capabilities need to be accomplished to work as a cohesive whole and the standards on which these specifications are based. The functions also identify who has responsibility for its fulfillment, the methods through which fulfillment will be evaluated, and, in some cases, additional, not yet completed data specifications that will be finalized in the coming months.

Specifications are Included for the Following IT Functions:

1. **The Automated Exchange of Data Between Public Health Partners -** To securely and automatically exchange information, as appropriate, between two computer systems to achieve a “live” network for data exchange between partners in public health

2. **The Use of Electronic Clinical Data for Event Detection -**To receive, manage and process electronic data from care systems at clinical care sites, laboratories, or their proxies

3. **Manual Data Entry for Event Detection and Management -** To accumulate, manage and process information manually entered via a web browser at a health agency or remote site

4. **Specimen and Lab Result Information Management and Exchange -** For laboratories involved in public health testing, to receive laboratory requests, accept specimen and sample data, manage these data and immediately report electronic results to public health partners

5. **Management of Possible Case, Contacts and Threat Data -** To electronically manage, link and process the different types of data (possible cases from detection, possible contacts, facility, lab results, prophylaxis and/or vaccination, adverse events monitoring and follow-up)

6. **Analysis and Visualization -** To analyze, display, report and map accumulated data and share data and technologies for analysis and visualization with other public health partners

7. **Directories of Public Health and Clinical Personnel -** To participate in and maintain directories of public health participants (including primary clinical personnel), including participant roles and contact information

8. **Public Health Information Dissemination and Alerting -** To receive, manage and disseminate alerts, protocols, procedures and other information for public health workers, primary care providers, and public health partners in emergency response

9. **IT Security and Critical Infrastructure Protection -** To ensure that sensitive or critical electronic information and systems are not lost, destroyed, misappropriated or corrupted

Additional Content:

- List of Data Specifications to be completed in early 2002
- CDC commitments to support these functions

Public Health Information Network
Functions and Specifications
(as Presented for Emergency Preparedness and Bioterrorism)
February 8, 2002

Function #1 – The Automated Exchange of Data Between Public Health Partners

This function involves the ability to securely and automatically send and receive information, as appropriate, between two computer systems, to achieve a "live" network for data exchange between partners in public health. Specific data and technical standards for event detection, the management of possible cases, case contacts, potential threats, specimens, lab results, alerts and procedures are referenced in other parts of this appendix. The specifications for this function define the technical infrastructure necessary to exchange this information between a computer system at one public health partner and a computer system at another public health partner.

This function should be implemented for the purpose of sending and receiving information between partners in public health including state and local public health agencies that run information systems. It should be used by laboratories participating in emergency preparedness and response activites and, at least in a sending mode, by participating clinical sites. The presentation of information to clinical sites and other participants in public health may be accomplished by public and secure web-based viewing via technologies identified in other included functions.

Technical Specifications

One side of each system-to-system data exchange will install and maintain an ebXML compliant SOAP web service that can be reached via an HTTPS connection after appropriate authentication. The other side of the system-to-system data communication can be behind a firewall where a traditional HTTPS port is open (as is normal for secure web access). Bi-directional messaging is possible through this implementation, but some partner to partner exchanges will have authenticated web services on both sides of the "conversation." Messages will be in the industry standard ebXML format and will include standardized HL7 Version 2.3, HL7 Version 3.0, X12 and LDIF message content. Software to enable public health ebXML messaging will be available for download from the CDC.

Sensitive data should be encrypted prior to being sent through the secure HTTPS data transport. Stored data from messages should be protected using strong authentication and other security precautions identified in Function #9 (IT Security and Critical Infrastructure Protection). Message creation and parsing to support system-to-system data exchange can be accomplished via a dedicated interface engine, HL7 message and translation software components, or integration broker technologies running on Windows NT / 2000, LINUX or UNIX servers. The ability to translate and manipulate LOINC, SNOMED, ICD and CPT codes and to map local codes into these standards will be necessary to process some messages. Specific messages, including their message structures and vocabularies, are referenced in other functions and/or identified for further specification at the end of this document.

Systems participating in this function need to be connected to the Internet at all times (they should not require manual dial-up each time for connection). The connection shall be a minimum of 56Kbps with a strong recommendation for 384 Kbps or greater.

Evaluation of Function

Regular testing of this function with reporting on completed data exchange between relevant public health partners should be initiated by the end of 2002. Successful fulfillment of this function will mean, for example, that a message can be sent from the CDC to appropriate public health agencies (state and/or local) covering every jurisdiction in the United States and its associated territories or that an electronic message about a bioterrorism pathogen could originate in a clinical or lab setting, be immediately sent via secure means, and no necessary human intervention, to the responsible local or state health department, where it would be immediately available for processing and analysis. The message would also be immediately electronically sent in linked, but de-identified form to the appropriate federal agencies.

Function #2 – The Use of Electronic Clinical Data for Event Detection

This function involves the receipt, management and processing of electronic data from clinical care sites, laboratories or their proxies, for the purpose of surveillance for the identification of a possible bioterrorism or other public health events. The data may originate in clinical care, laboratory information management or admission discharge and transfer systems and may be provided directly from clinical care sites or through their proxies. Accumulated data need to be stored in the specified standard data format, to be analyzable by humans and automated detection algorithms, to be presentable in tabular, geospatial and other report formats, and to be automatically sent, in appropriate aggregate or individual form, to other public health participants.

This function should be implemented by state and/or local public health agencies receiving electronic data from clinical sites and their surrogates. If implemented by the local health department, specified[1] data will be sent in real time to the responsible state health department, and in turn, other specified[2] data will be sent to federal agencies. If implemented by a state health department for a particular jurisdiction, local public health officials should be provided real-time secure access to the data for their jurisdiction.

Technical Specifications

Data will be received by public health partners via ebXML messaging identified in Function #1 (The Automated Exchange of Data Between Public Health Partners). Data storage should occur using the NEDSS logical data model specification of the HL7 Reference Information Model and extensions made to accommodate syndromic and other clinical data that will be completed in early 2002[3]. Data accumulated for this purpose need to be stored in a format compatible with the NEDSS / HL7-compatible Logical Data Model so that general analytic and reporting tools can be developed. The data repository should be able to associate incoming data with appropriate existing data (e.g., a report of a disease in a person who had another condition previously reported), and should 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. The data repository should implement common database technology (e.g., Sybase, Oracle or SQL Server) running on servers using Windows NT / 2000 /XP, LINUX or UNIX and supporting ODBC, ANSI standard SQL and JDBC access.

Evaluation of Function

Regular evaluation of the number of hospital and primary care sites that are functioning (as evidenced by receiving data from each site) compared with the total number of possible hospital and primary care sites in a state should be accumulated by the end of 2002.

Function #3 Manual Data Entry for Event Detection and Management

This function involves the capability to accumulate, at a public health agency, manually entered syndromic and other data (utilization, clinical census, aggregate diagnoses) from clinical points of care that may provide surveillance for the identification of a possible bioterrorism or chemical attack. It should also support heightened surveillance capabilities (more sensitive and detailed) for implementation during high profile events or after the identification of a likely case. Accumulated data need to be stored in the specified standard data format, so they may be analyzable by humans and automated detection algorithms, to be presentable in tabular, geospatial and other report formats, and to be automatically sent, in appropriate aggregate or individual form to other public health participants as specified in Function #1 (The Automated Exchange of Data Between Public Health Partners) and in the relevant message format. Systems to detect possible events need to link seamlessly (including the ability to track back to specific cases) with systems for case management, contact tracing and other public health follow-up and response activites.

This function should be implemented by state and/or local public health agencies performing electronic surveillance. If implemented by the local health department, specified[1] data will be sent in real time to the responsible state health department and, in turn, specified[2] data will be sent to appropriate federal agencies. If implemented by a state health department for a particular jurisdiction, local public health officials will be provided real-time secure access to their jurisdictional data.

Technical Specifications

The storage of data accumulated in this manner should follow the data specifications identified in Function #2 (The Use of Electronic Clinical Data for Event Detection) including the

NEDSS logical data model specification of the HL7 Reference Information model and extensions identified in early 2002[3]. Secure browser-based data entry should be used for data input and results reporting from and to primary care clinical care sites and other sources (e.g., infection control practitioners, small laboratories). Web browser-based data systems should 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 /XP, LINUX or UNIX and supporting generic web browsers (HTML 3.0+ / Java). The web server, the application server and the database server should be separate tiers of this system. 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. Application servers, regardless of physical platform, should be able to run shared JAVA code. Data delivery to an associated database should use ANSI standard SQL and ODBC or JDBC connectivity. Security over the Internet should be implemented using strong authentication, (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 as described in Function #9 (IT Security and Critical Infrastructure Protection).

Evaluation of Function

Regular evaluations of the number of hospital, local health department and other primary care sites that are functioning (as evidenced by receiving data from each site) compared with the total number of possible hospital and primary care sites should be accumulated by the end of 2002.

Function #4 – Specimen and Lab Result Information Management and Exchange

This function involves the ability to receive laboratory requests, accept specimen and sample data, manage these data and immediately report electronic results to public health partners. The function draws on the same infrastructure as Function #1 (The Automated Exchange of Data Between Public Health Partners). It also involves specific capabilities to receive specimen information and lab result reports from labs without electronic laboratory reporting and to manage and process data internal to the lab in Laboratory Information Management Systems (LIMS) in such a way that electronic lab result reports will be immediately available.

This function should be used by public health laboratories and public health partner laboratories with electronic information systems. Specimen and sample data need to be accumulated by other public health partners using the same data and data exchange standards as public health laboratories. Accumulated data need to be automatically sent, in appropriate aggregate or individual form to other public health participants as per Function #1 (The Automated Exchange of Data Between Public Health Partners).

Technical Specifications

Data associated with these activites need to be stored in HL7 compatible data formats. Coding of request and results messages with the LOINC and SNOMED vocabularies is a necessary component of the reliable interchange of data. Information exchange and message creation and parsing should be fulfilled as per Function #1 (The Automated Exchange of Data Between Public Health Partners). Web systems for receiving specimen information and for the entry of small numbers of lab results by facilities that are unable to exchange messages may also be supported. Web based results reporting should only be supported for entry to an organization participating in Function #1. Web based results entry does not fully meet the requirements for a "live" network for data exchange between partners in public health.

Evaluation of Function

Regular evaluation of the number of public health laboratories that can electronically manage specimen and results data, can code data with the appropriate vocabularies, and can automatically exchange data with partner public health organizations should initiated by the end of 2002.

Function #5 – Management of Possible Case, Contacts and Threat Data

This function involves having public health bioterrorism and preparedness systems that can manage all relevant data types and trace possible cases from detection, through lab testing and confirmation, possible prophylaxis and/or vaccination, adverse events monitoring, follow-up and possible death. These needs put a high emphasis on maintaining associated demographic (home and occupation), contact (communicable disease tracing), clinical, geospatial and event data (threat, facility, etc.) in forms that can be readily associated, re-linked and processed. Registry de-duplication and automated record linking capabilities should be established to ease data exchange between partners. Emphasis should be given to the development of management systems that allow for the management of public health surveillance and response data beyond the needs of case detection and alerting.

This function should be implemented by either a state and/or local health department for every jurisdiction in the United States and its associated territories.

Technical Specifications

The input and management of possible case and contact data should comply with the standards and specifications in Functions #1-4 above. Potential cases should be "linked" and traceable from detection via electronic sources of clinical data or manual entry of potential case data through confirmation via laboratory result reporting. Data storage should be implemented as specified in Function #2 (The Use of Electronic Clinical Data for Event Detection) using the NEDSS logical data model specification of the HL7 Reference Information Model and extensions thereof (completed for this purpose in early 2002). Data input and management should be implemented via Web browser-based systems as identified in Function #3 (Manual Data Entry for Event Detection and Management). Lab results should be derived from systems as identified in Function # 4 (Specimen and Lab Result Information Management and Exchange) and exchanged as per Function #1 (The Automated Exchange of Data Between Public Health Partners).

Evaluation of Function

Local and state public health agencies should initiate the evaluation of this function including consideration of tracking threats and cases and managing case contacts. A program of annual validation should be managed by the local and state public health agencies.

Function #6 – Analysis and Visualization

This function involves the ability to analyze, display, report and map data accumulated and stored according to the specifications in Functions #1 through 5 above. Selective data reporting according to user need-to-know, statistical analysis, Geographic Information Systems (GIS) and other visualization, display and mapping functions will be implemented using COTS (commercial off the shelf software) solutions through industry standards for access to the data repository. This function also involves the ability to install and operate outbreak detection algorithms that operate via standards base access to the specified data structures.

This function should be implemented by state and/or local health departments, which are supporting the storage and management of data as per Functions #2-5.

Evaluation of Function

Public health agencies that support information systems should evaluate their ability to clearly present, analyze and report accumulated data to meet detection, management and preparedness programmatic needs. Formal usability analysis should be considered for all systems and custom built reports.

Technical Specifications

Commercial reporting systems (e.g., Crystal Reports or Actuate), statistical analyses software (e.g. SAS or SPSS) 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.

Function #7 – Directories of Public Health and Clinical Personnel

This function involves the support of a directory of public health participants (including primary clinical personnel) and participants' roles and contact information for every jurisdiction.

These directories will be in a form as to be immediately usable for the direct or relayed transmission of public health notifications (via e-mail, pagers, voicemail, and/or automated faxing). The directories will also be regularly exported, in a specificed[4] data format, to appropriate public health partners (local, state and federal) to ensure redundant and complementary functions. These directories can also be used to support authentication of identified personnel to restricted access electronic resources. The directories should, minimally, be able to support the retrieval of individuals based on name, public health role, organizational affiliation and geographical location.

This function should be implemented by a state and/or local health department to achieve coverage of the United States and its associated territories.

Technical Specifications

These directories will present a Lightweight Directory Access Protocol (LDAP v3.0) standard-based service to allow data access and sharing across multiple computer systems and, as appropriate, organizational boundaries. Directory information transfer and sharing will be supported by a standard message format based on the LDAP Data Interchange Format (LDIF) standard. Data fields in the directory will use X.500 standards for field type and length. Implementation for individuals will be based on existing LDAP standards as embodied in the person, organizationalPerson, and inetOrgPerson LDAP object classes. Complete specification for LDIF format of LDAP data fields is in draft form and will be reviewed by public health partners and published in early 2002.[4] LDIF data messages should be exchanged between public health partners as content of ebXML messages as described in Function #1 (The Automated Exchange of Data Between Public Health Partners).

Evaluation of Function

Regular evaluation by local and state public health agencies of coverage (percent of target individuals included), effectiveness, and accuracy of the directories should be initiated by the end of 2002.

Function #8 – Public Health Information Dissemination and Alerting

This function includes the ability to receive, manage and disseminate alerts, protocols, procedures and other information for dissemination to public health workers, primary care physicians, public health laboratorians, and public health partners in emergency response. It includes the ability to "push" information via messages and allow participants to "pull" information via the browsing of secure web sites. It may also include the support of interactive communication sites for threaded discussion capabilities.

Message distribution between public health partners will be in a specified format[5]. Immediate distribution to public health partners should be possible through one or more mechanisms (e-mail, pagers, voicemail, and/or automated faxing). Based on specified[5] message descriptors for level of criticality and for involved program areas, the responsible organization will be able to:

- Immediately pass on highly critical information (as specified in message format) to personnel in their directory and, as needed recursively, to sub-jurisdictions with directories so that all public health and clinical personnel can be notified
- Edit messages for local needs and then transmit when they contain less time critical information
- Direct information to appropriate audiences based on the agreed to message subject descriptors and corresponding recipient descriptors in the public health directories identified in Function #8 (Directories of Public Health and Clinical Personnel)
- Securely archive information for subsequent viewing and facilitate secure discussion of public health issues through authenticated access to an appropriate web site

This function should be implemented, by a responsible local and/or state health department for full coverage of the United States and its associated territories. This function will serve critical and non-critical notification purposes among public health participants.

Technical Specifications

Message formats will be developed with content and descriptors in compatible XML format. Specific presentations of content will be translatable and shareable in ASCII text format for e-mail messages and faxes.

Web browser-based data systems should 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 /XP, LINUX or UNIX and supporting generic web browsers (HTML 3.0+ / Java). Secure web presentation over the Internet should be implemented using strong authentication, (Secure Sockets Layer (SSL) capable server and industry standard client certificates or token-based for authentication and selective authorizations). Systems should be protected according to Function #9 (IT Security and Critical Infrastructure Protection).

Evaluation of Function

Regular evaluation by local and state public health agencies of coverage (the percent of individuals reached by messages and in what timeframe) should be initiated by the end of 2002. Periodic exercises should be employed to assess the effectiveness of the function.

Function #9 - IT Security and Critical Infrastructure Protection

This capability involves assuring that access to sensitive or critical information and information systems is not lost, destroyed, misappropriated or corrupted by a internal or external malefactor or by systems failure or catastrophic event and that information is protected is ways that meet or exceed HIPAA standards. The function should also assure that processes cannot be initiated or controlled by unauthorized individuals and that continuity of operations can be maintained subsequent to a catastrophic event.

This function should be implemented for all state and local health departments and other public health related organizations including clinical care and laboratory providers who run electronic information systems.

Technical Specifications

Client and server X.509 digital certificates or comparable strong authentication methodology should be required for access to sensitive or critical resources from the Internet. Role-based, mandatory access control protocols, as well as realistic and effective policies for use and administration of information technology resources, should be established. Security patches and configuration corrections should be applied promptly. Desktop and server based virus scanning, intrusion detection, network vulnerability analysis including port scanning, security policy monitoring, regular penetration testing and active threat intelligence should be employed. Continuity of operations planning and procedure implementation should incorporate man-made and natural catastrophic event management, routine offsite back-ups and hot site considerations.

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. Firewalls will need to securely provide access to an ebXML SOAP receiver to present a service for secure Internet receipt of public health information as well as secure access to restricted access web sites.

Evaluation of Function

External verification of security and continuity processes and technology for public health agencies that support critical information systems should occur on at least a yearly basis. Independent validation and verification should include disaster simulations and intrusion detection.

CDC Commitments to Support These Functions

CDC systems developed or promoted to support these activities will:

- Will integrate into existing state or local strong authentication and authorization technologies using a single approach.
- Will use a common methodology for the exchange of data between partner systems (ebXML, SOAP, HTTPS and for some, not sensitive data SMTP)
- Will require only one single directory of public health, clinical and participant personnel (LDAP directory) for any particular jurisdiction.
- Will support standards-based access to major database management systems
- Will use the same implementation environment wherever possible and will be sensitive to the multiple operating systems and database management systems that exist on servers at state and local levels
- Will use single data and vocabulary standards, wherever possible, to describe the same data elements

The CDC will implement a central directory capability to provide effective linkage between state and local level directories, a central search capability, and where appropriate, an integration of public health organizational data.

The CDC will provide consultation and technical assistance on all communication and information technology components as well as the implementation of IT Functions and Specifications

The CDC will promote these industry standards-based approaches, wherever possible to other groups and organizations.

List of Additional Specifications to be Detailed by Public Health Partners

While a great number of data specifications (based on national standards like HL7, SNOMED, LOINC, ISO codes) have already been specified for the NEDSS Logical Data Model and are being specified for the HL7 Version 3.0 compatible Public Health Notification Messages, more work needs to be done by the public health partners to agree on complementary data specifications in several areas related to Emergency Preparedness, Bioterrorism, Chemical Event Detection and Response. In early 2002, the CDC will initiate several focused data modeling sessions (for data specification) and joint application development sessions (for necessary procedures) for public health partners to solidify standards-based data specifications and workflows in several areas listed below.

[1] Public Health Notification messages including data fields and vocabulary for the exchange of possible cases, contacts and bioterrorism surveillance data between local and state health departments to be specified in early 2002.

[2] Public Health Notification messages including data fields and vocabulary for the exchange of linked, but de-identified, possible cases and bioterrorism surveillance data between state health departments and federal agencies to be specified in early 2002.

[3] HL7 compatible extensions to the NEDSS logical data model to accommodate clinical and syndromic data.

[4] An LDIF exchange format, based on X.500 naming standards, to exchange data between LDAP directories is in draft form. This draft will be reviewed and specified through a formal partner joint application development session in early 2002.

[5] Formal modeling in the HL7 process to specify data fields and vocabulary for describing message criticality (and derivative message processing procedures), message content type descriptors (subject areas, sender type, recipient type) and potentially interested parties, etc.

Public Health Information Network
Functions and Specifications Glossary (version 1.2, December 18, 2002)

Glossary, References and Rationale Discussion

This document provides reference information and a glossary for the Public Health Information Network Functions and Specifications.

Functional Areas

Function #1 – The automated exchange of data between Public Health Partners
Function #2 – The Use of electronic Clinical Data for Event Detection
Function #3 – Manual Data Entry for Event Detection and Management
Function #4 – Specimen and Lab result Information management and Exchange
Function #5 – Management of Possible Case, Contacts, and Threat data
Function #6 – Analysis and Visualization
Function #7 – Directories of Public Health and Clinical Personnel
Function #8 – Public Health Information Dissemination and Alerting
Function #9 – IT Security and Critical Infrastructure Protection.

Function #s	**Term**: ANSI standard SQL
2,3	**Definition:** SQL is Structured Query Language. This language is designed to make it easy to build complex queries against a relation database. When The ANSI Standard version of SQL is followed any relational database can execute the statements. Each relational database vendor has created extensions to this standard that help performance or add functionality, but this is not ANSI Standard.
	Rationale:

	SQL has been the industry standard for accessing data from a relation data store for many years. When writing an application you should follow the ANSI SQL standards for writing SQL statements if you expect this code to function against various relation database products.
	Related Standards: XPATH – When accessing data through an XML, SAX, DOM interface an emerging standard query language is XPATH. Some of the relational database vendors will allow direct access to their data through this language as well as SQL. However, SQL is the most efficient language when accessing relational data directly.
	References: http://www.tek-tips.com/gfaqs.cfm/spid/220/sfid/1073
Function #s	**Term**: Apache
2, 8	**Definition:** Apache is an open source version of web and application servers. There are components to the apache server that can run a simple HTML request up through complex JAVA applications.
	References: www.apache.org
Function #s	**Term**: Authorization
3	**Definition:** Authorization is the giving of "access" to some resource and establishing what you can do with that resource. This is different than Authentication, which identifies a valid user of resources. Many times authorization is based on a "role" which provides a blanket access based on a person's role in an organization. This authorization may not only provide access but may segment what feature or data can be viewed by the user.
	Rationale: Applications are more efficiently written if they can dynamically adjust based on the access requirements of a user. By applying a "role-based" authorization technique this dynamic code adjustment can be achieved. In many cases this authorization is centrally controlled in the same manner the authentication is provided further simplifying the development of an application and providing better operational control.

	Related Standards: N/A
	References: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnservice/html/service02282001.asp
Function #s	**Term**: COOP / Disaster Recovery
9	**Definition:** Continuity of operations planning and procedure implementation. COOP is really just common sense when it comes to the operations supporting your computing systems. It is an excepted fact that system will break; it's just a matter of when. It is also a fact that we have become very dependent upon out computing systems such that being with them could be very debilitating. You need procedures, configurations, and planning in place that makes sure your can continue your operations through minimal or major disasters.
	Rationale: Another fact of life is that our system will go down. It may be from a deliberate action or a part of the system just wears out. Either way planning for this is imperative since we are relying on these systems ac critical components in our BT defense.
Function #s	**Term**: CORBA (**C**ommon **O**bject **R**equest **B**roker **A**rchitecture)
3	**Definition:** CORBA is Object Management Group's open, vendor-independent architecture and infrastructure that computer applications use to work together over networks.
	Rationale: Many viable distributed application systems have been constructed employing the CORBA infrastructure. In some cases you may want to integrate a CORBA object in your complex application system and that is why you want a diverse web application server as your information broker. If you are willing to write to the somewhat closed standards involved with the CORBA architecture a very powerful distributed application system can be built. An example is the RSVP syndromic surveillance system that has been prototypes by Sandia Labs.

	Related Standards: • J2EE • .NET • Web Services
	References: http://www.omg.org/gettingstarted/corbafaq.htm
Function #s	**Term**: COTS (Commercial-off-the-shelf) Reporting / Analysis Tools
6	**Definition:** When it comes to reporting there are many excellent COTS tools available such that custom reports are generally not required. Examples of programs for reporting are as follows. (Crystal reports, SPSS, SAS, Actuate, ArchView MapInfo) The trick is to choose a consistent data structure such that COTS reporting and analysis tools can make some sense of assembling the data extraction you want. Two things are a consideration. 1) The Tools should be able to "see" and extract your data from and into a varied set of reports. 2) The use of a standard model yields much of the strength one get from a COTS reporting tool.
	Rationale: Any time we can buy versus build and get the functionality we need it's a plus. In the case of reporting, analytical tools, and visualization there is a myriad of tools available on the market today. Examples of tools would be SAS, Crystal reports, Oracle reports, Mathematica, Business Objects, SSPS, Minitab
	Related Standards: • Custom programs
	References: www.sas.com
Function #s	**Term**: CPT Codes
1, 4	**Definition:** CPT (the physician's Current Procedural Terminology) Codes describe medical or psychiatric procedures performed by

	physicians and other health providers. The codes were developed by the Health Care Financing Administration (HCFA) to assist in the assignment of reimbursement amounts to providers by Medicare carriers. A growing number of managed care and other insurance companies, however, base their reimbursements on the values established by HCFA. There are 6 categories: Evaluation and Management, Anesthesiology, Surgery, Radiology, Pathology/Laboratory, and Medicine
	Rationale: • With medical procedures standardized but referenced by a wide set of name the coding is imperative to be able to track events or observations across procedures.
	Related Standards: • LOINC • SNOMED
	References: http://www.aacap.org/clinical/cptcode.htm
Function #s	**Term**: DCOM (Distributed Component Object Model)
3	**Definition:** DCOM is a protocol that enables software components to communicate directly over a network in a reliable, secure, and efficient manner.
	Rationale: Similar in capability of CORBA but demand significant resources to execute.
	Related Standards: • CORBA • J2EE
	References: http://www.microsoft.com/com/tech/DCOM.asp

Function #s	**Term**: De-duplication
5	**Definition:** The removal of duplicate records for the same data in a database.
	Rationale: Many times an event, person, or other types of records get entered with the same information into duplicate records in a database. This often happens when varied code sets are used, not all the attributes are available for a record, or data comes from two sources but on the same data item. The process of de-duplication removes the duplicate records and makes the data more viable. The process usually involves looking at the matching data in more than one field across the records and has some level of error tolerance to trap close records.
	Related Standards: N/A
	References: http://www.madison-info.com/Forms/CostofDupsArticle%20F401.pdf
Function #s	**Term:** ebXML
1, 2, 4, 7, 9	**Definition:** Electronic Business Extensible Markup Language – Is a modular suite of XML specifications to conduct business between partners over the Internet. Key components of ebXML are: Collaboration Protocol Profile (CPP), Collaboration Protocol Agreement (CPA), Business Process and Information Modeling, Core Components, Messaging and Registry/Repository.
	Rationale: EbXML is the only existing industry standard that enables the secure, bi-directional and immediate exchange of messages between business partners via the Internet. EbXML offers the high degree of specificity needed for the transport, acknowledgement and processing of industry standard data messages such as HL7, X12 and others. The following criteria support the selection of this as the messaging standard. • HL7 has endorsed ebXML messaging as the standard for data transport. The (a) link in the next column is an article on the endorsement from HL7 for the use of the ebXML messaging layer as the standard • EbXML is payload agnostic, which is critical for transport of many types of information and transaction between partners. • This message layer allows for the use of existing encryption and digital signature standards

- This protocol is a controlled environment that interacts between partners through a preexisting agreement. It follows standards for data exchange but not on a path that is openly discovered.
- EbXML is endorsed by the UCC and OASIS which is setting standards for many product vendor directions
- The standard supports interoperability between messaging partners through existing standards for data transmission and action.
- EbXML does not propose any new technologies. It is based on an aggregate of existing technologies that come together to solve controlled messaging needs. It is based on SOAP, XML, asynchronous reliable messaging architecture, web services architecture, and security standard interaction.
- The ebXML-messaging standard can be implemented across platforms.
- The standard provides for execution of multiple types of authorization.
- EbXML allows us to separate the translation layer from the application logic layer when sharing data between partners.
- Indeed some of the aggregate standard is evolving but it has been around longer than any of the others and continues to show strength being adopted by vendors and architectures
- EbXML is the main standard in Japan for business transactions following a Fujitsu implementation and is very successful.
- It executes over an open transport standard, HTTP, that is usually readily passed through firewalls.
- The standard implements a reliable transport for messages that can provide multiple levels of validation response. The standard also provides a recoverable structure from a failed transmission. This is critical in providing an asynchronous conversation that ensures a requested interaction take place between partners.

“EDI provides a fixed, predictable message format, which with high volumes and stable business processes make a lot of sense. With ebXML, one can have the messaging features of EDI, plus a larger framework of functions combining business process models, registries, company profiles, trading partner agreements, and semantic interoperability. While ebXML offers a complete framework, companies can implement parts of that framework, without having to swallow it all at once.” (web services.org: “the e-business continuum: Web Services, ebXML, and EDI) (d)

Related Standards:

There were a number of standards new and old that were considered for the message transport layer.

- EDI – Stable, well adopted but follows closed message layer that is binary therefore needs extensive vendor products to implement. Second, it requires a controlled secure transport channel, a VPN.

	• Web Services – A broad standard of which ebXML is a more specific implementation. EbXML uses web services, but has needed specificity regarding security, reliable transport, error handling, and controlled interaction. • XML/HTTP – this is the basis for ebXML, but like web services, is not specific enough to completely describe interaction on criteria above. • SMTP – Standard transport protocol, but completely open handling of message content resulting in all custom message interaction and content payload handling. No standard way for centralized encryption and storage. • FTP – similar to SMTP having a reliable transport, but completely open message handling method. • HTTP Put/Get – Standard message passing, but no standards structuring the message or handling it. • JMS – Good message standard, but missing higher level security components, payload handling declarations, and XML configuration. • SOAP – A foundation for ebXML but by itself is missing capabilities such as routing, reliability, and security. • HTTPR- this specification describes the exact reliable messaging mechanism that ebxml uses. It is designed to execute only on HTTP. The spec by itself does not provide the payload and conversational handling of ebxml.
	References: http://www.ebxml.org http://www.xmlglobal.com/prod/messageservice/index.jsp http://www.oasis-open.org/ http://www.hl7.org/press/05292001.asp (a) http://www.hl7.org/press/05022001.asp (b) http://www.cdc.gov/cic/functions-specs/function_1.htm/ibm_ebxml_course.pdf ebXML lecture Barry Rhodes.ppt (c) http://www.webservices.org/index.php/article/articleview/479/1/24/ (d)
Function #s	**Term**: EJB (Entity Java Beans)
3	**Definition:** EJB is a design architecture for java programs.
	Rationale: The EJB provides a way to hide a great deal of complexity in a java program. It is also designed to provide a high degree of reusability of a program function. EJB's are powerful but they have a number of layers that can be slow when executing.

	Related Standards: - CORBA ORB or Object – Similar is design but highly tied to the cumbersome CORBA infrastructure. - COM Object – Microsoft application object component proprietary to Microsoft environments.
	References: http://java.sun.com/products/ejb/
Function #s	**Term**: External Security Verification
9	**Definition:** Sometimes referred to as a “Security IV&V” meaning a security independent validation and verification procedure.
	Rationale: Monitoring your systems is the only viable defense to knowing if you systems remain secure. An industry standard method for testing this is to employ an external party to test the system. This is generally done using common attack methods and with little knowledge of your system. This emulates a typical attacker on the system, but will explore as many possible weak points as known. External validation also ensures no conflict of interest from internal knowledge or agendas.
Function #s	**Term**: Firewall
3	**Definition:** A firewall is a network part that controls the internet (TCP) traffic. It is designed to protect your network such that only requests for resources on your network are only the ones you approve.
	References: http://www.cdc.gov/nedss/Security/Secure_Data_Network3.pdf http://www.cdc.gov/nedss/Security/Security_InfoNB_Sys_Sites_V01.pdf
Function #s	**Term**: HIPAA (Health Insurance Portability and Accountability Act of 1996) Standards
9	**Definition:** A Federal law that allows persons to qualify immediately for comparable health insurance coverage when they change

	their employment relationships. Title II, Subtitle F, of HIPAA gives HHS the authority to mandate the use of standards for the electronic exchange of health care data; to specify what medical and administrative code sets should be used within those standards; to require the use of national identification systems for health care patients, providers, payers (or plans), and employers (or sponsors); and to specify the types of measures required to protect the security and privacy of personally identifiable health care information. The Centers for Medicare & Medicaid Services (CMS) is responsible for implementing various unrelated provisions of HIPAA, therefore HIPAA may mean different things to different people. Administrative Simplification Provisions (Title II, Subtitle F, of HIPAA) gives HHS the authority to mandate the use of standards for the electronic exchange of health care data; to specify what medical and administrative code sets should be used within those standards; to require the use of national identification systems for health care patients, providers, payers (or plans), and employers (or sponsors); and to specify the types of measures required to protect the security and privacy of personally identifiable health care information.
	Rationale: Originally conceived to protect the rights of people concerning Private patient data. This has also evolved to encompass many of the basic standards supported in the BT IT Specifications. That being the use of standards for data such as standard vocabularies.
	References: http://www.hipaa.org http://aspe.os.dhhs.gov/admnsimp/
Function #s	**Term:** HL7 2.3
1	**Definition:** HL7 is a formatting standard for structuring, storing, and messaging clinical data. The standard also supplies a basic set of vocabularies to be used for the attributes in the HL7 Reference Model. Version 2.3 is a segment based data structure that uses linked-lists to associate multiple records together. This is not an XML format.
	Rationale: The exchange of clinical information is critical in public health. Following a standard for this data exchange by using HL7 ensures consistent interpretation and completeness of the data. HL7 is the de facto standard for clinical data exchange and is endorsed by NCVHS as a standard for Computer-based Patient Records (CPR). It is also included in HIPAA as one of the major Standards Development Organizations (SDO)
	Related Standards: X12 – The ASC X12 standards body is focusing on building XML message standards to be used on a number of message

	transport methods for health care business transactions. This includes EDI. There is a set of X12 message segments that focus on medical insurance clinical data exchange. These messages and related vocabularies are not as complete as the HL7 message sets for the level of clinical data passed between public and private health organizations. Often the HL7 clinical data is “attached” to a X12 message segment. EDI – There were some early EDI message segments that existed as a standard for a while for moving clinical data. This has since been replaced by X12 and HL7. Vocabularies – LOINC, SNOMED can have some redundant coverage for attributes
	References: http://www.hl7.org/Library/Standards.cfm
Function #s	**Term:** HL7 3.0
1	**Definition:** HL7 version 3.0 is a greatly expanded and more specific data standard suite, building upon version 2.3 and allowing for the messaging of the HL7 records to be done by XML structures. Version 3.0’s Reference Information Model (RIM) is also expanded to include more than just clinical data. HL7 specifications describe 6 basic components. 1) The sets of fields or attributes that make up a message 2) The vocabularies that are needed to enforce consistent data entries in the fields 3) The logical database structure for storing the records 4) The messaging or transport method that the records are shared by 5) The structure of the message to be shared, XML 6) The relationships of the various components in an HL7 message that follow a hierarchy. HL7's primary goal for Version 3 is to offer a standard that is internally consistent, and provide the ability to certify vendors' conformance. Version 3 uses an object-oriented development methodology and a Reference Information Model (RIM) to create messages. The RIM is an essential part of the HL7 Version 3 development methodology, as it provides an explicit representation of the semantic and lexical connections that exist between the information carried in the fields of HL7 messages.
	Rationale:

	HL7 version 3 enables greater specificity for standard data structures for messaging, data storage, and vocabulary usage. In version 3, the relationships between types of data represented in the HL7 model can be understood and represented consistently. The model and message segments are expanded to accommodate pharmaceutical interactions and other data related to public health.
	Related Standards: HL7 version 2.3 could be considered a competing standard to version 3, but the older version is much more difficult to continue to evolve.
	References: http://www.hl7.org/Library/Standards.cfm http://aurora.rg.iupui.edu/v3dt/ITS-XML.html
Function #s	**Term**: HL7 RIM
1, 3, 4, 5	**Definition:** The Reference Information Model (RIM) is the cornerstone of the HL7 Version 3 development process. An object model created as part of the Version 3 methodology, the RIM is a large pictorial representation of the clinical data (domains) and identifies the life cycle of events that a message or groups of related messages will carry. It is a shared model between all the domains and as such is the model from which all domains create their messages.
	Rationale: This model and data dictionary expressed through UML (unified modeling language) is a well-developed generic model for representing, storing, and creation of message content for clinical data information exchange. This model is the industry standard and is supported by the National Committee on Vital and Health Statistics and other national standards setting organization. The overarching structure of the RIM is based on six "core" classes: Act, Entity, Role, Participation, Act_relationship, and Role_link. The HL7 RIM identifies two major "high-level" concepts that are fundamental to understanding the world of healthcare information: intentional "actions" or "services" (Acts), and "people, places and things" that are of interest in the world of healthcare (Entities).
	Related Standards: • Proprietary models – There are a number of variant models that exist in proprietary vendor products. Most all of

	these are either converting to the HL7 model or are extending the export of their data through HL7 standards. • ASTM E31.25 – is a Document Type Definition (DTD)/XML and RIM standard for clinical data handling that could be implemented on a less sophisticated reference model that the full blown HL7 RIM. The model is not as complete though and focused on documentation rather than interapplication messaging of data.
	References: www.hl7.org http://www.hmi.missouri.edu/course_materials/Residential_Informatics/semesters/W2000_Materials/401_hales/hl7_1.ppt http://www.ansi.org/rooms/room_41/paam/hisb247.pdf http://workflow.healthbase.info/monographs/RIM_rationale.html
Function #s	**Term**: HTML 3.0 (Hyper Text Markup Language)
3	**Definition:** HTML is the basic programming language interpreted by a browser. Version 3.0 and up have extensive programming structures such that complex user interfaces can be created and executed by a browser.
	Rationale: By employing a certain level of HTML you allow for the ability to provide very robust application systems over the web. It used to be an issue that the browsers would not support various levels of HTML functionality and you had to write applications to a lowest common level. This is less a problem today.
	Related Standards: • Flash – Specialized web applications that are supported by extensions to a browser execute private languages such as Flash. It is used for graphics and high end screen automation that is generally not well suited to be done in HTML. These types of applications are still launched by HTML though. • Heavy Client/Server applications – Power builder applications are an example of a heavy client application. It is difficult to deploy over an open interface such as a browser across many unknown users' systems.
	References: http://www.w3.org/MarkUp/
Function #s	**Term:** HTTPS
1	**Definition:**

	The Hyper Text Transfer Protocol, Secure version is the protocol used for data movement across a web or TCP based network. The Secure part (S) indicates that the messages sent using HTTP are encrypted between the sender and the browser such that the content of the message cannot be read. This encryption uses the PKI or public key infrastructure to encrypt the data through the X.509 standard. This is also known as SSL encryption.
	Rationale: HTTP allows for data to move between business partners in the same way that data moves between a web browser and a web server. As such it can pass easily though most firewalls and can build upon the web infrastructure. HTTPS is the standard implementation of encrypted HTTP transport that is supported by PKI (Public Key Infrastructure).
	Related Standards: Secure-FTP- This could be construed as a competing standard, but is not oriented to bidirectional, immediate message exchange, and is blocked at many corporate firewalls.
	References: http://www.business2.com/webguide/0,1660,25749,FF.html
Function #s	**Term**: ICD9/10/CM
1, 4	**Definition:** There are two related classifications of diseases with similar titles, and a third classification on functioning and disability. The International Classification of Diseases (ICD) is the classification used to code and classify mortality data from death certificates. The International Classification of Diseases, Clinical Modification (ICD-x-CM) is used to code and classify morbidity data from the inpatient and outpatient records, physician offices, and most National Center for Health Statistics (NCHS) surveys. NCHS serves as the World Health Organization (WHO) Collaborating Center for the Family of International Classifications for North America and in this capacity is responsible for coordination of all official disease classification activities in the United States relating to the ICD and its use, interpretation, and periodic revision. Note that ICD9 codes are used for Mortality data as well as Morbidity. Version ICD10 is only applied to Mortality data currently so we have to pay attention to how the vocabularies are applied even within versions of the same vocabulary.
	Rationale: The focus of this set is for classification of diseases.
	Related Standards:

	None
	References: http://www.cdc.gov/nchs/icd9.htm http://aspe.hhs.gov/admnsimp/faqcode.htm http://www.cdc.gov/nchs/about/major/dvs/icd9des.htm
Function #s	**Term**: Integration Broker
1	**Definition:** There are a number of products and frameworks available that provide much of the plumbing and transformation to share data between dissimilar application and data systems. This is an integration broker. A good example of one is the SAG Entire-X and Tamino products. These are used to access and interface with the Mainframe Natural programs through interfaces such as a COM object, XML, or JAVA.
	Rationale: In some cases providing the access, transformation, and access via an open standard such as ebXML messaging or web service are best serviced through an integration broker. It can be advantageous to buy a COTS broker that already knows how to execute application objects on a mainframe for example. A web application server is an integration broker by providing a middle tier that can handle executing many types of programs and interfaces from a web request or provide support for a web service to different types of back end systems.
	Related Standards: • SAG Tamino/Entire-x • Vitria • Webmethods • TIBCO • Seebeyond
	References: http://www.softwareag.com/corporat/default.htm http://www.webmethods.com http://www.vitria.com http://www.tibco.com

Function #s	**Term**: Intrusion Detection
9	**Definition:** Intrusion protection is an operational procedure where you monitor constantly for someone trying to use your networks or workstations in an unauthorized manner. This can be done by reviewing the logs of open points in your system such as the web server, or you can use various forms of automated software.
	Rationale: Constant monitoring, automated or by hand, is the only way to catch an attack to your systems before you lose control or damage is done.
	References: http://www.sans.org/newlook/resources/IDFAQ/ID_FAQ.htm
Function #s	**Term**: JAVA
3	**Definition:** JAVA is a programming language designed to provide the strength of a complex language such as 'C' and be simplified to use. A general architecture for building JAVA applications is called J2EE, which is a multi-tier structure.
	Rationale: The goal for JAVA is to be able to write code that runs on any platform with minimal or no modification. It is the industry standard for open systems applications.
	Related Standards: • Visual Basic – Microsoft product generally providing heavy client linear program systems. Very unstructured language although easy to program in. • C# - new Microsoft language deployed through .NET and is similar in design to JAVA. Very new and the industry support for the language is well behind JAVA. • COBOL, Fortran, Pascal – still around but look like the dead sea scrolls.
	References: http://java.sun.com/

Function #s	**Term**: JavaScript
3	**Definition:** The other most significant language employed by applications that run on browsers is JavaScript. This is a language that is relatively simple to program in and it provides a lot of capability to a normally limited HTML page. One of the main uses for JavaScript is to provide "edits" on a screen. An example is wanting to tell someone immediately that the format of his or her entered date is not right. This is much better than having to send a date field all the way back to the web server, figure it out there, and then send a whole web page back just to tell them the date is not right.
	Rationale: This common extension to HTML application systems is vital to be able to duplicate the strength of a standalone client server system.
	Related Standards: • CURL – not well known but is a web scripting language. • TCL – mostly used on server side applications.
	References: http://www.wdvl.com/Authoring/JavaScript/Tutorial/ http://www.javascript.com
Function #s	**Term**: JDBC
2, 3, 6	**Definition:** JDBC^{TM} technology is an API that lets you access virtually any tabular data source from the Java^{TM} programming language. It provides cross-DBMS connectivity to a wide range of SQL databases, and now, with the new JDBC API, it also provides access to other tabular data sources, such as spreadsheets or flat files
	Rationale: When writing open standards applications in JAVA the JDBC interface provides the best generic access to a data structure. There are JDBC drivers available for many types of data structures from flat files to industry standard relational databases.
	Related Standards:

	None.
	References: http://java.sun.com/products/jdbc/index.html
Function #s	**Term**: LDAP Directory
1, 7, 8	**Definition:** Lightweight Directory Access Protocol, which is a directory structure for centralized data for authentication, authorization, and general information about a user. The LDAP standard is based on an X.500 standard. The LDAP protocol described a structure for the data, the hierarchy relationships, how the data is described, and an access protocol.
	Rationale: • LDAP provides a standards-based directory of participating personnel with roles and responsibilities which can be used for communication purposes. • LDAP provides a standards-based implementation of authorization and authentication.. • Centralized control of applications, data, and roles is another reason to use a central directory. • The LDAP standard is industry accepted, as the standard interface to all of these types of directories even if they are not storing data in a standard LDAP structure. Microsoft ADS for example uses an LDAP interface for generic access. • The key here is interoperability no matter what the underlying data storage structure.
	Related Standards: • There are many variants of LDAP directory data services available that could be considered competitors, however, the big three, SUN iplanet, Novell, and MS ADS all follow interoperability standards using LDAP as the interface. • MS ADS could be considered a competitor to the standard LDAP directory. ADS was originally designed as a central directory for the windows/desktop environments. LDAP directories were originally designed for internet and network usage. ADS is evolving in the right direction but still lacks features needed for internet-centralized control.
	References: http://www.openldap.org/ http://www.kingsmountain.com/ldapRoadmap.shtml

	http://www.ldapzone.com/004_general_interest.html
Function #s	**Term**: LDIF
1, 7	**Definition:** LDIF (Lightweight Directory Interchange Format) is an **ASCII file format** used to exchange data and enable the synchronization of that data between Lightweight Directory Access Protocol (**LDAP**) **server**s called Directory System Agents (DSAs). LDAP is a software **protocol** for enabling anyone to locate organizations, individuals, and other resources such as files and devices in a network. An LDAP directory can be distributed among many servers. LDIF is used to synchronize each LDAP directory. The first step in synchronizing LDAP directories is extracting the full contents of or a portion of the original LDAP directory and formatting the contents into an LDIF file. The LDIF file is then sent to a directory synchronization handler. Updates to the Public Health Directory could be sent as LDIF structures through the ebXML messaging layer as a payload.
	Rationale: Using a standard directory interface such as LDAP, yields the advantage of applying synchronization through a standard interface such as LDIF. This is an industry standard protocol for DSA integration. This protocol can be structured and passed between systems across any wire protocol.
	Related Standards: • Proprietary interfaces - there are a number of meta-directory products that can react to events that cause data synchronization between directories. The problem is that you need the product. The LDIF standard allows for directory interchange between disparate versions of LDAP and heterogeneous directory environments.
	References: http://developer.netscape.com/docs/manuals/directory/admin30/ldif.htm
Function #s	**Term**: Laboratory Information Management System (LIMS)
4	**Definition:** Laboratory Information Management Systems (LIMS) are application systems used to automate the laboratory sample process. These applications generally handle the tracking of samples, the testing to be applied to the samples, and the results gathering associated with samples.

	Rationale: Application systems such as a LIMS become critical when attempting to electronically gather and share public health clinical data. They establish a centralized point where all lab data is collected and can be standardized to a format such as HL7. Transmission consistent data properly associated with a sample is a great deal easier when employing a LIMS in the architecture. An example of a LIMS is the CDC LITS+ application.
	References: http://www.cdc.gov/ncidod/dbmd/litsplus/default.htm http://www.appliedbiosystems.com/products/productdetail.cfm?prod_id=264
Function #s	**Term**: LINUX
2, 8	**Definition:** LINUX is an open source version of UNIX. It has grown in operational strength and very good user interface support.
	References: http://linux.com/
Function #s	**Term**: Logical Model
2, 3, 5	**Definition:** The database design problem can be stated very simply, as follows: Given some body of data to be represented in a database, how do we decide on a suitable logical structure for that data? In other words, how do we decide what relations should exist and what attributes they should have? We are concerned here with the *logical* design problem only, not the physical design problem. We are trying to produce a hardware-independent, operating-system independent, DBMS-independent - etc., etc. - abstract logical design.
	Rationale: We need logical models to reflect the business relationships and requirements in terms of an IT system.
	Related Standards: N/A
	References: http://dast.nlanr.net/Clearinghouse/DBDesign.html

Function #s	**Term**: LOINC
1, 4	**Definition:** LOINC is a medical terminology classification system. It provides a set of universal names and ID codes for identifying laboratory and clinical test names/ observations. he purpose of the LOINC terminology is to facilitate the exchange and pooling of results, such as blood hemoglobin, serum potassium, or vital signs, for clinical care, outcomes management, and research. Currently, where laboratories and other diagnostic services provide electronic messaging of data. They use HL7 to send their results electronically from their reporting systems to their care systems. LOINC provides a universal identifier for laboratory and clinical observations, so information about observations in electronic messages can be pooled in electronic medical record systems, and research and management databases. It provides a universal ID for HL7 OBX field #3 (Observation ID) in HL7 message. The laboratory portion of the LOINC database contains the content coverage of laboratory testing which includes categories of chemistry, hematology, serology, microbiology (including parasitology and virology), and toxicology; as well as categories for drugs and the cell counts you would find reported on a complete blood count or a cerebrospinal fluid cell count. Antibiotic susceptibilities are a separate category. The clinical portion of the LOINC database includes entries for vital signs, hemodynamics, intake/output, EKG, obstetric ultrasound, cardiac echo, urologic imaging, gastroendoscopic procedures, pulmonary ventilator management, selected survey instruments, and other clinical observations. It provides a universal ID for HL7 OBX field #3 (Observation ID) in an HL7 message or the “test type”. When mapping the concepts to the NEDSS model. *Example Syntax for an HL7 version 2.x data stream using LOINC:* <Analyte/component>:<Kind of property of observation or measurement>:<Time aspect>:<System (sample)>:Scale>:<Method> SODIUM:SCNC:PT:UR:QN

GLUCOSE^2H POST 100 G GLUCOSE PO:MCNC:PT:SER/PLAS:QN

BODY TEMPERATURE:TEMP:8H^MAX:XXX:QN

It is important to note that the data format in the example shows a “^” and “:” delimited set of fields. Following the messaging format standard dictated by HL7 Version 3.x an XML structure providing “named-pairs” of data will be used. Therefore, the last example above would appear as:

```
<Observation>
   <Analyte-component>
   BODY Temperature
   </Analyte-component>
   <Kind of property>
   TEMP
   </Kind of property>
   <Time>
   8H
   </Time>
   <System>
   MAX
   </System>
   <Scale>
   XXX
   </Scale>
   <Method>
   QN
   </Method>
</Observation>
```

Rationale:

Most laboratories and other diagnostic care services identify tests in these messages by means of their internal and idiosyncratic code values. Thus, the care system cannot fully "understand" and properly file the results they receive unless they either adopt the producer's laboratory codes (which is impossible if they receive results from multiple sources), or

	invest in the work to map each result producer's code system to their internal code system. LOINC codes are universal identifiers for laboratory and other clinical observations that solve this problem. LOINC has been endorsed by the Informatics Committee of the College of American Pathologists. American Clinical Laboratory Association (ACLA) has recommended LOINC for adoption by its members. Several organizations including Mayo Medical Group, LabCorp, Department of Defense, Intermountain Health Care, all US veterinary medicine laboratories, etc. have adopted LOINC as a standard. The LOINC codes have been incorporated into the National library of Medicine's UMLS
	Related Standards: • CPT – Also supplies Procedure codes but not as granular as LOINC, Also designed for use in insurance data exchange. • X12N 277 claim status codes – similar but focused for insurance claims but not specific enough for clinical reporting.
	References: http://www.regenstrief.org/loinc/ CONCURRENT 4.3 - SAM GROSECLOSE.PPT (318KB) "Where does Loinc fit in"
Function #s	**Term**: Message Parsing
1	**Definition:** When an electronic message is sent between partners, via HTTP or ebXML, the payload of the message needs to be broken apart so the individual fields of the message can be processed. This is referred to as Parsing.
	Rationale: The technique is required to be able to pass information between applications and make sense of the data on either side.
	Related Standards: N/A
	References: N/A

Function #s	**Term**: Microsoft IIS
2, 8	**Definition:** IIS is the Microsoft web and application server.
	References: www.microsoft.com
Function #s	**Term**: Microsoft NT/2000
2, 8	**Definition:** A Microsoft computer operating system
	References: www.microsoft.com
Function #s	**Term**: Multi-tiered architecture
3, 8	**Definition:** A Multi-tiered architecture is basically designed to separate logical parts of a program. The general view of the tiers breaks down into 3 parts, the user interface, the business rule layer, and the data layer. The J2EE platform is designed as a multi-tier architecture for JAVA applications. The Microsoft .NET architecture is migrating towards this architecture as well.
	Rationale: We design programs across these layers so that we can create a higher degree of reusable and maintainable code. We generally apply the same business rules repeatedly and often wish to present data in varied ways. This might include delivering data to a hand held unit and at the same time deliver the same information to a web page. The goal is to write as many layers of the program once and be able to repurpose the data to the user.
	Related Standards: • Single code, monolithic application systems – Not a good idea because of the maintenance issues and the need for distributed logic in an application system.

	References: http://www.15seconds.com/issue/011023.htm
Function #s	**Term**: NEDSS Logical Model
2, 3, 5	**Definition:** The NEDSS logical model is the conceptual model for the functionality that NEDSS application systems require. This model is based on the HL7 reference information (RIM) model and has evolved to the PHDIM (Public Health Domain Information Model) that incorporates BT and extended public health data structures.
	Rationale: See HL7 RIM
	Related Standards: See HL7 RIM
	References: CONCURRENT 1.2&2.2 - PHDOMAININFOMODEL.ZIP (245KB) This is the NEDSS conference document explaining the PHDIM which the NEDSS base model is based upon.
Function #s	**Term**: Network Vulnerability Analysis
9	**Definition:** This is an analysis that should be performed at regular intervals. Just as constant software patches are required to protect against evolving threats your total systems need to be checked for regular vulnerability. This is usually done against your networks and is based on the latest knowledge on how a network can be breached. Since the attack methods evolve so should your vulnerability testing evolve.
	Rationale: We need to perform this to check for missed, new, or created access points in our networks. This is also imperative to do because our systems change constantly and new issues arise.
	References: http://icat.nist.gov/vt_portal.cfm

Function #s	**Term**: ODBC (Open Database Connectivity)
2, 3, 6	**Definition:** ODBC is a widely accepted application programming interface (API) for database access. It is based on the Call-Level Interface (CLI) specifications from X/Open and ISO/IEC for database APIs and uses Structured Query Language (SQL) as its database access language.
	Rationale: Applications that need to access many types of database systems can often take advantage of the generic data interface being ODBC. It is designed to provide an open access standard to a data structure. ODBC can be very slow and often limit the SQL interaction to a data base.
	Related Standards: • JDBC - the JAVA generic data interface • Proprietary interfaces – Interfaces specific to the database product work more efficiently and provide extended data handling interfaces. An example is Oracle's SQL-Net.
	References: http://www.microsoft.com/data/odbc/default.htm
Function #s	**Term**: Penetration Testing
9	**Definition:** This is done as part of a vulnerability test. The penetration usually employs automated tools to try and break into you network or exposed servers and workstations. The testing is based on known ways that a system can be attacked and will give you some idea how safe you system really is.
	Rationale: Sub component of the vulnerability testing.
Function #s	**Term**: Physical Model
2, 3, 5	**Definition:** The physical model is a derivation of the logical model that takes into consideration the "physical" implementation of the

	model. In this case the actual storage structure is represented in the model. Many times the physical model looks different then the logical because it represents the actual data storage not the reflection of the business function.
	Rationale: A logical model needs to be transformed into a physical model so we understand how the actual IT or application system will really work. This technique guides the developers on how to properly build a system that meets a set of requirements.
	Related Standards: N/A
	References: N/A
Function #s	**Term**: Port Scanning
9	**Definition:** Port scanning is done as part of the vulnerability testing. This goes through a set of IP addresses and their "Ports" to determine if they can be compromised.
	Rationale: This is a sub function of the vulnerability testing that is required to test for TCP/IP ports that are not properly protected or configured.
Function #s	**Term**: Role Based Access
9	**Definition:** When providing control for authorization or access to resources in your systems is makes sense to make the management of this task as easy as possible. Almost every organization has a set of "roles" that govern what people can do and what they can access. These "roles" can also be used to establish access to applications and data. An LDAP directory might contain a list of roles that are associated with a list of User IDs. These roles can then be allowed to drive how an application acts when that User ID uses the program. Example: the Epidemiologist needs to be able to see and access full data manipulation capability for a registry. The data entry person only needs to be able to enter and update single records of the data.

	Rationale: We need to be able to efficiently write application systems that can dynamically change for a type of user. This also gives a reasonable management point for authentication and authorization of application systems.
	Related Standards: • No security control – write many applications of the same functionality and adjust users and security control for each. Very inefficient. • Very granular security and functionality control at an individual user level - not very efficient and often not really needed since most users fall into categories of application usage and security.
	References: http://csrc.nist.gov/rbac/
Function #s	**Term**: Security patches / Configuration corrections
9	**Definition:** Trying to keep a total infrastructure secure and well managed is virtually impossible if there are many different versions and configurations of workstations, operating systems, network configurations being used in an organization. It is required that you maintain a consistent level of operating systems patches, and similar operating systems to be able to catch security and use violations. An example is that an older version of the windows OS may be in use such as windows 98. As time goes on there are well know ways to penetrate and abuse a network through a retired OS. This is a constant battle and why the BT IT specification state the need for COOP that includes this type of activity.
	Rationale: It is well proven that inconsistent management of the many computing systems will provide easy access to penetration of a security policy. An older operating system or ill configured application can provide a “back-door” to be able to enter and control normally secure assets by non-authorized users.
	Related Standards: • Let management get out of hand and uncontrolled providing a viable security threat.
	References: N/A

Function #s	**Term**: Security Policies
9	**Definition:** These policies govern how your systems are design, used, and managed. Security policies are critical to be able to know you have control of your systems.
	Rationale: IT systems alone do not make a successful security plan. The policies govern the behavior and design of security compliance.
	Related Standards: N/A
	References: http://csrc.nist.gov/policies/
Function #s	**Term**: Security Policy Monitoring
9	**Definition:** At regular intervals your organization should review your security policies and make sure they are being followed and implemented as you intended. These include policies for physical locations such as building, behavior of your staff, and the implementation of your computing systems.
	Rationale: Systems, culture, business requirements change and so should your security policies to continue to be viable.
Function #s	**Term**: SMTP (Simple Mail Transport Protocol)
Commitments	**Definition:** The protocol followed in moving email around
	Rationale: Industry standard for email transmission.
	References: http://www.ietf.org/rfc/rfc0821.txt

Function #s	**Term**: SNOMED (Systematized Nomenclature of Medicine)
1, 4	**Definition:** SNOMED is a controlled medical terminology with comprehensive coverage of diseases, clinical findings, etiologies, procedures, and outcomes used by physicians, dentists, nurses, and allied health professionals. The SNOMED CT version comprises hierarchical concepts of terms that encompass the following areas. Procedure/Interventions Finding/disorder/observations Measurable /observable entities Social/Administrative concepts Body Structure/morphology Organisms Substances Physical Objects Physical Force Events (excluding procedures and interventions) Environmental /geographic locations Specimen Modeling concepts (Context-dependent categories, Attributes, Qualifier values) There are different sets of SNOMED vocabularies. SNOMED CT - Clinical Terms is a new version that combines the older versions of SNOMED RT – Reference Terminology and Clinical Terms. The HL7 Version 2.x would provide a universal ID for HL7 OBX field #5 () in an HL7 message or the “test result” When mapping the concepts to the NEDSS model.
	Rationale: The reason for employing this vocabulary and hierarchy of codes is the same as applying the LOINC and other code sets. The absolute need for similar data encoding. Employing the SNOMED set as part of the overall standards is required for

	specific areas to the BT data sharing domain. *A specific set of SNOMED concepts and dominance over the other overlapping code sets will be supplied as part of the standard declaration.* For the moment standards bodies such as SNOMED provide mapping tables between the various code sets.
	Related Standards: • CPTs - overlaps in procedures/interventions concept • ICDs – overlaps in Events and Findings, etc • LOINC – overlaps on findings, measurables, etc.
	References: http://www.snomed.com/ Organism List to Organism Mapping (SNOMED)
Function #s	**Term:** SOAP
1	**Definition:** Simple Object Access Protocol – This is the protocol for transmitting XML-based messages between listeners like a web service. The protocol also defines how to start a program or method on the target end. SOAP is a building block for the ebXML messaging standard. SOAP allows us to send payloads of information such as an XML-based observation record, declare where it should go, and how the data should be handled once it gets there. All this is done through a well-known standard so that anyone wishing to use this protocol will understand it when sending or received data via the protocol. SOAP also allows for different types of payloads that can be diverse such as an xml data structure or a binary graphic file.
	Rationale: SOAP is a cross platform industry standard that provides a basis for higher level specifications such as ebXML. Standardizing on SOAP solves a number of problems about how a message payload is to be structured, where it is sent to, and how it is to be interpreted or handled. This done through a known standard structure and conversation. This protocol can be used over many wire transport protocols.
	Related Standards: • CORBA IIOP/IDL – describes how a message or object is accessed but is tied to the cumbersome CORBA standard architecture.

	• REST - Representational State Transfer (REST), which is a new proposed process that expands on reliable HTTP interactions. The REST protocol is very new and not much of a following but does work to expand on the functionality provided by with SOAP. • XML-RPC– SOAP is based on this protocol, but XML-RPC is a specification and varies in implementation so no single convention widely adopted. • DCOM – Like IIOP this protocol has not adapted well to the internet and requires considerably more dedicated computing power to take advantage of the services.
	References: http://www.vbws.com/book/chapters/view.aspx?c=3 http://www.w3.org/2000/xp/Group/2/06/06/soap12-part1.html http://www.w3schools.com/soap/default.asp
Function #s	**Term**: SSL
1, 3, 6, 8	**Definition:** The primary goal of the SSL (Secure Sockets Layer) Protocol is to provide privacy and reliability between two communicating applications. The protocol is composed of two layers. At the lowest level, layered on top of some reliable transport protocol (e.g., TCP), is the **SSL Record Protocol**. The SSL Record Protocol is used for encapsulation of various higher-level protocols. One such encapsulated protocol, the **SSL Handshake Protocol**, allows the server and client to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before the application protocol transmits or receives its first byte of data.
	Rationale: One advantage of SSL is that it is application protocol independent. A higher-level protocol can layer on top of the SSL Protocol transparently. SSL is also the industry standard for message transport encryption on the web. It is also a standard for basic authentication on web application servers.
	Related Standards: • Private encryption – We can still use an open transport such as HTTP and handle all the encryption using a proprietary standard between applications. The problem is supplying this in every application when there is a viable “first defense” standard (SSL) already understood and implemented by browsers and application servers.

	References: http://www.openssl.org/
Function #s	**Term**: Standard Code Set (vocabulary concepts)
1, 4	**Definition:** When a field in the data record can use a standard set of codes it becomes possible to link records because you have a consistent set of data to work from. This is called using a “Standard Code Set”. The other term for this is using a vocabulary. Examples of vocabularies are the CPT codes. LOINC, HL7, and ICD contain codes but are more complex standards referred to as vocabulary concept standards. Most of the vocabulary standards are actually combinations of code, taxonomies, concepts, and other uniform data structures. A separate paper will be supplied to explain in further detail how these function and apply to the data schemas such as the NEDSS logical model.
	Rationale: The holy grail for data sharing is to be able to view or analyze a set of data knowing that the fields or attributes contain uniformly defined data. It is inefficient and in some cases close to impossible to correlate data that has used no coding standard or even a private set.
	Alternative Approaches: • Do nothing – and not be able to link and share data.
	References: http://aspe.hhs.gov/admnsimp/faqcode.htm http://www.claredi.com/hipaa/codesets.php
Function #s	**Term**: Standard Data Format
2	**Definition:** When data can be stored in a consistent set of fields and record layouts it allows for the data to be linked logically. A well thought through logical model generally handles many types of data and can be considered a “standard data format” The Public Health Domain Information Model, which NEDSS is based on, is such a logical model.
	Rationale: The goal for using a standard data model is similar to why we want to use standard vocabularies. We want consistency in

	the data so that we can provide linkage and analysis that makes sense.
	Related Standards: N/A
	References: N/A
Function #s	**Term**: Strong Authentication
1, 3, 6, 8	**Definition:** Strong authentication is ensuring that a requestor for a web resource is actually who they say they are. There are a number of techniques used for this that include the following. (SSL (Secure sockets layer), Digital Certificates, Tokens) The primary goal of this authentication method is to implement a strong authentication system that eliminates (so far as practical) the transmission of clear text re-usable passwords over the network and their storage on local systems.
	References: http://www.cdc.gov/nedss/Security/Secure_Data_Network3.pdf http://www.cdc.gov/nedss/Security/Security_InfoNB_Sys_Sites_V01.pdf http://archive.ncsa.uiuc.edu/SCD/Alliance/GridSecurity/Certificates/Strong.html
Function #s	**Term**: UNIX
2, 8	**Definition:** An operating system often used on servers. It is very robust and easy to manage but can be terse to learn.
	References: http://unix.oreilly.com/
Function #s	**Term**: Virus Scanning
9	**Definition:** Electronic viruses are a way of life. We have to make sure that we all systems protected to stop the disruption these

	programs can cause. There are many virus-scanning systems available that run on workstations, servers, and even firewalls.
	Rationale: Virus protection is an imperative COOP standard to protect from disrupted systems.
	Related Standards: • McAfee • Norton
	References: http://www.norton.com/
Function #s	**Term**: Vocabularies
1	**Definition:** See "Standard Code Sets"
	Rationale: N/A
	Related Standards: N/A
	References: N/A
Function #s	**Term**: Web Browser Data Entry
3	**Definition:** Browser-based applications generally run HTML and JavaScript to interact with a user. The idea is to be able to download all of the code required for the application at the time it is accessed. This might also be referred to as a "light client". There are limitations because HTML and JavaScript can only do so much. However, employing tools such as Style Sheets almost every Client/Server type of functionality can be duplicated in this type of application.

	Rationale: The main reason for deploying this type of application system is to take advantage of the ease of management. Since the code is centralized it is easier to control versions, connectivity across distributed components, and maintain a consistent interface. It is important to remember to employ multi-tier architectures when building browser-based applications. This will allow the application to service not only a browser-based system but also use the same business logic for a stand-alone application.
	Related Standards: Light Client or browser-based applications are not always appropriate. In the case were we do not have network connectivity a "stand-alone" application is required that will sync back up or interface to a centralized system when possible. An example of this might be employing a handheld unit and application to enter data in a hot area with no viable wireless networks.
	References: N/A
Function #s	**Term**: Web Service
1	**Definition:** A web service is an integration approach for implementing distributed application systems. The difference between a web service and other integration frameworks such as "Tibco, or Vitria" is that there is no middleware framework. It is designed to be a "listening post" for a standard message that all distributed applications will understand. This "listening post" can be discovered through a registry called a UDDI or EBXML registry, which also tells the remote application the following things. 1. What you are 2. How to talk to him 3. What methods can you invoke 4. How to bind, or offer the correct parameters to execute the methods 5. What security attributes are to be followed. All of the conversations employ a message content in XML and travel along a "wire protocol" called SOAP. SOAP is the glue that holds the rules for carrying messages to the web services and how to execute the methods that the web service offers.

	EBXML is similar to a web service in that the messaging payload layer of ebXML is doing the same thing as the SOAP interface in a web service. The ebXML interaction is more secure and reliable for exchanging messages that expect an action.
	Rationale: A web service is an open interface architecture that is very useful to consider for some of the services we deliver in the BT IT specifications. Where we don't need the controlled pipeline interaction for data sharing this is a simple data interface to employ. The basic web service is a sub component of the ebXML standard which provides the "handler" aspect of the message processing. There are situations where a web service provides an excellent integration architecture.
	Related Standards: • Proprietary information brokers – products such as VITRIA provide a similar functionality only tightly control the communications between the interacting parties. The web service uses an open standard to interact. • EDI – uses a very closed and controlled environment.
	References: http://www.vbws.com http://www.webservices.org
Function #s	**Term:** X12
1	**Definition:** X12 is an EDI protocol for sending healthcare related business transactions. ASC X12N has created a number of message standards for the insurance side of health care including: Benefit Enrollment and Maintenance - 834, Health Care Claim Payment/Advice - 835, Health Care Claim - 837, and Health Care Eligibility/Benefit Inquiry - 270. X12 is also developing a message for sending patient information (Patient Record Data - Response and Request - 274 and 275). X12 is also a key HIPAA standard. A message structured in this format can be transmitted across the ebXML message layer as a payload.
	Rationale: There is useful data contained in the data segments traded between insurance partners and medical professionals that are transmitted via the X12 standards. Therefore, while X12 may not be a suitable as the basis for developing clinical or

	public health transactions, it is important to be able to accept X12 data and move them across the same industry standard transport system, ebXML.
	Related Standards: EDI would be the traditional way to transmit X12 messages. EDI infrastructure is based on private networks that are not generally available to public health departments. EDI does not take advantage of the ubiquity of the Internet and in clinical institutions is principally oriented to the exchange of billing or reimbursement data.
	References: http://www.x12.org/ http://www.hl7.org/standards/x12.htm
Function #s	**Term**: X.509
9	**Definition:** X.509 is the standard for using "PKI" or public key infrastructure for validating messages that are sent between partners. The CDC SDN provides such a Digital Certificate that allows for authentication of a person asking for access to a web page or other web resource.
	Rationale: This is the industry standard for providing digital certificates in a secure, validated web environment
	Related Standards: • Kerberos • Secure ID
	References: http://www.ietf.org/html.charters/pkix-charter.html http://www.ietf.org/internet-drafts/draft-ietf-pkix-roadmap-08.txt http://www.cdc.gov/nedss/Security/Secure_Data_Network3.pdf
Function #s	**Term**: XML (Extensible Markup Language)
8	**Definition:** XML is actually a "metalanguage" -- a language for describing other languages - which lets you design your own customized markup languages for limitless different types of documents. XML can do this because it's written in SGML,

	the international standard metalanguage for text markup systems (ISO 8879).
	Rationale: The main key to XML is that it publishes data or information in a “self-describing” manner. This allows you to understand the label for the data; the type of the data and any relationship one data item has with another in the same set of XML
	Related Standards: • SGML • Proprietary data standard structures
	References: http://www.xml.org/xml/news_market.shtml http://www.xml.org/xml/resources_cover.shtml http://www.xml.com/