

Contents

1.0	EXECUTIVE PROJECT APPROVAL TRANSMITTAL	2
2.0	IT PROJECT SUMMARY PACKAGE	3
3.0	BUSINESS CASE	4
	3.1 Business Program Background	4
	3.2 Business Problems and Opportunities	8
	3.3 Business Objectives	11
	3.4 Business Functional Requirements	13
4.0	BASELINE ANALYSIS	18
	4.1 Current Method	18
	4.2 Technical Environment	27
5.0	PROPOSED SOLUTION	29
	5.1 Solution Description	29
	5.2 Rationale for Selection	35
	5.3 Other Alternatives Considered	37
6.0	PROJECT MANAGEMENT PLAN	40
	6.1 Project Management Plan	40
	6.2 Project Management Methodology	40
	6.3 Project Organization	41
	6.4 Project Priorities	42
	6.5 Project Plan	42
	6.6 Project Monitoring	47
	6.7 Project Quality	49
	6.8 Change Management	49
	6.9 Authorization Required	50
7.0	RISK MANAGEMENT PLAN	51
8.0	ECONOMIC ANALYSIS WORK SHEETS	64
	APPENDICES	65
	• Appendix A – CCR Title 17, Section 2505	
	• Appendix B - PHIN Cross Functional Component Self Assessment Tool	
	• Appendix C – Acronym List	
	• Appendix D – Department ISO Requirements	

1.0 EXECUTIVE PROJECT APPROVAL TRANSMITTAL

The following are the formal signature pages as required for the Department of Health Services acceptance of this Feasibility Study Report, and subsequent submittal to the DOF for the proposed information technology project.

These pages are included as separate files in the electronic version of this FSR.

2.0 IT PROJECT SUMMARY PACKAGE

The following is the Information Technology Project Summary Package prepared as required by DOF.

The Project Summary Package is included as a separate file in the electronic version of the FSR.

3.0 BUSINESS CASE

This section identifies the problems of and opportunities for the Division of Communicable Disease Control (DCDC) that are related to the laboratory reporting process, including consideration for the linkages to other division efforts coordinated with this effort to improve statewide disease surveillance. However, the focus and scope of this study and resulting project is confined to the statewide laboratory reporting process.

3.1 Business Program Background

California Public Health

Public health is supported by an array of local, State, and Federal organizations. These partner organizations are further divided into functional units that support clinical, health department, laboratory, disease program, and other operational divisions¹. California's public health system includes a network of people, information systems, organizations, and public health processes focused on the health of the State's population. The California Department of Health Services (CDHS) administers the public health system in California at the state-level. Sixty-one local health departments (LHD) – comprising the 58 counties and the cities of Berkeley, Long Beach, and Pasadena – manage the public health system at the local level.

The CDHS, through the Division of Communicable Disease Control (DCDC), is responsible for investigating and controlling communicable diseases and conditions in the State. The DCDC works in partnership with local, national, and international health officials, health care providers, and the public to monitor health trends. Through this monitoring process, termed "surveillance", the State is able to identify new and emerging conditions, control outbreaks, investigate existing and potential health problems, develop and implement prevention strategies, conduct research, provide education and training, and formulate and advise on public health policy. Surveillance is needed to detect epidemics, emerging or re-emerging infectious diseases, and bioterrorist events.

While there are many surveillance strategies, disease reporting originating from health care providers and laboratories is at the core of surveillance. State and local health departments rely on disease reports from clinicians and laboratories to rapidly identify and respond to outbreaks and other communicable disease problems, including the following activities:

¹ Centers for Disease Control and Prevention. "Notice of Cooperative Agreement Award, Public Health Information Technology Functions and Specifications." February 8, 2002.

- Determine the extent of the morbidity in the population (at the state and local level)
- Evaluate risks of transmission
- Intervene rapidly when appropriate
- Identify outbreaks and epidemics
- Develop prevention programs, identify core needs, and use scarce prevention resources efficiently
- Provide efficient and effective education and treatment programs
- Evaluate the success of long-term control and intervention efforts
- Facilitate epidemiologic research
- Assist with national and international disease surveillance efforts

Currently, disease reporting is mandated by the California Code of Regulations, Title 17, Sections 2500 and 2505. Section 2500 requires physicians to report incidents of specific diseases or conditions to the LHD in the jurisdiction where the patient resides. Section 2505 lists a subset of diseases that must be reported by laboratories to the Local Health Department of the referring physician. The LHDs then forward the confirmed disease case reports (regardless of whether initially reported by a provider or a laboratory) to the State in either electronic or paper format. State staff collects, aggregates, processes, analyzes, and disseminates data from LHDs on all reportable diseases. This information is used as described above to support epidemiological studies, and to satisfy national (CDC) reporting requirements. Detailed background information on disease reporting, and the relevant objectives and organizational structures of CDHS and DCDC, can be found in the FSR for provider reporting systems (“WebCMR”).

Federal Public Health Initiatives

At the national level, the Centers for Disease Control and Prevention (CDC) initiated an effort to streamline the collection, management, and reporting of data – primarily for the surveillance of communicable diseases. In 1999, the CDC introduced the National Electronic Disease Surveillance System (NEDSS) to promote the use of data and information system standards.

The CDC designed the NEDSS initiative to (1) facilitate the electronic transfer of appropriate information from clinical information systems used in the delivery of health services to public health departments; (2) reduce the burden on health service providers of collecting and reporting such information; and (3) enhance the timeliness and quality of public health information. NEDSS seeks to advance the development of efficient, integrated, and interoperable disease surveillance systems at all levels of public health administration. Specifically, the CDC’s goals for NEDSS are to:

- Emphasize, adopt, and promote national standards for the electronic exchange of information
- Foster integration of surveillance and health information systems

- Support the development of surveillance systems according to a defined information systems architecture
- Develop direct electronic communications between sources of data (such as health care providers or laboratories) and public health agencies
- Facilitate the ready exchange of data, as appropriate, between local and state health departments, among states and between states and the CDC

In late 2002, the CDC introduced the concept of the Public Health Information Network (PHIN). PHIN provides a network of information that functionally and organizationally integrates public health partners across the country. PHIN includes specific CDC initiatives that suggest the importance of this type of public health information technology integration. These include NEDSS, the Health Alert Network (HAN), the Laboratory Response Network (LRN), the Epidemic information Exchange (EPI-X) and the redesign of the CDC web site for public information and public health education. PHIN requirements include:

- An interoperable network – built on the Internet using industry standards to work with other networks/systems
- Support users – provide information and decision support to the public and public health professionals at all levels
- Live data – continuous monitoring of the nation’s health, continuous detection and evaluation of threats
- Dual use – meet BT preparedness and response needs, and transform routine public health practice into more efficient processes
- Engage industry – set direction for private sector participation and develop commercial and clinical opportunities
- A common data language – use of industry standards for comparable data use and exchange

Under this initiative CDC began providing funds to those public health jurisdictions reporting public health data to CDC and who are working to develop or procure applications that comply with the requirements identified above. CDC announced in 2005 that awardees of PHIN Preparedness grant funds would be required to begin the evaluation process required for certification to PHIN standards by August 2006.

The CalPHIN Initiative

The CDHS initiated the California Public Health Information Network (CalPHIN) initiative to support the CDC efforts and promote the public health goals of the State. CalPHIN demonstrates California’s commitment to adopting the NEDSS standards and supporting the PHIN philosophy of sharing information and technology resources among surveillance systems. The DCDC developed a CalPHIN Strategic Plan for incorporating the NEDSS elements and information sharing concepts of PHIN into the State’s disease surveillance systems. The strategic plan links the objectives of the NEDSS initiative with the goals set forth in the broader CDHS

Strategic Plan, and demonstrates how CalPHIN will help address important issues facing the CDHS.

Applications included within the CalPHIN framework are:

- California Electronic Laboratory Reporting (CA-ELR)
- California Web Based Morbidity Reporting (WebCMR)
- California Health Alerting Network (CAHAN)
- Laboratory Information Management System (LIMS) for California State Laboratory Complex in Richmond

History of Electronic Laboratory Reporting

Prior to the CDC recognition of the need for PHIN, CDHS identified the need for additional surveillance capabilities for disease tracking and emergency notification. With its partners in public health, CDHS has researched the significant problems with surveillance reporting and identified various means to expand the use of information technology to improve these activities. In 1996, CDHS convened the Electronic Laboratory-based Reporting Task Force (ELRTF), consisting of representatives from CDHS (laboratorians, epidemiologists, and information technologists), clinical laboratories, public health laboratories and software developers, to plan and coordinate electronic laboratory reporting (ELR) efforts in California.

ELRTF identified several areas having significant impact on the success or failure of an ELR system. One was the current lack of a common data formats for the electronic exchange of information. A common format is necessary for efficient communication among the numerous State, laboratory, providers and LHD partners. The State cannot function with a separate electronic message format for each LHD or laboratory. Rather than invent a one-of-a-kind format and carry the entire burden of its support, ELRTF focused on the Health Level Seven® (HL7) message format. HL7 is an ANSI standard messaging format that has become a recognized standard in healthcare industry electronic communication, widely used among health care providers and increasingly so in government.

Another problem identified was the inconsistent coding system for laboratory tests. Different scientific specialties have often developed their own coding standards that may conflict within overlapping areas. Laboratories and providers also tend to develop their own proprietary codes. Recently the Logical Observation Identifiers Names and Codes (LOINC®) standard has received widespread acceptance as a response to this situation. LOINC provides a common coding database allowing sending and receiving agencies to speak the same electronic language. The LOINC database of an estimated 36,000 different laboratory tests, clinical observations and supporting material is publicly available at: <http://www.loinc.org>

A similar need is a common coding schema for medical descriptions and observations. The Systematized Nomenclature of Medicine (SNOMED®) provides a common medical terminology, enabling the recording, storage, retrieval, and

analysis of clinical information. The SNOMED CT Core terminology contains over 366,170 health care concepts with unique meanings and formal logic-based definitions organized into hierarchies. As of July 2005, the fully populated table with unique descriptions for each concept contains more than 993,420 descriptions. Approximately 1.46 million semantic relationships exist to enable reliability and consistency of data retrieval. The SNOMED standards are maintained by SNOMED International, a not-for-profit division of the College of American Pathologists. Additional information regarding SNOMED is available at: <http://www.cap.org>

In response to the ELR needs, the DCDC has successfully implemented both a demonstration and a pilot electronic laboratory reporting project which prove the viability of statewide electronic lab reporting. For the demonstration project, an internal proof-of-concept project was initiated in late 1999 involving the use of HL7 messaging and integration broker software to move laboratory data from the State's Microbial Disease Laboratory (MDL) test system to a CDHS Information Technology Services Division (ITSD) database. This was followed by a the formal demonstration project that was completed in Fall 2001 that demonstrated the capability of collecting electronic laboratory reports in a consolidated reporting environment and generating disease alerts based upon business rules established for specific diseases. The California Electronic Laboratory Disease Alert and Reporting (CELDAR) system was successfully demonstrated through a joint effort of the DCDC, ITSD, and IBM. The demonstration project was based upon receiving "dummy" laboratory test transactions from several laboratory partners, including MDL, local public health laboratories, and the State veterinary diagnostic laboratory, collecting the laboratory information in a common database, and generating an alert (e.g. pager, mobile phone, and e-mail) for specific diseases. The CELDAR Pilot was active from January 7, 2002 through March 20, 2003 and identified the following objectives:

- The development of a standard process for the submission of laboratory reports
- Provide Web-enabled reporting capability
- Create a secure environment for the transmission and retention of confidential patient information

The project's Post-Implementation Evaluation Report (PIER) concluded the pilot successfully met the stated objectives. The results of the demonstration and pilot projects have provided DCDC with a set of clear, concise business and system requirements, as well as proof that the theoretical concepts can be successfully applied in a current non-production laboratory reporting environment.

3.2 Business Problems and Opportunities

Based on an analysis of the current processes, four critical issues have been identified that relate to communicable disease surveillance activities. The following concerns are critical for the CDHS to address in its implementation of a solution through an Electronic Lab Reporting (ELR) System.

1. Limited information technology and systems are available to public health staff to collect and process disease data. The process does not take advantage of current technology and limit staff's ability to process increasing amounts of information.
2. Current methods for collecting information about communicable disease are outdated. The paper-intensive data collection methods are burdensome, time-consuming, redundant, and error prone.
3. Health care providers and laboratories are not reporting information about notifiable disease conditions in a consistent manner. The paper-intensive process impedes timely and accurate reporting of communicable diseases. Additionally, laboratories have little incentive to report diseases to the LHDs, and the inefficient processes that exist for reporting make such more difficult for the laboratories.
4. The State's disease reporting methods and formats are not standardized. Both LHD and State surveillance staffs must contend with a variety of input formats (electronic and paper-based) and maintenance of data. In addition, the existing systems do not meet the CDC's PHIN standards and specifications.

The following section further describes and discusses these critical business issues.

Problem 1 – Limited Information Technology and Systems are available to Public Health Officials to collect and process disease data.

- 1a. The current reporting process requires providers to submit laboratory reports through the mail, facsimile, or phone. The data collection process is not automated and the handling of paper and multiple data entry is a cumbersome process for local and State public health surveillance staffs. In addition, the current paper-intensive reporting processes does not provide a secure and confidential environment for sensitive public health information.
- 1b. Laboratory reports submitted to the wrong LHD. Many times laboratories submit disease reports to the incorrect jurisdiction, or the receiving LHD determines that the report belongs in another jurisdiction. There is no automated process to complete the transfer of disease report data from one LHD to another. The current method involves a substantial amount of manual effort on the part of both the transferring and receiving LHDs.
- 1c. As a result of the manual processes in place, significant effort is required to cleanse and convert current data received from various public health partners. The CDHS Surveillance and Statistics staff spends significant time filtering and cleansing the disease report data to create meaningful information for analysis and further reporting.

Problem 2 - Current Methods for Collecting Information about Communicable Disease are Outdated

The data collection method is both paper and staff intensive. The nature of the problem involves:

- 2a. Labor-intensive data collection. The current process includes a significant amount of manual intervention. The process includes laboratories completing a paper form and sending to the LHD where staff then enters the data into one or more systems. The manual effort creates problems including data entry errors, redundant data collection processes, and mailing costs.
- 2b. Redundant data collection and entry processes. Many LHDs lose time and money by performing double data entry of the demographic data into several information systems (at least one for reporting and one for case management). This redundancy increases the workload for LHD public health staff.
- 2c. Time-consuming processes. No matter how the disease reports are transmitted (e.g., facsimile, mail, phone), significant delays are inherent in the time for laboratories to complete the disease report, send it to the LHDs and, ultimately, enter the CDHS reporting process. As new pressures for early detection of disease outbreaks arise, most notably for outbreaks from bioterrorism, it is critical that public health officials have timely and accurate information to develop appropriate responses.
- 2d. Lack of data interaction between LHDs and the State specifically for laboratory reporting. The laboratory disease report information ends up as part of the case report at the LHD, and the data flow from the LHDs to the State is one-way. Once the data is sent to the State, it is difficult for LHDs to query, edit, or track submitted data or perform regional trend analysis. LHDs only have access to the data in their system. If the data are modified in their systems, there is a difference than what exists in the State system, and LHD staff is unable to access data in the State-level systems for comparison. As a result, LHDs cannot perform epidemiological reviews of data from the State's database in a timely manner. Further, there is no separate statewide laboratory reporting system – centralized aggregation and evaluation of laboratory reports is completely dependent on the antiquated disease reporting systems at the local level resulting in delays and incomplete reporting.
- 2e. Current processes do not adequately protect private health information. The public health systems have an obligation to protect the confidential health information of individuals that has been identified with specific communicable diseases. Inadequate protection of health information has significant financial, legal, regulatory, and business continuity repercussions, including civil and criminal penalties. Manual, paper-based processes may not have the ability to incorporate adequate measures to maintain the confidentiality of private health information.

Problem 3 - Laboratories are Not Reporting Notifiable Disease Conditions in a Consistent Manner

The current reporting structure results in inconsistencies in disease reporting. The nature of the problem involves:

- 3a. Redundant reporting process. There are instances when a case is required to be reported by the physician, the laboratory that initially receives the specimen, and a State laboratory. The opportunity for double counting of a single case increases due to these multiple reporting mechanisms. In addition, when a report is to be submitted by both the physician and laboratory, neither may follow through due to the assumption that the other entity will generate the report.
- 3b. Paper-intensive reporting process. Most laboratories do not have an automated method to report disease reports. They rely on paper-based processes that may be inconsistent, or are inefficient in creating and submitting the information to the appropriate LHD. This may result in the under-reporting of many diseases. In addition, there are no automatic filters or data validations to verify completeness or correctness of the information.

Problem 4 - The State's Disease Reporting Methods and Formats are Not Standardized

Both State and local public health staff must contend with a variety of input formats in laboratory reporting process. The nature of the problem involves:

- 4a. Lack of standards and formats. Reporting to the State is completed in multiple, non-standard formats by the LHDs. This requires highly skilled statisticians to reformat and normalize disparate data formats. This lack of standards and consistency results in multiple data transformations and increases the possibility of errors.
- 4b. The current process is a compromise in data accuracy and validity. Due to the many transformation and edits, much of the original data from the source is lost in State-level systems. In addition, this results in duplicate effort (data entry and manipulation) and the inability to share information among public health entities.
- 4c. The health care industry and the CDC have identified, and are promoting, standards (i.e., HL7, LOINC, SNOMED) for common communication of public health data. The State and local disease surveillance staffs have not fully implemented these standards in the laboratory disease reporting process.

3.3 Business Objectives

The overall objective of an Electronic Laboratory Reporting application is to enhance and strengthen State and local disease surveillance capacity and promote public health. This type of application will improve the ability to collect more complete and timely surveillance information from laboratories on a statewide basis used to increase the efficiency of existing surveillance activities and the early detection of public health events (e.g. bioterrorist). This will be accomplished through automating manual processes such as data importing and accuracy verification, decreasing paper-based data submittals, eliminating data redundancy and duplicate data entry, and providing easy accessibility to data for planning, analysis, and decision-making.

Specifically, the proposed solution will provide a mechanism for the CDHS to collect and manage laboratory data more efficiently and effectively by:

Business Objective		Solves Business Problems
1.	Provide an automated means of laboratory reporting and notification with a single, statewide lab reporting system.	1a, 1c
2.	Eliminate outdated manual reporting submissions	1b, 1c, 2a, 2b, 2c, 4b
3.	Create a secure environment for confidential medical information to reside, restricting access to the data for reporting purposes	2e
4.	Reducing elapsed time to collect data from LHDs measured from time of test to the time CDHS receives notification.	2a, 2b, 2c, 3b
5.	Increase laboratory reporting from lab partners by eliminating current manual processes.	1a, 3b
6.	Enable the sharing of data across LHDs and public health program areas and business functions	1b, 2d, 3a
7.	Establish a standard vocabulary and process to share standard data elements and formats statewide	4a, 4c

It is important to note that business objectives numbers 4 and 5 do not state specific measures of improvement. Current baseline measures do not exist and will need to be developed prior to the project to ensure proper measurement of project objectives.

3.4 Business Functional Requirements

Listed in the table below are the business requirements, identified to date that the proposed electronic laboratory reporting solution must support.

Business Requirements		Meet Business Objectives
General		
Overall		
1.	The solution must provide a single web entry point (i.e., web portal) for all laboratories to submit required reports.	2, 5
2.	The solution must provide a single data repository for laboratory-reportable disease reports that will be accessible to authorized CDHS staff.	3
3.	The solution must provide authorized users from CDHS divisions and programs (e.g., DCDC, TB Control Branch, STD Control Branch, LHDs) access to data contained within its database.	3
4.	The solution must utilize a standard naming convention and codes for all laboratory related data (e.g., LOINC, SNOMED).	7
5.	The solution must ensure complete, accurate, and standardized data entry through enforcement of business rules and edits.	7
6.	The solution must be able to accommodate additional data elements.	6
7.	The solution must provide the ability for authorized CDHS staff to export defined datasets and data reports for external data analysis	6
8.	The solution must maintain historical records on patient case data.	6
9.	The solution should be developed using technology that exists in the CDHS technical infrastructure.	1
10.	The solution must have the data backed up on a regular basis and accessible for quick recovery, if necessary.	1
11.	The solution must retain data for reporting purposes for the current year plus the 5 most recent calendar years.	6
12.	The solution must have the capability to perform a master file update of add changes and deletes to the data.	1
13.	The solution must provide an easy-to-use mechanism	6

	to search for information within the database.	
14.	The solution must generate appropriate notifications when problems or systems failures occur.	1
15.	The solution must be easily maintainable and scalable for additional laboratories.	1
16.	The solution must be able to create and maintain a journal of all messages and data received, processed, and updated. The journal must identify the date, time, and submitter of the data.	1
17.	For auditing purposes, the solution must track all reports and alerts that are generated from the data. The results of the alert or query will be logged indicating the date and time of the request, who made the request, and the individuals receiving the results.	1
18.	The solution must provide an interface that consists of easy-to-navigate menus, pick lists, on-line window and field help with visually distinguishing optional and required fields.	1
19.	The solution must assign and maintain unique user logon ids and passwords.	1
20.	The solution must support data capture and storage about patients, submitters, providers, and specimens transmitted electronically in a safe and secure manner.	3, 4
21.	The solution will validate the data, translate it into the appropriate formats, check for inconsistencies or lack of completeness, and load the data into a database.	3, 4
22.	The solution will notify the submitters of any and all errors in the data.	1
23.	The solution should be developed using technology that exists in the CDHS technical infrastructure whenever possible.	1
24.	The solution will have a 24-hour, seven-days-per-week uptime.	1
Interactions with Other Systems		
25.	The solution must interface with or accept downloads of data from external systems, including other CDHS, state, local, and federal systems.	6
26.	The solution will be separated from other CDHS program data to prevent unauthorized access or entry. Separation of data and communications between the solution and other systems, specifically, no "logged on to the network" traffic is supported from clients of other applications on the same physical and/or logical network segments.	3
27.	The solution must be able to transmit message	2, 6

	transactions to other ELR/CMR applications.	
Security		
28.	The solution must provide security to limit access to system functions, data, and reports based on role and responsibilities.	3
29.	The solution must provide appropriate security levels to ensure that only authorized users can read and/or update data.	1
30.	The solution must meet the requirements of the CDHS, ITSD, Information Security Office for transmission and retention of confidential patient information.	1
31.	The solution must authenticate HL7 messages and data files from laboratories to ensure the submitter is authorized to send data to the system.	2, 7
32.	The solution will support all CDHS documented Health Insurance Portability and Accountability Act (HIPAA) requirements.	1
33.	The solution must have the capability to identify approved individuals to access the data, to download data, create reports for epidemiological studies, and evaluate trends to take public health actions.	1
34.	The solution must authenticate reporting requests from laboratories, LHDs, and CDHS to ensure access is provided only to individuals approved for access.	3
35.	The solution must be separated from other CDHS program data to prevent unauthorized access or entry.	3
36.	The solution should perform all transactions using an integrated security model that will support the CDC Health Alert Network (HAN), Secure Data Network (SDN) and National Electronic Disease Surveillance System (NEDSS) requirements as they become available.	1
37.	The solution will include a security mechanism that includes data encryption and technology to authenticate users.	3
Privacy		
38.	The solution must comply with appropriate HIPAA privacy regulations.	1
Laboratory Reporting		
39.	The solution should provide a web-enabled user interface for data submission and reporting capability.	2, 5
40.	The solution must provide laboratories with the ability to update and change selected data that have been submitted to CDHS within a defined timeframe.	5

41.	The solution must provide the ability to generate electronic receipt notifications to laboratories for report submittals.	2, 5
42.	The solution must provide the ability to electronically distribute laboratory reports and other notifications to the appropriate LHDs or programs.	2, 4, 5
43.	The solution must provide the capability for transactions to be submitted in various formats.	5
44.	The solution must allow files and HL7 messages to be queued as they are received to balance the load of transactions.	5
45.	The solution must have the capability to accept electronic laboratory data from existing laboratory computer systems.	5
46.	The solution must be able to accept HL7 messages for laboratory results.	2, 7
47.	The solution must incorporate a standard format for receiving non-HL7 files.	7
48.	The solution must have the capability to read and separate HL7 transactions into meaningful data elements.	7
49.	The solution should include LOINC and SNOMED as the standard coding schemes.	2, 7
50.	The solution should accommodate a unique patient identifier.	5
51.	The solution must have the capability to receive laboratory reports containing positive and negative test results.	5
52.	The solution must provide an ad hoc query tool to access the laboratory data.	3
Alerts		
53.	The solution must have the capability of generating alerts on a 24 hour, seven day a week basis.	1
54.	The solution must allow maintenance of user accounts to support alert notifications.	1
55.	The solution must use existing web, and other technology to produce emergency alert notifications based upon specific thresholds for diseases. The alerts will be communicated via email, pager, or cellular phone.	1
56.	The solution must be able to maintain a list of email addresses, pager numbers, and cellular phone numbers of appropriate public health officials.	1
57.	The solution must have the capability to identify the appropriate public health official(s) to notify in the event a threshold criterion is met.	1

Management Reports		
58.	The solution must provide the ability for all authorized users to generate standard, predefined reports.	6
59.	The solution must provide the ability to select users to generate ad hoc reports.	6
60.	The solution must provide the ability to query on-line and generate reports.	6
61.	The solution must provide the ability to generate all State and federal-mandated reports.	6
62.	The solution must support web-enabled reports in both summary and detail format, as well as be able to support download of results for subsequent offline analysis.	6

4.0 BASELINE ANALYSIS

This section contains a review of the current method of operation in order to provide a framework for exhibiting the full technical and work process implications of the existing system and to provide a baseline against which the impact of alternative solutions can be assessed.

4.1 Current Method

This section describes the existing work procedures. A later section presents the supporting system infrastructure.

4.1.1 Introduction

Providing effective disease surveillance throughout the State requires cooperation between State and local public health stakeholders. While the DCDC administers the State's disease surveillance programs, the LHDs manage the day-to-day surveillance and case management activities. LHDs use a variety of systems and levels of technical sophistication to process information, and the process to collect and notify the State of reportable diseases remains consistent across them. Although physicians follow a similar process for reporting notifiable diseases, the focus of the descriptions in this section relate to laboratory reporting. The participants in the disease surveillance process are described below and a description of their activities is described in a subsequent section.

4.1.2 Participants

The participants of the laboratory disease reporting process include:

Private (Hospital), Commercial and Public Health Laboratories

Laboratories are responsible for reporting over 25 named conditions, as well as any outbreaks of unusual diseases, within a specified timeframe of identifying the disease. Laboratories report these specific conditions to the LHD, based on the location of the physician's office. The laboratory report may be submitted to the appropriate LHD by various means including a phone call, facsimile, or mail.

Local Health Departments

While the State disease program offices (such as the DCDC TB Control Branch and STD Control Branch) are responsible for state-level program management, the LHDs are responsible for the day-to-day disease management activities of patients. Once the LHD receives a laboratory disease report for a suspected or confirmed case, it notifies the appropriate public health staff to manage and track the case. In addition, the LHDs report disease case information to the State. The primary source of information is the laboratory disease report and physician report.

California Department of Health Services, Division of Communicable Disease Control

There are six branches within DCDC which play a role in the laboratory disease reporting process. They are:

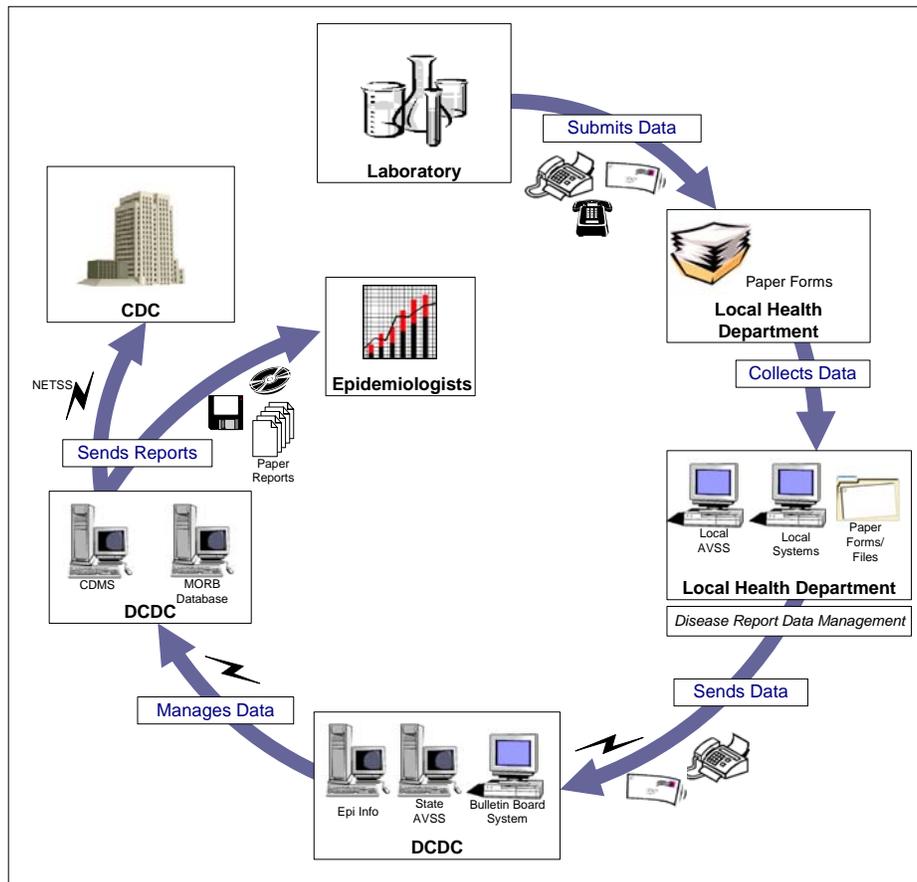
- Microbial Disease Laboratory - MDL
- Viral and Rickettsial Disease Laboratory - VRDL
- Sexually Transmitted Disease – (STD) Control Branch
- Tuberculosis - (TB) Control Branch
- Immunization Branch
- Infectious Disease Branch – IDB

Centers for Disease Control and Prevention

The Centers for Disease Control and Prevention (CDC) is recognized as the lead federal agency for public health in the United States. The CDC provides credible information to enhance health decisions, and promote public health through strong partnerships. The CDC provides the national focus for developing and applying disease prevention and control, environmental health, and health promotion and education activities designed to improve the health of the people of the United States – at home and abroad. California submits information on reportable diseases to the CDC on a weekly basis.

A summary of the reporting process is illustrated in Figure 4-1. A detailed description of the process follows after the summary illustration.

Figure 4.1



Current Reporting Process

4.1.3 Current Reporting Process

4.1.3.1 Submit Data

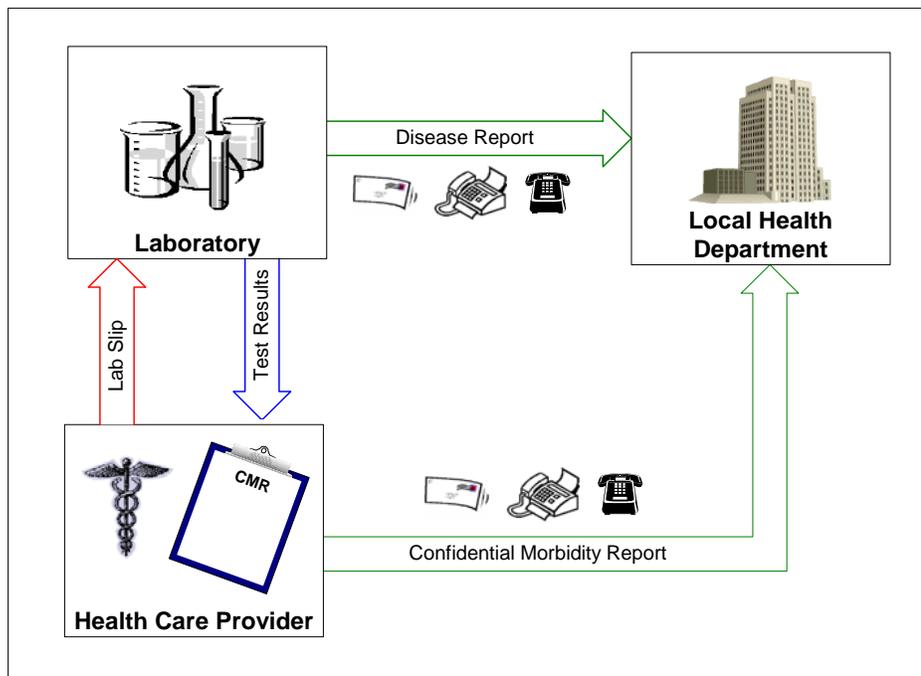
California has a dual reporting system for communicable diseases. Both health care providers (physicians) and laboratories are required to report a case, or suspected case, of notifiable diseases to public health officials. Figure 4.2, below, illustrates California’s dual reporting system for communicable diseases.

California Code of Regulations (CCR), Title 17, §2500, requires health care providers to report over 80 named conditions, as well as any outbreaks of unusual diseases. California Code of Regulations (CCR), Title 17, §2505, requires laboratories to report over 25 named conditions, as well as any outbreaks of unusual diseases. The laboratories are mandated to report directly to the LHD in the jurisdiction where the physician’s office resides. The regulations list the reportable communicable diseases as well as the timeframe for reporting (from one hour up to one week) and the means (by phone, facsimile, mail, email) depending on the disease category. Patient consent is not needed for laboratories and providers to

report cases or suspected cases or to supply additional information requested by State or local public health officials.

CCR, Title 17, § 2505 also states two categories of laboratory reporting based on whether or not a disease agent is considered a high-level bioterrorism candidate. The first category contains seven high-level bioterrorism disease candidates (e.g., anthrax, plague, smallpox). Laboratories are to notify a State laboratory within one hour of receiving a specimen and report positive test results to the LHD within one hour after notifying the health care provider. The second category of laboratory reporting requires laboratories to notify the appropriate LHD within one working day from the time that the health care provider who submitted the specimen receives notification.

Figure 4.2



Reportable Disease Data Flow

Laboratory reports to the LHD must include the following information:

- Date the specimen was obtained
- Patient identification number
- Specimen accession number or other unique specimen identifier
- Laboratory findings for the test performed
- Date that any positive laboratory findings were identified
- Name, gender, address, telephone number, and age or date of birth of the patient
- Name, address, and telephone number of the provider who ordered the test

Private (Hospital) Laboratories

The private or hospital clinical laboratories are those that are associated with a hospital enterprise. They provide laboratory result reports to LHDs on both in-hospital patients and outpatients that referred to them by physicians with ordering privileges assigned by that enterprise.

The majority of these laboratories have Laboratory Information Systems (LIS) that are typically purchased from a vendor specializing in this type of software application. The LIS provides for the electronic receipt and storage of patient demographic, laboratory orders, and test results. They are also capable of transmitting order and result transactions to other clinical and hospital information (HIS) systems. While these applications are able to transmit message transactions, often using HL7 formats, to LHDs, there has not been, until recently, a significant effort to support this type of interfacing. The reasons for the slow adaptation of this methodology include:

- There is no mandate in California to require electronic reporting of communicable disease results, with the exception of Lead.
- The LIS application may require modification to support the PHIN compliant HL7 message structure, which often means additional costs that must be borne by the hospital enterprise.
- The volume of results reported to the LHD represents a fraction of the total results reported by the laboratories. When compared to the number of IT projects in the enterprise, those that are viewed as providing significant improvements in efficiency and cost savings are assigned highest priority.

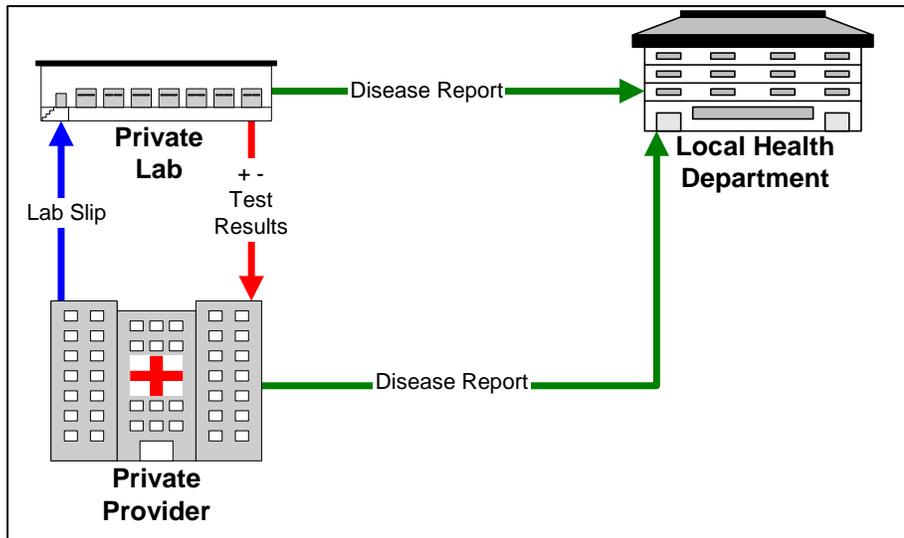
Figure 4.3 illustrates the current disease report workflow utilized by private (hospital) laboratories.

Commercial Laboratories

The commercial laboratories in California utilize a wide variety of LIS applications to maintain information on specimens and results. The standard LIS product tracks specimens from collection to results reporting. The LIS are written in a variety of programming languages with varying technological capabilities.

To meet mandated reporting requirements, a majority of these laboratories complete a paper form and generally either mail or fax the disease report to the LHDs. While LHDs use automated systems to generate the disease reports, there exists little or no automation of the process to get the information to the LHD. Figure 4.3 illustrates the current disease report workflow for commercial laboratories.

Figure 4.3



Private (Hospital) and Commercial Laboratory Reportable Disease Data Flow

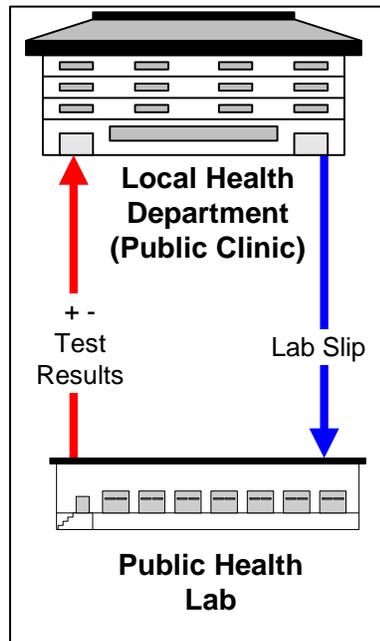
Public Health Laboratories

Public health laboratories differ dramatically in size, structure, and range of services. With the exception of Los Angeles County, California's public health laboratories process significantly fewer laboratory tests in comparison to the commercial laboratories. Being relatively small laboratories, most do not have sophisticated laboratory information systems. Consequently, most public health laboratories are still using paper records for much of their activity².

Patients tested at public clinics, often co-located with LHDs, have tests performed at these public health laboratories. The public health laboratory reports both positive and negative results to the LHD. The reporting requirements for these laboratories are minimal as they often share information systems. Figure 4.4 illustrates the current disease reporting workflow for public health laboratories.

² The Lewin Group "Public Health Laboratories and health System Change." Department of health and Human Services. October 1997.

Figure 4.4



Public Health Laboratory Reportable Disease Data Flow

While private providers primarily send patient specimens to a local laboratory, sometimes services and laboratories outside of California are utilized. In this instance, the reporting process differs from that of in-state laboratories. Out-of-state laboratories provide the analysis of the specimen and send positive and negative results to the healthcare provider. Positive test results are reported to the California CDHS and then forwarded to the appropriate LHD. The locality of the provider who first submitted the specimen determines the specific LHD.

As most LHDs receive hard copy reports from laboratories via mail or fax, the current process has been adequate for reporting health conditions after the fact, but has become increasingly marginal for identifying new outbreaks of disease or other conditions.

4.1.3.2 Collect Data

LHDs have the responsibility to oversee communicable disease control within their jurisdiction. Notifiable disease reports (from a laboratory or health care provider) may trigger epidemiological and laboratory investigations in an LHD to identify such things as the source of the disease, or appropriate control and prevention measures. LHDs use the disease report information and subsequent investigations to provide the appropriate public health assistance to individuals and their community. For some diseases there is a critical period of time for the LHD to take action. Thus, it is extremely important for the laboratory report information to be timely and accurate.

The CDC published a 1990 report, Case Definitions for Public Health Surveillance, and subsequent updates to provide uniform criteria for health department personnel to use when reporting notifiable diseases. To support the disease reporting process, local health officers investigate and confirm that the submitted laboratory report meets the case definitions published by the CDC for disease reporting.

All records, interviews, written reports, and statements produced during an investigation are kept confidential. The LHDs store the disease report and investigation data in a variety of formats. Most LHDs use a combination of paper-based files and information systems to store disease report data. The LHDs' information systems range from systems provided by the State (such as AVSS) to locally-developed information systems (such as simple Microsoft Excel spreadsheets and Access databases) to more complex case management systems).

Typically, the LHDs use at least two information systems to accomplish their disease reporting and case management responsibilities. One information system is used for case management (capturing confirmation, investigation and treatment data) and a second system (typically AVSS) is used for reporting data to the State. The disease report data is entered by LHD staff into the case management system and then must be re-entered into the reporting system (AVSS). AVSS does not have the capability to capture case management data nor to import data from other systems, making dual data entry a necessity.

4.1.3.3 Send Data

Once a case of a reportable disease is confirmed, the LHDs report the information to DCDC in one of three ways: (Note that *none* of these represent transmission of laboratory data to the State, although the initial "trigger" for such a disease report may have been a laboratory report.)

1. Using AVSS.³

Primarily, LHDs communicate morbidity data to the State using AVSS. While AVSS was designed primarily to automate birth and death certificate production, it has been modified to collect data on the State's reportable communicable diseases. Staff at the LHD receive the report for reportable diseases from laboratories (except for Human Immunodeficiency Virus (HIV) and Acquired Immune Deficiency Syndrome (AIDS) disease reports, which have a unique reporting process) and enter confirmed disease reports into AVSS. On a weekly basis, the State installation of AVSS automatically connects, via modem, to each of the local AVSS installations to retrieve new morbidity data.

2. Hardcopy disease reports by mail or facsimile.⁴

Low-incidence or low-population LHDs do not have direct access to AVSS. These LHDs mail or fax the disease case reports to DCDC staff. Staff then enters the disease report data into the State instance of AVSS. Summary disease report data is then entered into the Epi Info system.

3. Use an electronic bulletin board (BBS).⁵

³ 45 LHDS use AVSS.

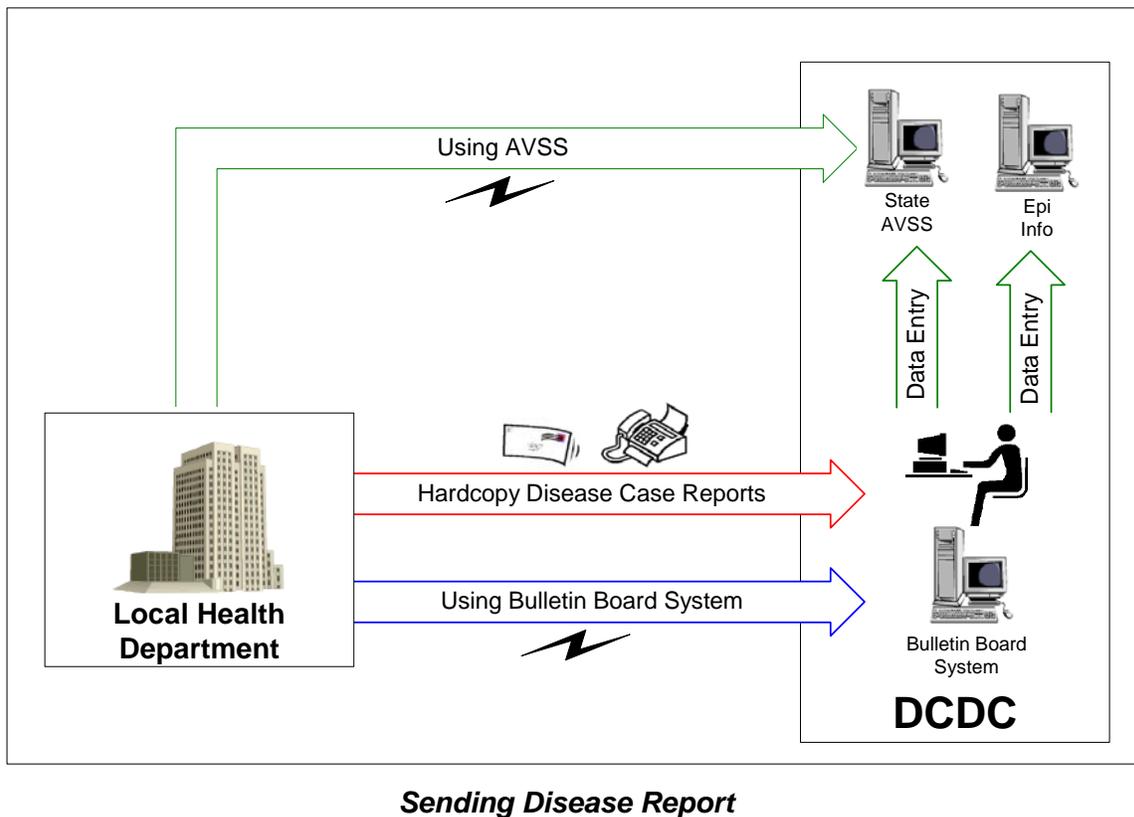
⁴ 12 LHDs mail or fax CMR forms.

⁵ 4 LHDs submit CMR data via an electronic bulletin board system.

A small number of LHDs extract morbidity information from their internal systems to be electronically updated for the State's reporting to the CDC. The files are submitted to the State via an electronic bulletin board system (BBS).

Figure 4.5 illustrates how LHDs submit disease report data to the State.

Figure 4.5



4.2 Technical Environment

4.2.1 Existing Systems

There is currently no state ELR production environment -- no electronic information is transmitted from local clinical laboratory stakeholders to the Department as part of an on-going program. Within some local health jurisdictions, however, some county laboratory information is transmitted to respective public health departments for disease syndromic surveillance and case management purposes.

4.2.2 Existing Infrastructure Environment

4.2.2.1 Hardware and Software Standards

The CDHS current IT hardware and software standards to which all equipment procurement and software must comply is located at <http://itsd.int.dhs.ca.gov/ei/standards/pdf/DHSHardwareSoftwareStandards.pdf>. Most important is the Network Server Technology Standard in Section 3 describing server performance and configuration requirements.

4.2.2.2 Web-based Application Architecture Standards and Processes

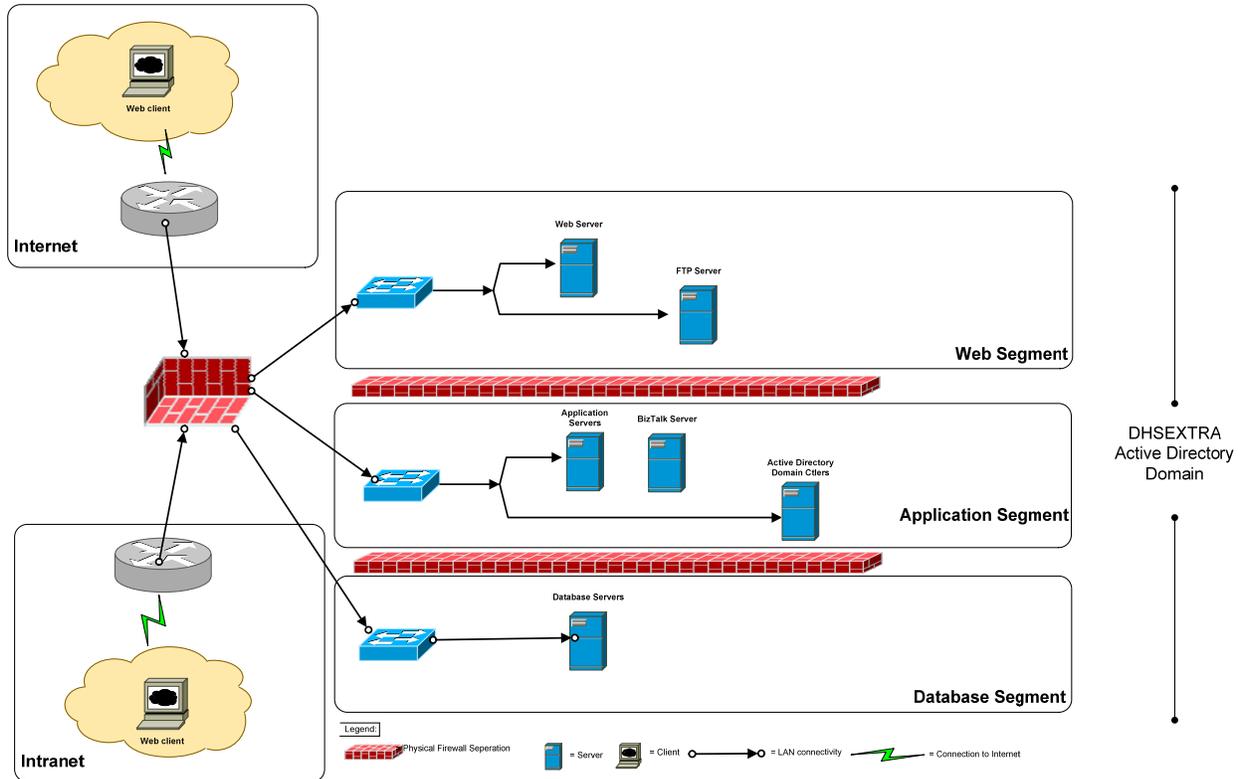
The CDHS standard application development architecture contains details about the standard architecture, technologies, database conventions, and required presentation. This document also includes the standard set of support services defined and created by the Information Technology Services Division (ITSD) to support CDHS business functions, and is intended to identify best practices, procedures, and processes allow developers to create applications that are efficient, secure, and maintainable. It may be found at <http://itsd.int.dhs.ca.gov/ei/standards/pdf/Application%20Architecture%20V3.0.pdf>

4.2.2.3 Network Infrastructure and Topology

CDHS has designed and implemented a wide area network (WAN) to support the many applications required by the State of California. Within this network there exist three different security models which support the EDP needs of the department. These models, sometimes called zones, are referred to as the Extranet, Intranet and Internet. Each of these zones provides a unique security profile that allows appropriate access and protection to data and applications. Figure 4.6 illustrates the CDHS current network topology.

Figure 4.6

CDHS WAN Topology



1. **Internet Zone** - An area of the network accessible by anyone. The identity of the individuals is usually not required but may be confirmed if needed and communications encrypted if required. The Internet zone is typically used by the general public, connected over the public Internet. This zone is the least secure, and therefore will not contain or allow access to any data not publicly available.
2. **Extranet Zone** - An area of the network used primary by non-CDHS staff, whose identity must be specifically identified and authorized to access resources typically considered confidential or proprietary, for example counties, consultants, suppliers. All communication must be encrypted. The Extranet zone is typically used by CDHS business partners that may connect over the public Internet or through a direct dial-up connection and requiring an authentication method, such as a password or certificate.
3. **Intranet Zone** - The internal CDHS network, accessible only by authorized CDHS staff. The Intranet zone is typically used by CDHS staff that is directly connected to the internal private network. These users are usually responsible for maintaining the information in each of the three zones and therefore, may require access to information or data contained in each of the zones.

5.0 PROPOSED SOLUTION

This section examines a system solution and identifies the alternative that best satisfies the previously defined objectives and functional requirements.

5.1 Solution Description

This section identifies the proposed solution and discusses the business processes that will be enabled by its implementation.

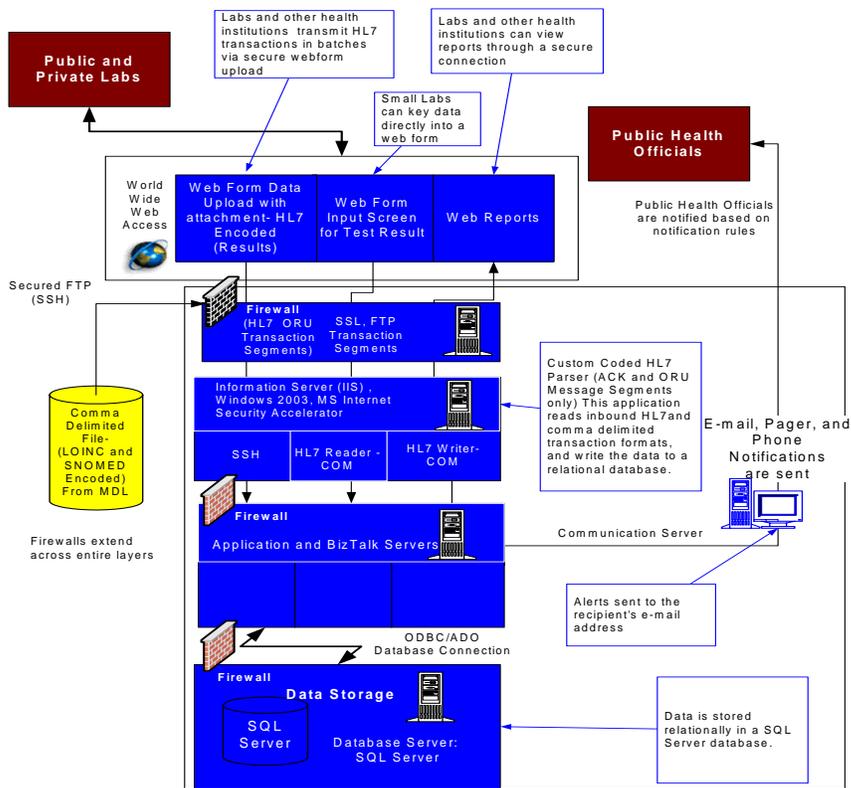
The proposed solution for the electronic submission of laboratory reports is a Commercial Off-the-Shelf (COTS) or Modified Off-the-Shelf (MOTS) procured product. The Department has identified no less than four vendors capable of supplying a solution that requires only configuration of service interfaces to procured software or some software modification. The solution consists of a web-based application and back-end database that will support laboratory reporting and data management. The COTS/MOTS system solution offers the following features:

- Web entry of laboratory disease report forms
- Ability to transfer and share disease report information between LHDs
- Batch interfaces for importing data from laboratory sources
- Automated business logic for data field cleansing and validation
- Automated reporting to the State and CDC in standard formats
- Alerting or early event detection of aberrations
- Ad hoc reporting capabilities

Figure 5.1 illustrates the conceptual architecture of the proposed solution anticipated to be housed within the CDHS IT infrastructure.

Figure 5.1

Conceptual Solution Architecture



5.1.1 Hardware

The hardware architecture of the proposed production environment will require a number of servers. Other required environments (Testing, Staging, “Hot Fix”) necessary to support the ongoing maintenance and operation will necessitate an additional subset of the above system components. The specific hardware configuration will be determined upon selection of the solution vendor. The solution may use existing components of the current hardware infrastructure.

5.1.2 Software

In specifying a solution, vendors will be requested to describe how closely the software solution complies with current CDHS ITSD standards. Compliance with these standards is recommended, but not an absolute requirement of any solution.

5.1.3 Technical Platform

If the solution is a Microsoft supported solution, then the hardware operating system software will be the current versioning of Microsoft Windows IIS, SQL, and ISA or a later version complementing the current technology infrastructure. The system will operate within the CDHS’s existing network infrastructure described in Section 4.2.

5.1.4 Development Approach

The appropriate development methodology will be determined through joint discussions with the State and the vendor. The methodology selected will align with published standards in the Statewide Information Management Manual (SIMM) as expressed in the Department's procurement, operating, and other standards identified in Section 4.2. CDHS standards are identified in the State SAM, the ITSD Web Based Application Architecture document, ITSD Standards document, and the ITSD Extranet Technical Standards document.

5.1.5 Integration Issues

The system will be required to interface with a solution specified in the Confidential Morbidity Report (CMR) project currently defined in a separate department-sponsored FSR. For a possible alerting feature provided in the solution, integration with a Health Alert Network available through a web service may be required. Message encoding services to LOINC, SNOMED, and PHIN standards may require integration with commercial messaging engines such as the BizTalk server currently in place at CDHS.

5.1.6 Procurement Approach

From previous demonstration efforts involving CMR and ELR projects, much of the hardware and operating software specified in the solution will be redirected to this project's effort. For those hardware components remaining, standard CMAS vendors and competitive procurement procedures will be followed. The COTS/MOTS vendor selection will occur through a structured product evaluation process.

5.1.7 Technical Interfaces

The proposed solution utilizes a batch import feature through secure FTP to import data from laboratories incorporating laboratory Information management systems (LIMS). This import feature is designed to be flexible and provide the ability to import new data sources as the need arises from the multitude of prospective public health and private laboratories around the state. Other technical interfaces will be supplied or used as web services through application program interfaces (API).

5.1.8 Testing Plan

Consistent with best practices, the vendor will be required to develop and submit a Testing Plan designed to assure the installed solution is configured and operating as intended. In addition, the vendor will perform unit and system testing before user acceptance testing. Independent verification will be performed by the CDHS. User acceptance testing will include representatives from selected laboratory report provider, local health jurisdictions, and the CDHS. As a final system effectiveness measure, the CDHS plans to obtain PHIN certification to the standards contained in the Appendix.

5.1.9 Resource Requirements

The CDHS plans to use existing staff with the assistance of contract personnel to provide domain expertise in the implementation of similar systems. Contractors are expected to perform most roles within the project team due to limited available state staffing. This effort will be augmented by the CDHS’s technical staff that will provide project installation and operational support. In addition, the CDHS will provide expertise on business processes and policies from programmatic staffs. Figure 5.2 summarizes the anticipated resource requirements.

Figure 5.2

Anticipated CDHS and Vendor Project Resource Requirements

Contract Staff	FY 1	FY 2	FY 3
Project Manager			
Project IV&V			
Project IPO			
Project Business Lead			
Subject Matter Experts (Reqs/Design/UAT)			
Quality Systems Analyst			
State Staff			
CDHS Project Director			
CDHS Technical Support			
Project Totals			

Both during and following implementation of the ELR capability at CDHS, the DCDC program will be responsible for marketing, outreach, and recruitment of possible submitters of laboratory information. The potential outreach must address recruitment of over 2100 possible submitters of electronic data statewide.

To support this effort, the CDHS will require the following resources:

Business Lead – This person has overall responsibility for coordinating the marketing and communication efforts. This position must have existing ties to the public health community and to private labs in order to effectively perform outreach and recruitment activities. This role will act as a liason between the potential submitters and CDHS.

Certification Testing Analyst (2) – This role will be responsible for setup, performing, and analyzing the results of all certification tests for each of the 2100 labs. For each lab, a test must be organized, planned, and managed to confirm that each lab is submitting data according to the California HL7 specification (developed during the project). In addition, at each point where either a certified submitter, or CDHS encounters a software upgrade, each submitter may be required to perform a regression test to ensure they continue to adhere to the certification standards following each change.

ELR/HL7 Support Engineer – This role will supply detailed technical support to the team with regard to message setup, message routing, message analysis, and will act as a technical liaison in support of the business lead when communicating with technical staff at each laboratory.

5.1.10 Training Plan

Since this is a technical solution for automating laboratory reporting, the only training anticipated is that of System Administration designed to instruct laboratory staff on the necessary level of expertise required for the maintenance of messaging components installed at the local level. Support, in the form of a normal business hour Help Desk, will be provided by the CDHS.

5.1.11 Ongoing Maintenance

CDHS program staff will provide basic assistance to laboratory reporters and LHD staffs. Included with this support will be the marketing and outreach effort to solicit additional reporting from prospective laboratories. This effort will require the development of informational materials describing the technical and business interfaces to the selected system, availability of CDHS staff for technical consultation, exercising of testing and verification strategies designed to assure successful laboratory reporting, and on-going troubleshooting support.

Contracted services and CDHS technical support will perform software maintenance, serve as the second-level help desk, and serve as the liaison for the technical hosting of the application. Ongoing maintenance of the technical infrastructure (e.g., servers, network, etc.) will be performed by the CDHS in its network environment as part of on-going operating services. The system's COTS/MOTS vendor will be contracted to provide on-site maintenance support as required for six months after implementation with an option to renew the maintenance at CDHS's discretion.

5.1.12 Information Security

The proposed database and application software will require users to log in with a user identification and password. The system will restrict authorized access to functions and screens by a CDHS-developed two-factor authentication (2FA) mechanism. The hosting environment maintains a perimeter firewall to protect systems from inappropriate access. Furthermore, appropriate software virus detection and Intrusion Detection (network and host) software will be installed on the system's servers to protect against unauthorized access and provide an additional level of information security.

Use of Public-Key Infrastructure (PKI) technology may be used to enable the CDHS to properly secure its health data, while meeting multiple federal security guidelines. A PKI based solution would be identified, designed, tested, and implemented for ultimate use by most public health applications. PKI is a 2FA authentication method used by a number of leading health care organizations for e-commerce and HIPAA

compliance solutions. It has been demonstrated to be a viable approach for appropriate protection with sensitive health information. Very specific processes and policies will be developed in support of PKI, particularly regarding issuance of digital certificates to individuals, and validating their identity. To allow interoperability with outside entities through the Federal Bridge, federal guidelines on these policies will need to be followed.

5.1.13 Confidentiality

Public health data is highly confidential and subject to Federal and State laws. The solution provides for network and application security enhancements (including PKI, data encryption, and firewalls) that meet industry standards. The system will use Secure Sockets Layer (SSL) data encryption, Secure FTP, and server validation via registered certificates.

5.1.14 Impact on End Users

None identified

5.1.15 Impact on Existing Systems

None identified

5.1.16 Consistency with Overall Strategies

In the fall of 2000, the State of California introduced an e-government initiative designed to use the power of technology to bring state government closer to California citizens and businesses. The intention of this effort is to use information technology to make State government information, services, and programs more accessible by leveraging the power of the Internet. The proposed solution is fully consistent with the State's initiative to create on-line utilization for government information and services.

The proposed solution directly aligns with the CalPHIN effort's overall goals and strategies documented in the June 2003 *CalPHIN Strategic Plan*. This project supports the following CalPHIN Strategic Goals:

- **Standards:** Develop and implement standards and procedures to support the management of public health information
- **Collaboration:** Develop and manage public health systems collaboratively with partners and key stakeholders to improve public health data sharing and infrastructure development
- **Enabling Technology:** Implement reliable, effective, and efficient information technology solutions to support the public health information infrastructure
- **Security/Confidentiality:** Provide a secure environment for public health information that protects the privacy of Californians
- **Project Success:** Deliver public health projects on time and within budget while successfully achieving objectives

In addition, the proposed solution supports CDHS's mission to protect and improve the health of all Californians and is consistent with the CDHS Strategic Vision (March 2000). In addition, this solution is consistent with recommendations provided in the State's January 2002 *Bioterrorism Surveillance and Epidemiologic Response Plan*. Lastly, the proposed solution supports federal NEDSS goals and PHIN requirements from the CDC as a requirement of the CDC's Bioterrorism Preparedness Grant funding.

5.1.17 Impact on Current Infrastructure

The proposed solution will use CDHS current network infrastructure; the increase in data communication traffic as a result of this project is not expected to be significant enough to increase bandwidth requirements.

5.1.18 Impact on Data Center(s)

None identified

5.1.19 Backup and Operational Recovery

The solution will be subject to the normal backup procedures currently in place within the CDHS, and operational recovery practices defined within the CDHS's *IT Operational Recovery Plan*.

5.1.20 Benefits

This solution provides the following benefits to the CDHS:

- Eliminates the current burdensome process of transferring and sharing data across public health program and LHDs
- Reduces the possibility of data entry errors from manually re-keying data from paper forms from laboratories to LHDs
- Standardizes data elements and formats used in the evaluation of disease characterization
- Potentially increases the collection of disease reports valued in syndromic disease surveillance
- Most importantly, increases the timeliness and completeness of disease reports, enabling better surveillance and early detection of communicable disease problems and appropriate public health responses to control and prevent disease.

5.2 Rationale for Selection

Different alternatives were evaluated against five main categories of: functionality, costs, risks, schedule, and strategic alignment. The process was to score each alternative on a scale of 1 to 5, with 5 being the best. For example, the alternative with the lowest cost scored a 5, the alternative with the highest functionality scored a 5, etc.

Shown on the next page is a summary of the different alternatives evaluated against standard criteria. It shows that the Proposed Solution has the highest overall score.

Criteria	Proposed Solution (COTS)	5.3.1 Transfer System from State	5.3.2 Build In House
TOTAL	28	21	22
Primary Business Objectives	4	3	5
Functional Requirements	4	4	5
One-Time Development Costs	3	4	2
On-Going Costs	5	2	2
Risks (Project and Technical)	4	2	1
Schedule	4	3	2
Strategic Technical Architecture	4	3	5

The business case for implementation of an electronic lab reporting system has been described elsewhere. This section discusses why the proposed solution is the best, compared to the alternatives listed below. The primary reasons for choosing the selected approach are:

- This approach meets all of the business objectives.
- This approach meets all objectives at the lowest projected cost.
- This approach also results in the shortest project timeframe as it does not require lengthy custom software design and development life cycles.

5.3 Other Alternatives Considered

5.3.1 Develop Custom System Application

- Description

Use a competitive bid process with a written Request for Proposals (RFP), distributed to interested bidders. This process involves a procurement intended to result in the acquisition of a system integrator to design, develop, and implement a custom solution. This solution would be completely owned by CDHS when complete and would require custom application maintenance when complete. This entire process, from inception to signing a contract for software development, could take nine months or longer, to complete.

- Costs

The one-time development cost estimate associated with this type of development far exceeds the proposed solution due to the additional personnel required to complete the project.

Development Schedule:

Development Cost:

Development Effort:

On-Going Maintenance:

Note: These costs include services costs focused on the system development life cycle and do not include mandatory project oversight or verification and validation services.

- Advantages

Best match to primary business objectives

Best match of functional requirements

Best match to CDHSt strategic technical architecture

- Disadvantages

Highest one-time development costs

Highest on-going maintenance costs.

Highest risks of all the alternatives considered.

Longest schedule of all the alternatives considered.

Solution requires extensive DCDC and LHD and Lab business subject matter experts to answer questions from development team.

5.3.2 Transfer Solution

- Description

Select system from another State, and transfer to California. Several other states have PHIN compliant systems that were either built in-house or by a contractor. Because these systems were developed with Federal funds, they are open source. Both Washington and New York have potential systems.

- Costs

This solution is relatively expensive when considering on-going maintenance costs. Transferring a solution from another State requires a sizable staff to maintain the system. Each State is responsible for maintenance.

Development Schedule:
Development Cost:
Development Effort:
On-Going Maintenance:

Note: These costs include services costs focused on the system development life cycle and do not include mandatory project oversight or verification and validation services.

- Advantages

Match of Functional Requirements: Because solutions are implementation of Federal PHIN requirements, the basic functionality should match.

High One-Time Development Costs: Because functionality supports other states, California only needs to modify the system, not start from scratch. However, these costs are significantly higher than the preferred alternative.

- Disadvantages

High On-Going Costs: Transfer solution typically require customization and enhancement, they are not designed to be configured to transfer to another installation site. That is, programming is required to make changes, instead of simply changing values in a configuration table.

Relative high risks: This solution requires both people knowledgeable in the transfer solution and knowledgeable in California operations. The system must be customized to work in California's operational environment.

Solution requires extensive DCDC and LHD and Lab business subject matter experts to answer design questions from development team.

6.0 Project Management Plan

6.1 Project Management Plan

The ELR Project will be managed by a project manager within DCDC, under the guidance and oversight from the CDHS Project Management Office (PMO), in the ITSD Project Planning and Management Branch (PPMB). DCDC will procure a project manager with specific experience in similar projects to manage the ELR project. The project manager will report to the project sponsor, and will periodically report status to the ITSD PPMB to ensure adherence to statewide California and CDHS policies, procedures, and practices. The Project Manager will work closely with the DCDC business team and the vendor to manage installation and configuration project tasks, cost, schedule, quality, and risks.

6.1.1 Project Manager Qualifications

The successful completion of the project will require a project manager with experience and training appropriate to the size, complexity and risk level of ELR Project.

The DCDC, will procure a project manager with the following minimum qualifications:

- At least five years experience in information technology (IT) project management.
- Knowledge and experience in managing software development, systems development and data conversion.
- Demonstrated experience in providing project management for an IT project of at least the scope and size of the ELR project.
- Demonstrated experience in implementing similar systems in other jurisdictions within the US.
- Knowledge and experience in California state procurement and IT project management practices.

Additional desirable qualifications include the following:

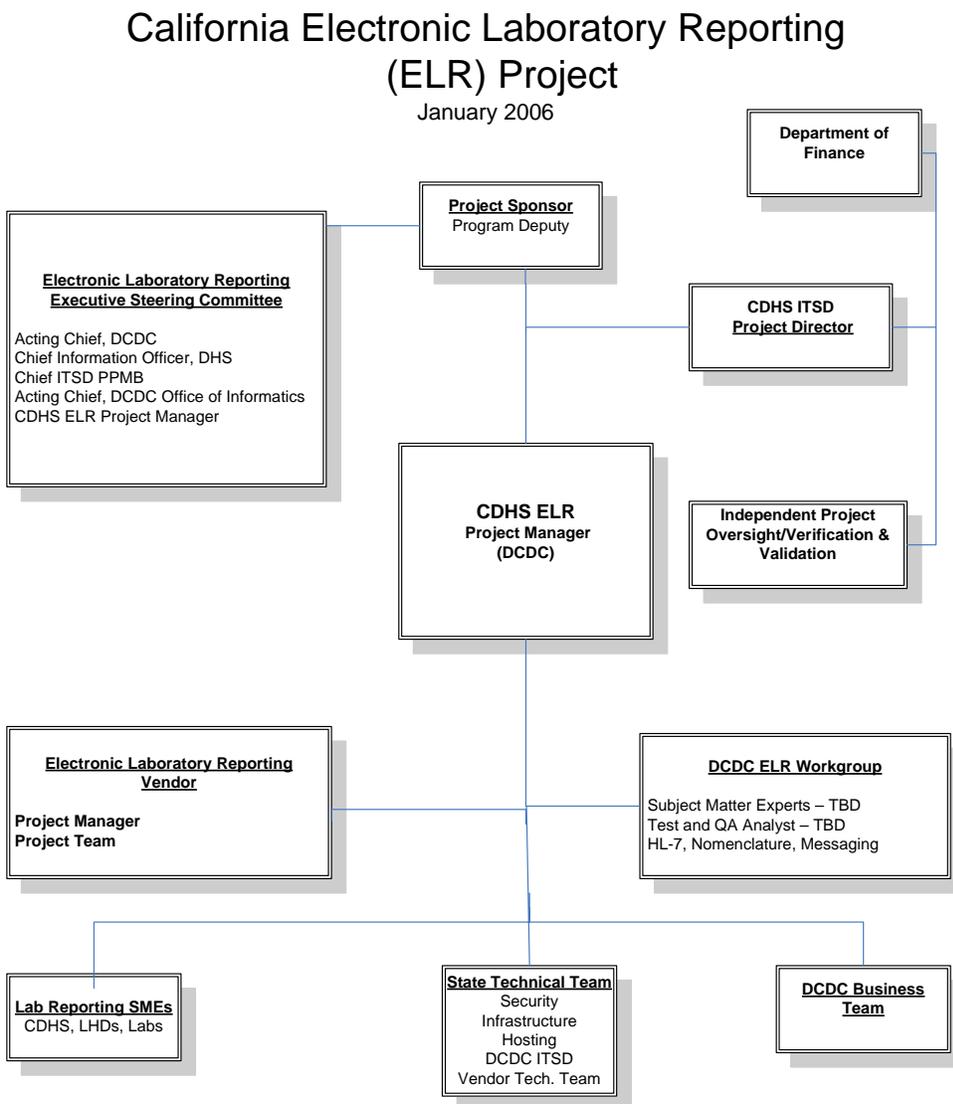
- Project management certification such as:
 - Project Management Professional certification from the Project Management Institute.
 - Degree in Project Management or related discipline from an accredited university.
- Knowledge and experience with health-related data system projects, especially an understanding of disease surveillance strategies and systems.
- Knowledge/experience working with CDHS programs and organization.

6.2 Project Management Methodology

The CDHS Project Management Methodology is based on the guidelines in the California Statewide Information Management Manual (SIMM) Section 200, the Project Management Body of Knowledge (PMBOK) from the Project Management Institute, and the recommended project management and risk management practices of the DOF Information Technology Project Oversight Framework. Industry best practices and lessons learned from prior CDHS projects are also included.

6.3 Project Organization

The organization chart for the ELR Project is shown below.



6.4 Project Priorities

Managing a project requires balancing of three interrelated factors: resources, schedule, and scope. A change in one factor may result in a change in another factor. Project stakeholders should agree on the importance of each of these factors before the project begins by assigning one of the following to each factor:

- Constrained: the factor cannot be changed.
- Accepted: the factor is somewhat flexible to the project circumstances.
- Improved: the factor can be adjusted.

The following presents the trade-off matrix for this project.

Schedule	Scope	Resources
Improved	Constrained	Accepted

6.5 Project Plan

This section provides an overview of the following areas:

- Project scope.
- Project assumptions.
- Project phasing.
- Roles and responsibilities.
- Project schedule.
- Project monitoring.
- Project quality.
- Change management.
- Authorization required.

6.5.1 Scope

The scope of the ELR project is to provide a system that accomplishes the business objectives and functional requirements defined in this document.

6.5.1.1 Project Scope

The PMBOK defines project scope as the work that must be done to accomplish the objectives of the project. Project scope management includes the processes to ensure that the project includes all of the work required and only the work required to successfully complete the project. The ELR project scope will be defined and

managed using a detailed work breakdown structure to be developed and maintained by the project manager. Any changes in project scope will be managed through the change control process.

6.5.1.2 Product Scope

Product scope is defined as the features and functions to be provided by the product of the project. Product scope management ensures that the product includes all of the necessary features and functions, without any unnecessary bells and whistles that could lengthen the project schedule and increase cost. Product scope of the ELR system will be defined in system requirements documentation. Any changes to product scope will be managed through the change control process.

6.5.1.3 Business Scope

The business scope of a project can be defined as the processes and systems that form the boundaries for the business areas directly included and impacted by the project. The business processes and respective organizations (i.e., process owners) impacted by the ELR project are identified in the following table.

Business Processes Impacted by ELR

Business Process	Process Owner
Submit ELR Data	Local Public and Private Labs
Collect Data	Local Health Departments, DCDC
Send Case Report Data	Local Health Departments, Local Public and Private Labs
Assess/Review Lab Report Data	DCDC, Surveillance and Statistics Staff
Send Reports	DCDC, Surveillance and Statistics Staff

6.5.2 Project Assumptions

The major project assumptions include the following:

- This FSR will receive timely approval from CDHS, HHSA, and DOF.
- Project procurements will not be delayed by the complex and time-consuming state procurement and approval processes.
- The project will be responsible for implementation of a single lab interface to ensure a functioning system. The recruitment, certification, and ongoing monitoring of electronic submitters is an ongoing program activity outside of the project.

- All new hardware and software related to ELR must be in accordance with the Department’s current technology infrastructure.
- CDHS program and information technology staff and representative agencies are available to participate in requirements definition, systems design, and user acceptance testing.
- At least one CDHS information technology staff member will participate on the ELR project for knowledge transfer purposes.
- Full project funding will be provided.
- Federal funding will be provided at a consistent level throughout the project.
- The project will receive demonstrable CDHS support.
- End users will have participation and buy-in to ensure the solution’s success.

6.5.3 Project Phases

The project will be conducted in a single installation and configuration phase as the submission process cannot be split into multiple components which could be usefully implemented at DCDC.

6.5.4 Roles and Responsibilities

The following table identifies the major participants in the project and their roles and responsibilities:

Role	Responsibilities	Organization
Project Sponsors	<ul style="list-style-type: none"> ▪ Makes key business decisions. ▪ Resolves significant issues that the Project Management Team cannot resolve. ▪ Determines the final scope of the ELR project. ▪ Makes the final decision on the vendors retained throughout the ELR project. ▪ Leads Steering Committee meetings. ▪ Communicates project status to CDHS Management and the Budget Committee. 	<ul style="list-style-type: none"> ▪ DCDC ▪ ITSD
Project Manager	<ul style="list-style-type: none"> ▪ Coordinates project work efforts. ▪ Develops project management-related deliverables. ▪ Serves as a liaison between vendors and internal/external stakeholders. ▪ Maintains Issues Database and Change Management Database. ▪ Maintains project work plan. ▪ Reviews all project deliverables. ▪ Coordinates monthly ELR Project Management Team meetings. ▪ Attends Steering Committee meetings. ▪ Conducts weekly Project Team Meetings. ▪ Develops weekly project status reports. 	Vendor (reports to DCDC and Project Sponsors)

Role	Responsibilities	Organization
Contract Manager	<ul style="list-style-type: none"> ▪ Participates in the procurement processes to secure Systems Integration services, Project Management services, and Independent Project Oversight services. ▪ Reviews and approves all Deliverable Expectation Documents (DEDs) and final deliverables. ▪ Reviews and approves invoices. ▪ Maintains information on contracted costs vs. actual costs. ▪ Attends monthly ELR Project Management Team and Steering Committee meetings. ▪ Communicates project status to internal and external stakeholders, as needed. 	DCDC
Steering Committee	<ul style="list-style-type: none"> ▪ Assists in the identification of business needs. ▪ Assists in the coordination of efforts between the ELR project and other related CDHS projects. ▪ Assist in the definition of business processes and business rules. ▪ Assists in policy setting related to implementation of the ELR system ▪ Participate in interviews and working sessions with the ELR project team. ▪ Confirms project goals and scope. ▪ Provides strategic guidance at key intervals. ▪ Communicates project status to respective external stakeholders, as needed. 	<ul style="list-style-type: none"> ▪ DCDC ▪ Public Health Program Offices ▪ LHDs
Subject Matter Experts (SMEs)	<ul style="list-style-type: none"> ▪ Assist in the coordination of efforts between the ELR project and other related CDHS projects. ▪ Publish California HL7 specifications for ELR ▪ Publish California Lab Certification guidelines ▪ Assist in the identification of business needs and analysis of the current operating environment. ▪ Assist in the definition of business processes and business rules. ▪ Participate in interviews and working sessions with the ELR project team. ▪ Participates in user acceptance testing of the new system. 	<ul style="list-style-type: none"> ▪ DCDC ▪ LHDs ▪ Private and Public Health Care Providers

Role	Responsibilities	Organization
Systems Development Team	<ul style="list-style-type: none"> ▪ Designs and configures ELR, in accordance with the functional requirements and business needs. ▪ Conducts unit and systems integration tests. ▪ Conducts system design and configuration walkthrough sessions. ▪ Develops test cases for acceptance testing. Oversees acceptance testing. ▪ Develops system documentation. ▪ Determines technology architecture required for system interfaces. ▪ Designs, tests, and documents system interfaces. ▪ Develops user manuals, addresses user questions and issues (e.g., help desk), develops training materials, and conducts training sessions. 	<ul style="list-style-type: none"> ▪ Systems Development Vendor ▪ DCDC ▪ ITSD ▪ Data Center
Independent Project Oversight	<ul style="list-style-type: none"> ▪ Serves as an independent expert that provides recommendations in managing all of the activities that are critical to the project's success. ▪ Oversees the project to ensure that it is following a structured and defined project management approach. ▪ Reviews all draft and final project management deliverables to ensure that they are aligned with defined standards and project needs. ▪ Provides monthly assessment and review reports to DOF and CDHS management 	Independent Project Oversight Vendor (Reports to ITSD/POS)
Independent Verification and Validation	<ul style="list-style-type: none"> ▪ Serves as an independent expert that provides recommendations in performing the technical activities that are critical to the project's success. ▪ Oversees the project to ensure that the products of each phase fulfill the requirements levied on them (verification), and that the final product of the project will fulfill the business objectives and functional requirements (validation). ▪ Reviews all draft and final technical deliverables to ensure that they are aligned with defined standards and project needs. ▪ Provides monthly assessment and review reports to CDHS management 	IV&V Vendor (Reports to ITSD/POS)

Upon completion of the project, the maintenance team will fulfill the following roles and responsibilities.

Role	Responsibilities	Organization
------	------------------	--------------

Role	Responsibilities	Organization
Laboratory Readiness Team	<ul style="list-style-type: none"> ▪ Serves as liaison between CDHS and electronic lab report submitters ▪ Maintains ELR application. Designs, develops, and implements approved system changes post-implementation. ▪ Maintains ELR database. Designs, develops, and implements approved system changes post-implementation ▪ Addresses user questions and issues (e.g., second level help desk). ▪ Maintains ELR technology architecture, including servers and external network. ▪ Designs changes related to program changes. 	<ul style="list-style-type: none"> ▪ ITSD ▪ Systems Development Vendor ▪ Data Center
Systems Maintenance Team	<ul style="list-style-type: none"> ▪ Serves as technical liaison supporting the Lab Readiness team in communications between CDHS and electronic lab report submitters ▪ Analyzes and responds to errors related to electronic lab submittals ▪ Maintains ELR configurations for lab submitters ▪ Maintains ELR system components, including application of software releases ▪ Advises Laboratory Readiness Team of technical issues affecting electronic submitters ▪ Maintains ELR technology architecture, including servers and external network. 	<ul style="list-style-type: none"> ▪ ITSD ▪ Systems Development Vendor ▪ Data Center

6.5.5 Project Management Schedule

Task/ Activity	Duration	Milestone/ Decision Point	Estimated Completion
FY 2005/2006			
Develop Software Evaluation Criteria	1 month	Project Sponsor approval of criteria	Feb. 2006
Develop RFP/RFQ	1 month	RFP/RFQ released to vendors	March 2006
Vendor Selected	2 months	Signed Contract	May 2006
Hardware/Software Installation	2 months	Signed Contract	July 2006
Software Configuration	2 months	Sign off on Test Completion	Sept 2006
Test/Certify Pilot Laboratory	1 month	Pilot approved as electronic submitter	Oct 2006

6.6 Project Monitoring

The ELR project manager will maintain the project plan and associated schedule and make it available to all project stakeholders. Team members will report progress, issues, possible risk factors, change requests, etc. to the project manager as they occur, but no less often than monthly.

Software vendor progress will be reported no less often than twice monthly. The contract manager will assess the vendor's performance.

Any problems that might jeopardize the schedule, cost, quality or scope of the project or require additional resources to be added, will be called to the attention of the Project Steering Committee and the Project Sponsor as soon as they are discovered, so remedial actions may be planned.

Project stakeholders will receive monthly status reports of the project's progress, along with other material developed to ensure a successful implementation in the field.

6.6.1 Project Oversight

Project oversight involves independent review and analysis to determine if the project is on track to be completed within the estimated schedule and cost, and will provide the functionality required by the sponsoring business entity. ELR project oversight will be managed by the ITSD Planning and Oversight Section (POS). The POS will procure highly qualified consultants to perform Independent Project Oversight (IPO) and Independent Verification and Validation (IV&V).

6.6.1.2 IPO

IPO will be conducted in accordance with the DOF IT Project Oversight Framework. The IPO consultant will perform the following functions:

- Perform continuous review and analysis to determine if the project is on track to be completed on cost and schedule.
- Ensure that the project is following a structured and defined project management approach.
- Independently identify and analyze project risks.
- Review project management deliverables to ensure that they are aligned with defined standards and project needs.
- Provides monthly assessment and review reports to DOF and CDHS management
- Provide recommendations in managing all of the activities that are critical to the project's success.

6.6.1.3 IV&V

IV&V will be conducted using the Institute of Electrical and Electronic Engineers (IEEE) Standard 1012-2004, Software Verification and Validation. The IV&V consultant will perform the following functions:

- Perform continuous review and analysis to ensure that the products of each phase fulfill the requirements levied on them (verification), and that the final product of the project will fulfill the business objectives and functional requirements (validation).
- Reviews technical deliverables to ensure that they are aligned with defined standards and project needs.
- Provides monthly assessment and review reports to CDHS management
- Serves as an independent expert that provides recommendations in performing the technical activities that are critical to the project's success.

6.7 Project Quality

Quality is defined as the delivery of a work product or deliverable that satisfies the requirements and objectives of the project with minimal errors and defects. In order to minimize the risk of receiving a work product or deliverable of poor quality, a Deliverable Expectations Document (DED) will be completed prior to the start of any major deliverable. Within the DED, the following is identified:

- Deliverable name.
- Description of the deliverable.
- Deliverable outline.
- Planned delivery date.
- Deliverable reviewers.
- Deliverable sign-off sheet.

The project manager and contract manager will review and approve each DED. Walkthroughs will be conducted on all deliverables. The IPOC and IV&V consultants will be provided draft and final versions of applicable deliverables as well as participate in the walkthrough sessions. A deliverable sign-off sheet will be completed by the project manager upon receipt of a completed and approved deliverable. This sign-off sheet must be attached to the vendor invoices in order for the contract manager to process the invoice.

6.8 Change Management

Change is an inevitable occurrence on any project. In order to effectively manage change for the ELR Project Manager will leverage the Change Management Plan used within other CDHS projects to manage the process, procedures and outputs for all change-related project activities. The plan will be updated identify the ELR parties responsible for identifying, resolving, supporting, and making project changes. The implementation of a change management plan ensures that all changes are evaluated for potential scope, cost, and schedule impacts. The

process allows decision-makers the opportunity to evaluate changes in a systematic manner.

The major goal of this change management strategy is to ensure that only approved changes are made, and those changes are made using standardized methods and procedures.

The change management process will define the processes and procedures for:

- Reporting an identified need for change;
- How the change request will be analyzed and documented;
- How the change will be acted upon for review, approval or denial;
- How approved changes will be executed.

The plan is designed to:

- Allow for needed changes and prevent unnecessary changes.
- Minimize disruption to the project.
- Communicate changes to stakeholders.
- Minimize unanticipated impacts to schedule and/or budget.

The implementation of a change management plan ensures that all changes are evaluated for potential scope, cost, and schedule impacts. The process allows decision-makers the opportunity to evaluate changes in a systematic manner.

6.9 Authorization Required

The following external authorizations are required for purchase, installation, and configuration of the ELR project.

Type	Organization
Appropriation of Federal Funds	Legislature
Approval to Spend Federal Funds	DOF and Joint Legislative Budget Committee (JLBC)
Technical Approach	DOF

7.0 RISK MANAGEMENT PLAN

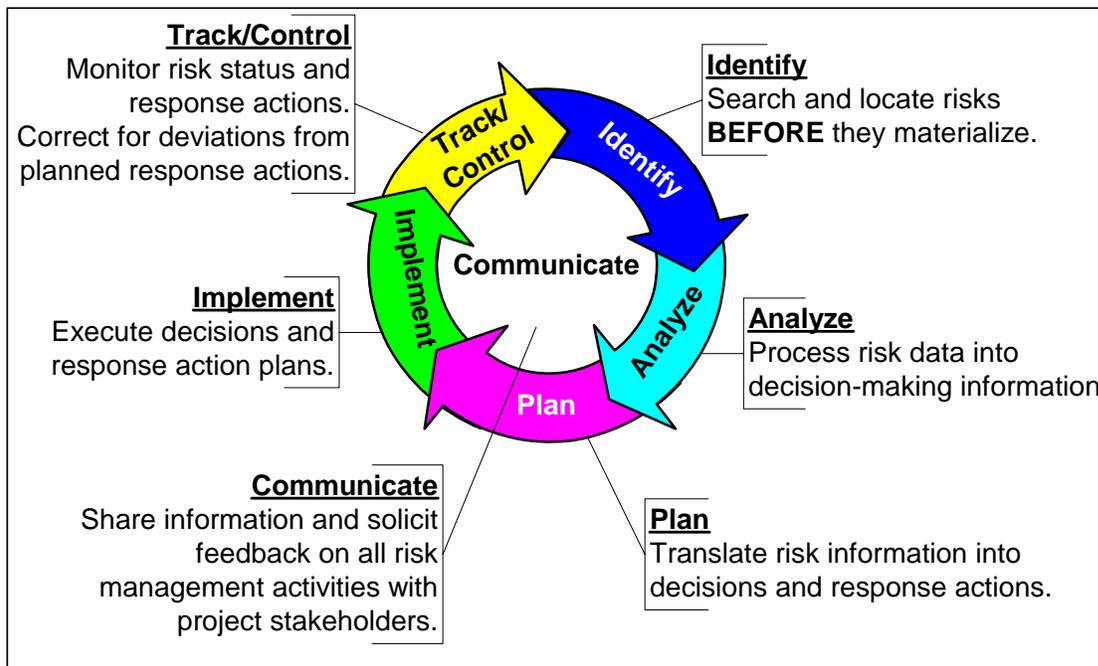
This section documents the process and procedures that will be used to manage project risks.

This Risk Management Plan describes the methods that the Electronic Lab Reporting (ELR) team will use to manage risks throughout the life of the project. A risk is any potential problem that may interfere with the successful completion of the project. Risks may potentially affect project schedule, cost, and/or quality.

Risk management includes the following major components:

- Risk analysis – identifying and prioritizing risks.
- Risk action planning and tracking – developing a plan of action for each identified risk, and tracking progress against the plan.
- Risk escalation – providing appropriate visibility of risks to management.

The continuous cycle of risk management activity is depicted graphically below.



References Consulted

- Project Management Institute's *Project Management Book of Knowledge* (PMBOK), 2000 Edition, Chapter 11 (Project Risk Management)
- Department of Finance (DOF) *Information Technology Project Oversight Framework*, Section 5 (Risk Management and Escalation Procedures)
- DOF *State Information Management Manual* (SIMM), Section 200.3.11 (Risk Management Plan)

Goals and Objectives

The goal of this Risk Management Plan is to improve the probability of success of the ELR by providing a roadmap for:

- Ongoing assessment of potential problems; and
- The opportunity to make adjustments to avoid or lessen the impact of those problems before they occur.

The objectives of this Risk Management Plan are the continuous identification, assessment and documentation of:

- The risks faced by the project;
- The estimated probability of each risk;
- The consequences in terms of impact on project schedule, cost, and quality if the risk events should occur;
- The priority of each risk for response action and escalation;
- The owner of each risk;
- The plan of action for responding to each risk; and
- The thresholds and procedures for escalating risks.

Scope

This Risk Management Plan includes the risk management activities for the duration of the ELR.

Roles And Responsibilities

The table below identifies the project stakeholders and their related risk management responsibilities.

Title	Role/Responsibilities
-------	-----------------------

Title	Role/Responsibilities
Steering Committee	Final approval of Risk Management Plan. Review escalated high and medium severity risks. Provide direction when needed. Determine if risks have become unacceptable for the project to continue.
ITSD/Planning and Oversight Section	Provide general risk management assistance as requested. Review escalated high and medium severity risks. Provide feedback and suggestions as needed.
Project Director	Approve Risk Management Plan. Review escalated high, medium, and low severity risks. Provide direction and feedback as needed.
Risk Manager (ELR Project Manager)	Overall responsibility for risk management. Develop the Risk Management Plan. Determine which risk candidates represent actual risks. Assign Risk Owners. Maintain the Risk Management Forms. Maintain the Risk List. Escalate risks.
Risk Owners (Project team members as assigned)	Assign risk attributes. Determine risk priority. Determine risk response strategy. Develop risk response action plan. Execute risk response actions. Track and report risk status and response activity.
Project Team Members	Identify risk candidates.
Independent Project Oversight Consultant (IPOC)	Provide an ongoing independent review and analysis of project risk management practices. Independently identify and analyze project risks. Develop Independent Project Oversight for submission to management and DOF.

Risk Analysis

Risk analysis includes the steps necessary to identify and prioritize risks.

Risk Identification

Risk identification is the process of discovering those risks which could negatively impact project quality, cost, and/or schedule. It would be impossible to identify all possible risks to the project, therefore emphasis is on identifying risks that are at least somewhat likely to occur and that could have a significant impact on the project. All project team members and the IPOC are responsible for identifying potential risks to the project. At a regular periodic basis, all risks will be reviewed by the Project Manager and IPOC. It is also anticipated that monthly project team meetings will include a standing agenda item for raising new risk candidates to the attention of the Risk Manager. Project team members and the IPOC may also communicate risk candidates to the Risk Manager by email, telephone, or ad hoc meetings—however, all project participants will be trained and encouraged to enter risks into the project's risk management tool Clarity. Project participants will be instructed to communicate potentially serious risk as soon as practical rather than waiting for the next monthly team meeting.

Sources of Risk

Project risks can come from many and varied sources. Project team members must be vigilant in recognizing and documenting potential risks so that they can be properly evaluated for project impact. Some common risk sources include:

- The technology used on the project;
- The legal and regulatory environment in which the project is executed;
- Relationships between the organizations involved in the project;
- Sufficiency and allocation of project resources;
- Unrealistic or conflicting stakeholder expectations;
- Mandated implementation date.

Risk Determination

The Risk Manager, with participation as needed by applicable project team members, determines which risk candidates constitute actual risks to the project. A risk is a potential event that would have a negative impact on the success of the project if the event were to occur. The following considerations support the determination of "Is it a risk?":

- Time frame: A risk is a potential future event. Risk events that have already occurred are not risks, but rather represent problems or issues to be managed outside of the Risk Management process. Events that may occur after the project is completed, but not during the project, are not risks to the project.
- Probability: What is the estimated likelihood of the risk event occurring? If there is little or no probability of the risk event occurring, the risk may not warrant inclusion in the Risk Management process. An event that is certain to occur is not a risk but rather a problem or issue.
- Impact: What is the estimated impact to the project schedule, cost, or quality if the risk event should occur? Risks with little or no impact may not warrant inclusion in the Risk Management process.

Risk candidates that are judged to meet the three criteria described above are included in the project Risk Management process.

Risk Attributes

Risk attributes are described in the table below. Risk attributes are documented by the Risk Owner, as described in paragraph 3.2 Risk Tracking.

Risk Attribute	Description
Risk Name	A brief sentence or phrase that summarizes the risk.
Risk ID	A unique number used to identify the risk. The Risk ID is assigned sequentially by the system.
Creator	The name and organization of the person who identified the risk.
Creation Date	The date that the risk was recognized as a project risk.
Owner	The project team member responsible for responding to the risk and tracking risk status. The Risk Manager assigns the Risk Owner.
Description	A concise definition of the risk using the sentence structure Concern • Likelihood • Consequence for example, "Mandated unrealistic implementation date • will likely • lead to significant missing functionality in the system implementation".
Risk Symptoms	Elaboration of warning signs or triggers (an early indication that the risk is starting to occur).
Impact Description	Elaboration of the Consequences if the risk is manifested. I.e. the increased costs, delayed schedule, reduced quality, and/or unrealized scope that could occur if the risk occurs.

Risk Attribute	Description
Impact Date	The expected date the risk might manifest. This is used to calculate the Time Frame.
Target Resolution	The target date for the Risk Owner to implement mitigation, transfer, or contingency plans. This date must be earlier than the Impact Date.
Impact	An ordinal value to indicate the severity of consequences. Possible values are: very low, low, medium, high and very high.
Probability	A cardinal value to indicate the likelihood of occurrence: 1%, 10%, 20%, 30%, 40%, 50%, 60%, 70%, 80%, 80%, 90%, 99%
Calculated Risk	A system calculated value of risk exposure. Calculated by multiplying impact * probability. A higher value indicates a greater exposure. Maximum value is 495.

Risk Prioritization

Risks are prioritized by severity, with the highest severity risks given the highest priority for response action and escalation. Risk severity is determined by the probability, impact and Timeframe.

Probability

Risks are assigned a probability rating based on the estimated likelihood of a risk event occurring.

Impact

Risks are assigned an impact rating based on the estimated negative impact on project cost, schedule and/or quality.

Criteria	Impact Rating
One or more of the following: - Project cost increase of 16% or more - Project schedule increase of 16% or more - Schedule predicts missing formal public milestone - Failure to meet major performance requirements - Failure to provide major required functionality	Very High

Criteria	Impact Rating
None of the above Very High criteria, one or more of the following - Project cost increase of 11% to 16% - Project schedule increase of 11% to 16% - Schedule predicts missing formal department milestone - Significant discrepancies in desired performance - Significant discrepancies in desired functionality	High
None of the above High criteria, one or more of the following: - Project cost increase of 6% to 10% - Project schedule increase of 6% to 10% - Some discrepancies in desired performance - Some discrepancies in desired functionality	Medium
None of the above Medium criteria, one or more of the following: - Project cost increase of 3% to 5% - Project schedule increase of 3% to 5% - Minor discrepancies in desired performance - Minor discrepancies in desired functionality	Low
None of the above Low criteria, one or more of the following: - Project cost increase of less than 2% - Project schedule increase of less than 2%	Very Low

Time Frame

Risks are assigned a Time Frame based upon the Target Resolution date based on the time period within which action must be taken to successfully respond to the risk. Target Resolution is the date all mitigation, contingency and/or transfer activities must be completed. Target Resolution is less than the Impact Date. Impact Date is the date the result will occur and impact the project.

Exposure

Risk exposure is determined from the probability and impact ratings, and is used along with the time frame rating to determine severity. The exposure rating for each risk is the intersection of that risk’s impact and probability in the matrix below:

Risk Exposure Matrix

Probability			
--------------------	--	--	--

		10	20	30	40	50	60	70	80	90	100
Implementation	Very Low	10	20	30	40	50	60	70	80	90	100
	Low	20	40	60	80	100	120	140	160	180	200
	Medium	30	60	90	120	150	180	210	240	270	300
	High	40	80	120	160	200	240	280	320	360	400
	Very High	50	100	150	200	250	300	350	400	450	500

Severity

Risk severity is determined from the exposure and time frame ratings, and is used to prioritize the risk. Risks with “High” severity have the highest priority for risk response activity and escalation, followed by “Medium” and then “Low” severity risks. The severity rating for each risk is the intersection of that risk’s exposure and time frame in the matrix below:

Risk Severity Matrix

		Exposure / Calculated Risk		
T	F	<119	120 to 269	>269
Time	Very Long	60	194	231
	Long	120	388	462
	Medium	180	582	693
	Short	240	776	924

Risk Action Planning and Tracking

The Owner is responsible for planning appropriate risk response action and for tracking the status of the risk and the response activity. The Owner reports any changes in risk status at the monthly project team meeting.

Risk Action Planning

The Owner, with approval of the Risk Manager, determines the appropriate risk response strategy and actions plan.

Risk Response Strategy

The Owner, with the approval of the Risk Manager, determines the appropriate risk response strategy from the options below:

- Research – Additional research will be taken prior to determining the appropriate strategy.
- Accept – If the project can continue and be successful with the anticipated impact of the risk, or if there is no practical way to avoid or mitigate the risk, the project may choose to accept the risk and expend no further resources managing it other than tracking the risk status.
- Avoid – Risk avoidance involves taking steps to reduce the probability of the risk.
- Transfer – Transfer the risk to a third party. If the risk occurs, the third party suffers the impact instead of the project. Typically accomplished via insurance.
- Mitigate – Risk mitigation involves taking steps to reduce the impact of the risk. These steps can include actions to be taken immediately, and/or contingency plans to be implemented if a risk event occurs.

When appropriate a risk response strategy can include transfer, avoidance and/or mitigation actions.

Action Planning / Response Strategy

The Owner, with the approval of the Risk Manager, determines the action plan to be taken to implement the selected strategy. Often a simple list of one or more action items, with responsibilities and due dates identified, will be an adequate plan. Some high severity risks may require more elaborate planning. These are recorded in the Response Strategy.

Risk Tracking

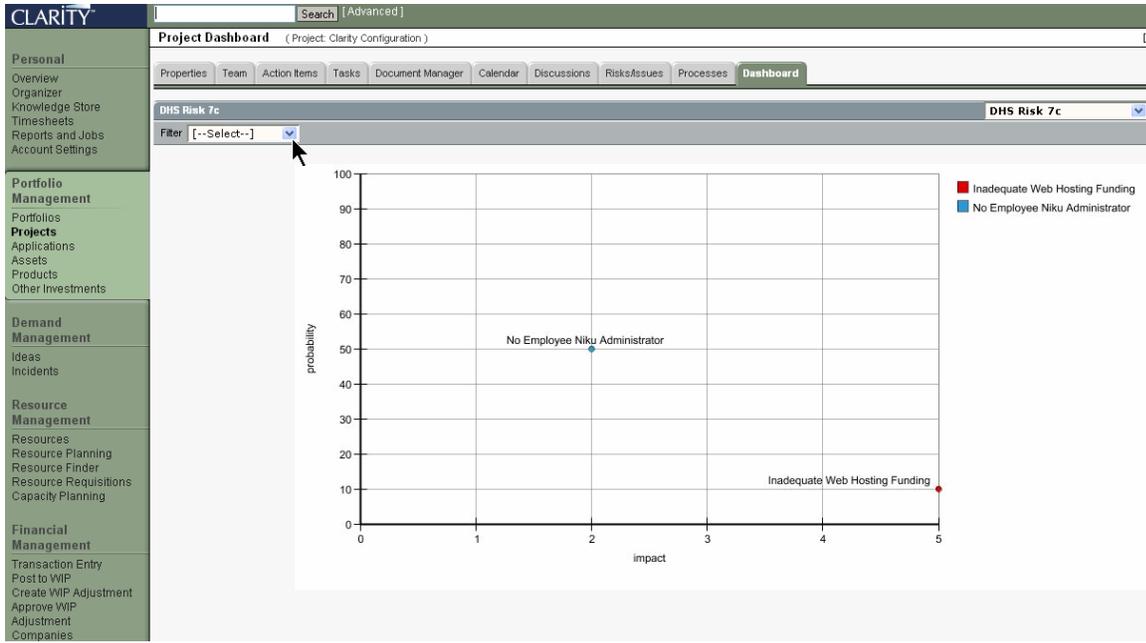
Clarity is used as the system of record for all project risks. This project management repository is available to all project participants. Shown below is an example screen print of the Risk's General Property page. This is used by any project participant to create or edit a risk.

The Risk Manager, or any project participant, may use Clarity to list or summarize the risks via Clarity on a regular basis: A listing of risks, with two example risks, is shown on the following page.

	Name	ID	Status	Owner	Probability	Impact	Calculated Risk	Above Threshold
<input type="checkbox"/>	No Employee Niku Administrator	RSK-0004	2 Work in Progress	Williamson, John	⚠	⚠	100	
<input type="checkbox"/>	Inadequate Web Hosting Funding	RSK-0103	2 Work in Progress	Williamson, John	⚠	⚠	50	

Total Results: 2

A dashboard view, with two example risks, is shown below:



Risk Escalation

The Project Manager escalates risks to the Project Director, the Planning and Oversight Section (POS), and the steering committee depending on risk severity, as indicated in the risk escalation matrix below:

		Risk Severity		
		High	Medium	Low
Escalation	DOF	X		
	Steering Committee; POS	X	X	
	Project Director	X	X	X

The method of risk escalation is as follows:

- High, medium, and low severity risks are reported to the Project Director in regular project status reports.
- High and medium severity risks are reported to the Steering Committee during Steering Committee Meetings.
- Printouts of Risk Inventory for high and medium severity risks are included in the monthly Executive Project Status Reports provided to the POS.

Appendix: Risk List

Name	ID	Owner	Probability	Impact	Calculated Risk	Target Resolution Date	Status
Delayed Procurement	RSK-0130	Williamson, John	60	Medium	120	04/06/06	1 Open
Inadequate Federal Funding	RSK-0128	Williamson, John	60	Medium	120	06/06/06	1 Open
Low Quality Application	RSK-0134	Williamson, John	30	High	90	06/06/06	1 Open
Low User Satisfaction	RSK-0132	Williamson, John	80	Low	80	06/06/06	1 Open
Inadequate Cost Estimating	RSK-0131	Williamson, John	70	Low	70	06/06/06	1 Open
Unclear or Changing Requirements	RSK-0137	Williamson, John	20	High	60	06/06/06	1 Open
Poor Project Management	RSK-0123	Williamson, John	20	High	60	06/06/06	1 Open
Interfaces to Other Systems	RSK-0129	Williamson, John	30	Medium	60	06/06/06	1 Open
Inadequate Configuration Control	RSK-0127	Williamson, John	30	Medium	60	06/06/06	1 Open
Inability for Vendor to Deliver	RSK-0126	Williamson, John	10	Very High	50	06/06/06	1 Open
Canceled Federal Funding	RSK-0124	Williamson, John	10	Very High	50	06/06/06	1 Open
Unanticipated Acceptance Criteria	RSK-0136	Williamson, John	30	Low	30	06/06/06	1 Open
Excessive Paperwork and Oversight	RSK-0125	Williamson, John	10	Medium	20	06/06/06	1 Open
Operation Problems	RSK-0133	Williamson, John	10	Medium	20	06/06/06	1 Open

8.0 ECONOMIC ANALYSIS WORK SHEETS

The following pages present the Economic Analysis Work Sheets (EAWS) for the existing and proposed systems

The spreadsheets are included as a separate file in the electronic version of this FSR.

APPENDICES

- **Appendix A – CCR Title 17, Section 2505**
- **Appendix B - PHIN Cross Functional Component Self Assessment Tool**
- **Appendix C – Acronym List**
- **Appendix D – Department ISO Requirements**

Title 17, California Code of Regulations (CCR), Section 2505
REPORTABLE CONDITIONS: NOTIFICATION BY LABORATORIES

California Code of Regulations, Title 17, Section 2505 requires laboratories to report laboratory testing results suggestive of the following diseases of public health importance to the local health department:

List (e)(1)

Anthrax
Botulism
Brucellosis
Plague, animal or human
Smallpox (Variola)
Tularemia
Viral hemorrhagic fever agents (e.g., Crimean-Congo, Ebola, Lassa and Marburg viruses)

List (e)(2)

Chlamydial infections
Cryptosporidiosis
Diphtheria
Encephalitis, arboviral
***Escherichia coli* O157:H7 infection**
Gonorrhea
Hepatitis A, acute infection, by IgM antibody test or positive viral antigen test
Hepatitis B, acute infection, by IgM anti-HBc antibody test
Hepatitis B surface antigen positivity (specify gender of case)
Listeriosis
Malaria
Measles (Rubeola), acute infection, by IgM antibody test or positive viral antigen test
Rabies, animal or human
Syphilis
Tuberculosis
Typhoid
***Vibrio* species infections**
Salmonella (Section 2612 – see below)

WHEN TO REPORT

These laboratory findings are reportable to the local health officer of the health jurisdiction where the health care provider who first submitted the specimen is located within one (1) hour (List (e)(1) diseases) or within one (1) working day (List (e)(2) diseases) from the time that the laboratory notifies that health care provider or other person authorized to receive the report. If the laboratory that makes the positive finding received the specimen from another laboratory, the laboratory making the positive finding shall notify the local health officer of the jurisdiction in which the health care provider is located within the time specified above from the time the laboratory notifies the referring laboratory that submitted the specimen. If the laboratory is an out-of-state laboratory, the California laboratory that receives a report of such findings shall notify the local health officer in the same way as if the finding had been made by the California laboratory.

HOW TO REPORT

Laboratory reports must be made in writing and give the following information:

- the date the specimen was obtained,
- the patient identification number,
- the specimen accession number or other unique specimen identifier,
- the laboratory findings for the test performed,
- the date that any positive laboratory findings were identified,
- the name, gender, address, telephone number (if known), and age or date of birth of the patient,
- the name, address, and telephone number of the health care provider who ordered the test.

The notification for List (e)(1) diseases shall be reported by telephone within one (1) hour, followed by a written report submitted by electronic facsimile transmission or electronic mail within one (1) working day, to the local health officer in the jurisdiction where the health care provider who submitted the specimen is located. The notification for List (e)(2) diseases shall be submitted by courier, mail, electronic facsimile transmission or electronic mail within one (1) working day to the local health officer in the jurisdiction where the health care provider who submitted the specimen is located. Whenever the specimen, or an isolate therefrom, is transferred between laboratories, a test requisition with the above patient and submitter information shall accompany the specimen. The laboratory that first receives a specimen shall be responsible for obtaining the patient and submitter information at the time the specimen is received by that laboratory.

ADDITIONAL REPORTING REQUIREMENTS

ANTHRAX, BOTULISM, BRUCELLOSIS, PLAGUE, SMALLPOX, TULAREMIA, and VIRAL HEMORRHAGIC FEVERS

Whenever a laboratory receives a specimen for the laboratory diagnosis of a suspected human case of one of these diseases, such laboratory shall communicate immediately by telephone with the Microbial Diseases Laboratory (or, for Smallpox or Viral Hemorrhagic Fevers, with the Viral and Rickettsial Disease Laboratory) of the Department of Health Services for instruction.

TUBERCULOSIS

Any clinical laboratory or approved public health laboratory that isolates *Mycobacterium tuberculosis* from a patient specimen must submit a culture to the local public health laboratory as soon as available from the primary isolate on which a diagnosis was established.

The following information must be submitted with the culture:

- the name, address, and the date of birth of the person from whom the specimen was obtained,
- the patient identification number,
- the specimen accession number or other unique specimen identifier,
- the date the specimen was obtained from the patient,
- the name, address, and telephone number of the health care provider who ordered the test.

Unless drug susceptibility testing has been performed by the clinical laboratory on a strain obtained from the same patient within the previous three months or the health care provider who submitted the specimen for laboratory examination informs the laboratory that such drug susceptibility testing has been performed by another laboratory on a culture obtained from that patient within the previous three months, the clinical laboratory must do the following:

- perform or refer for drug susceptibility testing on at least one isolate from each patient from whom *Mycobacterium tuberculosis* was isolated,
- report the results of drug susceptibility testing to the local health officer of the city or county where the submitting physician's office is located within one (1) working day from the time the health care provider or other authorized person who submitted the specimen is notified,
- if the drug susceptibility testing determines the culture to be resistant to at least isoniazid and rifampin, in addition, submit one culture or subculture from each patient from whom multidrug-resistant *Mycobacterium tuberculosis* was isolated to the public health laboratory for the local health jurisdiction in which the health care provider's office is located.

Whenever a clinical laboratory finds that a specimen from a patient with known or suspected tuberculosis tests positive for acid fast bacillus (AFB) staining and the patient has not had a culture which identifies that acid fast organism within the past 30 days, the clinical laboratory shall culture and identify the acid fast bacteria or refer a subculture to another laboratory for those purposes.

MALARIA

Any clinical laboratory that makes a finding of malaria parasites in the blood film of a patient shall immediately submit one or more such blood film slides for confirmation to the local public health laboratory for the local health jurisdiction where the health care provider is located. When requested, all blood films will be returned to the submitter.

SALMONELLA

California Code of Regulations, Title 17, Section 2612 requires that a culture of the organisms on which a diagnosis of salmonellosis is established must be submitted to the local public health laboratory and then to the State's Microbial Diseases Laboratory for definitive identification.

All laboratory notifications are acquired in confidence. The confidentiality of patient information is always protected.

Appendix B – PHIN Cross Functional Component Self Assessment Tool

For further information regarding the use and structure of this tool, please contact DCDC or access <http://www.cdc.gov/phn>.

ELR Project

Appendix C – Acronym List

ANSI	American National Standards Institute
BT	Bioterrorism
AVSS	Automated Vital Statistics System
CAPHLD	California Public Health Laboratory Directors
CCR	California Code of Regulations
CDC	Centers for Disease Control and Prevention
CDMS	Communicable Disease Management System
CMR	Confidential Morbidity Report
COTS	Commercial Off-the-shelf Software
DCDC	Division of Communicable Disease Control
DHS	Department of Health Services
ELR	Electronic Laboratory-based Reporting ELR is the electronic transmission of public health data from clinical laboratories to public health agencies.
Epi-X	Epidemic Information Exchange
FSR	Feasibility Study Report
HAN	Health Alert Network
HIPAA	Health Insurance Portability and Accountability Act
HL7	Health Level 7 HL is a standards development organization formed in 1987 to produce a standard for hospital information systems.
IPO	Independent Project Oversight
IV&V	Independent Validation and Verification
IZ	Immunization
LHD	Local Health Department
LHJ	Local Health Jurisdiction
LIS	Laboratory Information System
LOINC	Logical Observation Identifiers, Names and Codes

MDL	Microbial Disease Laboratory
MOTS	Modified Off-the-Shelf Software
NEDSS	National Electronic Disease Surveillance System
PHL	Public Health Laboratory
PMBOK	Project Management Body of Knowledge
SNOMED	Systemized Nomenclature of Medicine
SQL	Structured Query Language
SSL	Secure Sockets Layer
SSS	Surveillance and Statistics Section
STD	Sexually Transmitted Disease
TB	Tuberculosis
TCP/IP	Transmission Control Protocol/Internet Protocol
TIMS	Tuberculosis Information Management System
VRDL	Viral and Rickettsial Disease Laboratory
XML	eXtensible Markup Language



**INFORMATION
SECURITY OFFICE**

STANDARD:	New Project Information security Requirements
No:	S19
PROGRAM:	ISO
AUTHOR:	Andrew Lancashire, Security Consultant Brett Kelsey, Security Consultant
DATE SUBMITTED:	
DATE APPROVED:	

REVISION HISTORY

REVISION No.	PROGRAM/NAME	DATE SUBMITTED	DATE APPROVED	REVISION SUMMARY



INFORMATION SECURITY STANDARDS

ISO

STANDARD NO. S19

New Project Information security Requirements

The purpose of this standard set of requirements is to provide direction for projects conforming to DHS policies. This document will serve as a universal set of requirements which must be met regardless of physical hosting location or entities providing operations and maintenance responsibility. These requirements do not serve any specific project, instead they are a tangible set of requirements based on DHS policies.

Number	Requirement
A	Application must be able to be segmented into an n-tier model separating at a minimum the Presentation, Application/Business Logic and Database layers
B	Each layer must be separated both logically and physically by a firewall.
C	Each information system shall require the use of password-based authentication and other security safeguards and precautions to restrict logical and physical access to authorized users only.
D	<p>The following password requirements must be met:</p> <ul style="list-style-type: none"> • Are not to be shared. • Must be 8 characters or more in length • Must be a Non-dictionary word • Password must not be stored in clear text • Must be changed every 60 days. • Must be changed immediately if revealed or compromised. • Must be composed of characters from at least three of the following four groups from the standard keyboard: <ul style="list-style-type: none"> ○ Upper case letters (A-Z); ○ Lower case letters (a-z); ○ Arabic numerals (0 through 9); and ○ Non-alphanumeric characters (punctuation symbols) • System must time-out user session after 20 minutes of inactivity
E	All user and data input must be validated
F	Any system request made to the Business logic layer must be authenticated

Number	Requirement
G	All calls to the Database layer must be made as a trusted sub-system that utilizes a single database access account to all transactions
H	The system shall provide secure role-based access for any authorization utilizing the principle of least privilege at all layers.
I	System must log success and failures of user authentication at all layers as well as log all user transactions at the database layer as required by regulation, policy or standard and as prescribed for the given application/system. This logging shall be included for all user privilege levels including but not limited to systems administrators.
J	The system shall not allow direct database access from the presentation layer and In-line SQL calls must not be allowed from the business logic layer.
K	The system shall encrypt any transmissions of data that contains confidential information with an industry-recognized encryption standard that is in compliance with CDHS standards.
L	All transmission and data-links between the data and application/system and DBMS and the HHSDC WAN shall be secure between transmission systems as required by regulation, policy or standard and as prescribed for the given application/system.
M	The system shall comply with all applicable Department Security requirements, standards and guidelines, as specified in the State Administrative Manual, Health Administrative Manual, HIPAA, Privacy Act, and any other applicable state or federal regulation. All security safeguards and precautions shall be subject to the approval of the DHS.
N	All systems shall install and actively use comprehensive third-party anti-virus and virus protection software, and routinely update such software when updates are released. In-sourced applications must adhere to DHS department standards. All security safeguards and precautions shall be subject to the approval of the DHS.
O	All systems shall install and actively use comprehensive third-party patch management program and routinely update system and application software when updates are released. In-sourced applications must adhere to DHS department standards. All security safeguards and precautions shall be subject to the approval of the DHS.
P	All systems shall install and actively use comprehensive third-party real-time intrusion prevention program that reports security events directly to the DHS information security office. In-sourced applications must adhere to DHS department standards. All security safeguards and precautions shall be subject to the approval of the DHS.

Number	Requirement
Q	All systems shall comply with HHSDC and DHS standard change control process and procedures.
R	<p>All systems shall allow for periodic system security reviews that provide assurance that management, operations, personnel, and technical controls are functioning effectively and providing adequate levels of protection.</p> <p>The reviews may include technical tools and security procedures such as virus scanners, vulnerability assessment products (which look for known security problems, configuration errors, and the installation of the latest hardware/software “patches”), and penetration testing.</p>
S	The system/application maintainers shall immediately and in writing report to the ISO on any and all breaches or compromises of system and/or data security, and shall take such remedial steps as may be necessary to restore security and repair damage, if any. In the event of a breach or compromise of system and/or data security, the ISO may require a system/application security audit. The ISO shall review the recommendations from the security audit, and make final decisions on the steps necessary to restore security and repair damage. The system/application maintainers shall properly implement any and all recommendations of the security audit, as approved by the ISO.
T	Conduct a Business Impact Analysis of the application to determine the Maximum Acceptable Outage (MAO), cost of lost functionality, system component dependencies, business function dependencies, and business partner dependencies. This shall be completed annually.
U	Establish procedures for responding to an emergency or other occurrence (e.g., fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information. The emergency procedures shall be added to the existing Operational Recovery Plan (ORP) to restore any loss of data and assure continuity of computing operations for support of the application and data. The ORP shall address what to do if a computer system and/or the data files are violated, lost, damaged, or inaccessible. Recovery procedures shall be developed using Appendix “J” Template from the CDHS ORP
V	Establish an Emergency Mode Operation Plan to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode. This plan shall be added to the existing ORP.

Number	Requirement
X	Establish and implement Data Backup Plan and procedures to create and maintain retrievable exact copies of electronic protected health information. Files should be copied and kept in a secured off-site location identified in the ORP. There must be a regular schedule for making backup copies; The frequency between backups depends on how data files are used and the amount of time that would be required to restore the data should it be lost; at a minimum, data should be backed up at least once a week.
Y	Establish procedures that allow facility access in support of restoration of lost data under the ORP and emergency mode operations plan in the event of an emergency.

**INFORMATION TECHNOLOGY PROJECT SUMMARY PACKAGE
SECTION A: EXECUTIVE SUMMARY**

1. Submittal Date	1/9/2006
--------------------------	----------

	FSR	SPR	PSP Only	Other:
2. Type of Document	X			
Project Number				

		Estimated Project Dates	
3. Project Title	Electronic Lab Reporting System	Start	End
Project Acronym	ELR	1/2006	10/2006

4. Submitting Department	California Department of Health Services
5. Reporting Agency	California Health and Human Services Agency

6.	Project Objectives
	<ol style="list-style-type: none"> 1. Provide an automated means of laboratory reporting and notification with a single, statewide lab reporting system. 2. Eliminate outdated manual reporting submissions. 3. Create a secure environment for confidential medical information to reside, restricting access to the data for reporting purposes. 4. Reducing elapsed time to collect data from LHDs measured from time of test to the time CDHS receives notification. 5. Increase laboratory reporting from lab partners by eliminating current manual processes. 6. Enable the sharing of data across LHDs and public health program areas and business functions 7. Establish a standard vocabulary and process to share standard data elements and formats statewide

8.	Major Milestones	Est Complete Date
	Vendor Eval. Criteria Complete Vendor Selected Hardware Software Installation Software Configuration Complete First Laboratory Tested/Certified	Feb 2006 May 2006 July 2006 Sept 2006 Oct 2006

7.	Proposed Solution
	The proposed solution is to implement a COTS/MOTS ELR solution compliant with CDHS needs.

**INFORMATION TECHNOLOGY PROJECT SUMMARY PACKAGE
SECTION B: PROJECT CONTACTS**

Project #	
Doc. Type	

Executive Contacts								
	First Name	Last Name	Area Code	Phone #	Ext.	Area Code	Fax #	E-mail
Agency Secretary	Kimberly	Belshé	916	654-3724		916		kbelshe@chhs.ca.gov
Dept. Director	Sandra	Shewry	916	440-7400		916		sshewry@dhs.ca.gov
Budget Officer	Mieko	Epps	916	552-8364		916		mepps@dhs.ca.gov
CIO	Christy	Quinlan	916	440-7340		916		cquinlan@dhs.ca.gov
Proj. Sponsor	Kevin	Reilly	916	440-7575		916		kreilly@dhs.ca.gov

Direct Contacts								
	First Name	Last Name	Area Code	Phone #	Ext.	Area Code	Fax #	E-mail
Doc. prepared by	Dr. Mark	Starr	916	552-9700				Mstarr1@dhs.ca.gov
Primary contact	Dr. Mark	Starr	916	552-9700				Mstarr1@dhs.ca.gov
Project Manager	John	Williamson	916	552-8624				jwilliam@dhs.ca.gov

INFORMATION TECHNOLOGY PROJECT SUMMARY
SECTION C: PROJECT RELEVANCE TO STATE AND/OR DEPARTMENTAL PLANS

1.	What is the date of your current Operational Recovery Plan (ORP)?	Date	
2.	What is the date of your current Agency Information Management Strategy (AIMS)?	Date	11/14/2003
3.	For the proposed project, provide the page reference in your current AIMS and/or strategic business plan.	Doc.	
		Page #	

Project #	
Doc. Type	

4.	Is the project reportable to control agencies?	Yes	No
	If YES, CHECK all that apply:		X
	X	a) The project involves a budget action.	
		b) A new system development or acquisition that is specifically required by legislative mandate or is subject to special legislative review as specified in budget control language or other legislation.	
	X	c) The estimated total development and acquisition cost exceeds the departmental cost threshold and the project does not meet the criteria of a desktop and mobile computing commodity expenditure (see SAM 4989 – 4989.3).	
	d) The project meets a condition previously imposed by Finance.		

**INFORMATION TECHNOLOGY PROJECT SUMMARY PACKAGE
SECTION D: BUDGET INFORMATION**

Project #	
Doc. Type	

Budget Augmentation Required?	No	<input checked="" type="checkbox"/>								
	Yes	<input type="checkbox"/>	If YES, indicate fiscal year(s) and associated amount:							
			FY		FY		FY		FY	
			\$		\$		\$		\$	

PROJECT COSTS

1.	Fiscal Year	2004/05	2005/06	2006/07	2007/08	2008/09	TOTAL
2.	One-Time Cost						
3.	Continuing Costs						
4.	TOTAL PROJECT BUDGET						

SOURCES OF FUNDING

5.	General Fund						\$
6.	Redirection						\$
7.	Reimbursements						\$
8.	Federal Funds						\$
9.	Special Funds						\$
10.	Grant Funds						
11.	Other Funds						
12.	PROJECT BUDGET						

PROJECT FINANCIAL BENEFITS

13.	Cost Savings/Avoidances	\$	\$	\$	\$	\$	\$
14.	Revenue Increase	\$	\$	\$	\$	\$	\$

Note: The totals in Item 4 and Item 12 must have the same cost estimate.

**INFORMATION TECHNOLOGY PROJECT SUMMARY PACKAGE
SECTION E: VENDOR PROJECT BUDGET**

Vendor Cost for FSR Development (if applicable)	\$
Vendor Name	

Project #	
Doc. Type	

VENDOR PROJECT BUDGET

1.	Fiscal Year	2004/05	2005/06	2006/07	2007/08	2008/09	TOTAL
2.	Primary Vendor Budget						
3.	Independent Oversight Budget						
4.	IV&V Budget						
5.	Other Budget						
6.	TOTAL VENDOR BUDGET						

-----**(Applies to SPR only)**-----

PRIMARY VENDOR HISTORY SPECIFIC TO THIS PROJECT

7.	Primary Vendor	
8.	Contract Start Date	
9.	Contract End Date (projected)	
10.	Amount	\$

PRIMARY VENDOR CONTACTS

	Vendor	First Name	Last Name	Area Code	Phone #	Ext.	Area Code	Fax #	E-mail
11.									
12.									
13.									

INFORMATION TECHNOLOGY PROJECT SUMMARY PACKAGE
SECTION F: RISK ASSESSMENT INFORMATION

Project #	
Doc. Type	

RISK ASSESSMENT

	Yes	No
Has a Risk Management Plan been developed for this project?	X	

General Comment(s)