C. Solution Architecture

1. System Security Compliance

The system must comply with all applicable CDPH security policies and requirements, as well as those specified in the State Administrative Manual (SAM), Public Health Administrative Manual (PHAM) Privacy Act, and any other applicable State or Federal regulation. All security safeguards and precautions must be subject to the approval of the CDPH ISO.

The system may share data with other entities only after all applicable agreements are in place. For example, using a CDPH data release form, Business Associate Agreement, or Data Use Agreement. These agreements must ensure data is protected according to all applicable standards and policies.

Any data which is exported outside the scope of the system and its security provisions (such as exports for statistical analysis) require approval by the CDPH ISO to ensure sufficient security is in place to protect the exported data.

2. Warning Banner

All systems containing CDPH information must display a login warning banner stating that information is classified, activity is logged, and system use is for business purposes only. User must be directed to log off the system if they do not agree and comply with these requirements.

The following warning banner must be used for all access points (such as desktops, laptops, web applications, mainframe applications, servers and network devices):

> ***WARNING: This is a State of California computer system that is for official use by authorized users and is subject to being monitored and/or restricted at any time. Unauthorized or improper use of this system may result in administrative disciplinary action and/or civil and criminal penalties. By continuing to use this system you indicate your awareness of and consent to these terms and conditions of use.***
>
> ***LOG OFF IMMEDIATELY, if you do not agree to the conditions stated in this warning.***

3. Layered Application Design

Applications must be able to be segmented into a layered application design separating, at a minimum, the Presentation, Application/Business Logic, and Data Access Logic, and Data Persistence/Database layers.

The Presentation, Application/Business Logic, and Data Access Logic layers must be separated physically by a firewall regardless of physical implementation.

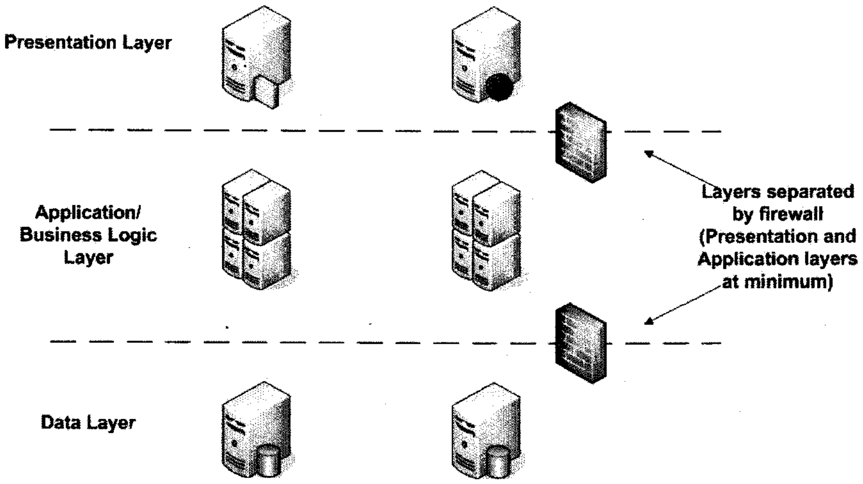
Any system request made to the Business logic layer must be authenticated.

The Data Access Logic Layer may take the form of stored procedures, database Application Programming Interface (API), Data Access Objects/Components, Data Access Middleware, Shared Data Services, or Secure Web Service. Any system request made to the Data Access logic layer must be authenticated and authorized. No direct access to the Data Persistence/Database layer will be permitted, except through the Data Access logic layer.

All calls to the Data Persistence/Database layer will be made through the Data Access logic layer as a trusted sub-system that utilizes a single database access account to all transactions.

The Data Access Logic Layer must take the form of stored procedures, database API, Data Access Objects/Components, Data Access Middleware, Shared Data Services, or Secure Web Service. System requests made to the Business logic and Data Access logic layers must be authenticated and authorized.

Vendor-provided commercial off-the-shelf (COTS) packages, or components where physical separation of layers is not possible, requires CDPH ISO approval.


Presentation Layer
Application/ Business Logic Layer
Data Layer
Layers separated by firewall (Presentation and Application layers at minimum)

4. Input Validation

All user input must be validated before being committed to the database or other application information repository. The system must manage client input controls from server side to the extent possible. Data queries from the Presentation or the Business Logic layers must be validated for appropriate use of query language, and validated for appropriate quantity and quality of data input. This includes In-line Structured Query Language (SQL) calls. The system must validate client input on the server side to the extent possible. All third-party client side input controls must be documented and approved by the CDPH ISO.

5. Data Queries

All Data queries (including In-line SQL calls) will not be allowed from the Presentation or the Business Logic layers unless validated for appropriate use of query language and validated for appropriate quantity/quality of data input. All data queries solution must be approved by the CDPH ISO.

Database table names and column names must not be exposed. Applications must use an alias for every table and column.

Dynamic SQL will not be permitted from the Presentation Layer without prior approval from the CDPH ISO.

6. Username/Password Based Authentication

When usernames and passwords are going to be used as the method for system authentication, the following requirements must be met:

- Username requirements:
  - Must be unique and traceable to an individual.
  - Must not be shared.
  - Must not be hard-coded into system logic.
- Password requirements:
  - Must not be shared.
  - Must be 8 characters or more in length.
  - Must not be a word found in the dictionary, regardless of language.
  - Must be encrypted using irreversible industry-accepted strong encryption.
  - Must be changed at least every 60 days.
  - Must not be the same as any of the previous 10 passwords.
  - 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:
    - Upper case letters (A-Z);
    - Lower case letters (a-z);
    - Numbers (0 through 9); and
    - Non-alphanumeric characters (punctuation symbols).
- Account security:
  - Accounts must be locked after three (3) failed logon attempts.
  - Account lock-out reset timers must be set for a minimum of 15 minutes.
  - Accounts must be promptly disabled, deleted, or the password changed upon the transfer or termination of an employee with knowledge of the password.

7. Administrative / Privileged Accounts Management

A privileged account is an account that allows an individual to perform maintenance on an operating system or applications (e.g. create/remove users, install applications, create/modify databases, etc.). Privileged accounts require the approval of the individual's manager, the CDPH ISO, and must include a business justification stating why privileged access is required and what it will be used for. Individuals granted privileged accounts must have already signed the Security and Confidentiality Acknowledgement Statement. (Contact the CDPH ISO for the current version of the Security & Confidentiality Acknowledgement Statement in use.)

The use of shared privileged accounts (e.g. Administrator) is strictly prohibited.

System administration must be performed using a different username rather than the one used for daily non-administrative activities. Administrative accounts must be used only for administrative activity within the authorized role of that account and the individual using it. It must be logged out of immediately after administrative work is complete.

- Username requirements:
  - Must be unique and traceable to an individual.
  - Must not be shared.
  - Must not be hard-coded into system logic.
  - Must be the same across different zones (e.g. Web Zone, Internal network, and Test Labs / Environments).
  - The default built-in Administrator account must be renamed and disabled.

    - The naming convention for privileged accounts must not make it obvious that usernames belong to privileged accounts.
    - If a generic privileged account is created:
        - Must only be used in an Emergency.
        - Must not be used for routine maintenance.
        - The password storage and management process for generic privileged accounts must be approved by the CDPH ISO.
- Password requirements:
    - Must not to be shared.
    - Must be 12 characters or more in length.
    - Must not be a word found in the dictionary, regardless of language.
    - Must be encrypted using irreversible industry-accepted strong encryption.
    - Must be changed at least every 60 days.
    - Must not be the same as any of the previous 10 passwords.
    - Must be changed immediately if revealed, or compromised.
    - Must be comprised of characters from at least three of the following four groups from the standard keyboard:
        - Upper case letters (A-Z);
        - Lower case letters (a-z);
        - Numbers (0 through 9);
        - Non-alphanumeric characters (punctuation symbols).
    - Must be changed immediately upon the termination or transfer of an employee with knowledge of the password.
    - Must not be the same across different zones (e.g. Web Zone, Internal network, and Test Labs / Environments).
- Account security:
    - Accounts must be locked after three (3) failed logon attempts.
    - Account lock-out timers must be set for at least 60 minutes.

8. Service Accounts Management

A service account is an account used to run a service and whose password is known by multiple individuals, When and where it is necessary to use a service account, the account request will be approved by the manager of the Project/Program requesting the account and by the CDPH ISO. Requirements, stating the need for a service account, will be documented in the request. A service account password is shared among the individuals authorized to access the account, and is subject to controls as stated in the password requirements in this document.

Restrictions for Service Accounts

- Sharing passwords via email is prohibited, unless the body of the email itself is encrypted using strong encryption.
- When users are no longer authorized to access an existing service account, the service account password must be changed.

9. Authentication and Authorization

Any system deployed during a project, or as a result of a project, must provide secure role-based access for authorization (separation between system/server administrators and application/database administrators) utilizing the principle of least privilege at all layers/tiers.

In all cases, applications must default to explicitly deny access where authentication and/or authorization mechanisms are required. No application that requires a login can offer to, or be capable of, remembering a user's credentials.

10. Authentication Logging

The 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 must be included for all user privilege levels including, but not limited to, systems administrators. This requirement applies to systems that process, store, and/or interface with CDPH information.

11. Automatic System Session Expiration

The system must provide an automatic timeout, requiring re-authentication of the user session after 20 minutes of inactivity.

12. Automatic System Lock-out and Reporting

The system must provide an automatic lock-out of users and a means to audit a minimum of three (3) failed log-in attempts. The means of providing audit information must be approved by the CDPH ISO.

13. Audit (Access)

All systems/applications will implement role-based access to auditing functions and audit trail information utilizing the principle of least privilege.

All systems/applications will implement a secure online interface to Audit Capabilities and Reporting by way of API or network service (or Web Service) to allow CDPH ISO to view logs, auditing procedures, and audit reporting.

14. Audit (Minimum Information)

The minimum log information below is required for any system that contains, or is involved in the transmission of, classified information. The log information should be available on every system running a production environment. This information must be provided upon request of the CDPH ISO for investigations and risk assessments.

The system must record, at minimum, the following events and any other events deemed appropriate by the CDPH ISO:

<u>Transaction Types</u>

- Any and all administrative changes to the system (such as administrative password changes, forgotten password resets, system variables, network configuration changes, disk sub-system modifications, etc).
- Logon failures.
- Logons during non-business hours.
- Failed access to an application or data.
- Addition, deletion, or modification of users or program access privileges.
- Changes in file access restrictions.
- Database addition, deletion, or modification.
- Copy of files before and after read/write changes.
- Transaction issued.

Individual audit trail records must contain the information needed to associate each query transaction to its initiator and relevant business purpose. Individual audit trail records should capture, at a minimum, the following:

Minimum Audit Trail Record Content

- Date and time stamp.
- Unique username of transaction initiator.
- Transaction recorded.
- Success or failure of transaction recorded.
- Relevant business process or application component involved.
- Data captured (if any).

Audit Trail logs must be maintained at minimum for three (3) years after the occurrence, or a set period of time determined by the CDPH ISO that would not hinder a detailed forensic investigation of the occurrence. The CDPH ISO has final approval authority.

15. Application Security Controls

For any application which accesses classified information, the following technical controls must be present, unless an exception is granted by the CDPH ISO:

- Must use *least privileged accounts* to execute code and to access databases.
- User access rights must be authenticated and authorized on entry to each application tier.
- All user input must be validated, including parameters passed to all public web service methods.
- Information that is not required must not be exposed.
- If a web application fails, it must not leave sensitive data unprotected or expose any details in error messages presented to the user. Any exceptions must be logged or emailed to the appropriate team member.
- Any sensitive data stored in session, cookies, disk files, etc., must be encrypted. Any sensitive data passed between tiers must be encrypted or must use SSL.
- Applications must be protected from the Internet by a front-end web application, firewall, gateway, and proxy of a type approved by the CDPH ISO, which must be included in the documented system design.
- Postback Universal Resource Locators (URLs) must not contain unencrypted record identifiers or database keys.
- Postback URLs must not include query strings.

16. Application Code Security

Application developers should use tools and methods during development to ensure all custom source code is free from security vulnerabilities. At a minimum, the application must be free of the vulnerabilities described in the CWE/SANS Top 25 Most Dangerous Programmer Errors (http://www.sans.org/top25errors/).

CDPH has the right to conduct a vulnerability scan against the application prior to its activation, and may disapprove use of the application until the vulnerabilities are remediated and the application re-tested. Any verified vulnerabilities from this list must be corrected by the organization which developed the application, at no additional cost to CDPH. Unless an exception is granted by the CDPH ISO, vulnerabilities identified within third-party components must be remediated by the third-party vendor at no additional cost to CDPH. Otherwise, a different third-party component must be selected and implemented.

17. Strong Authentication

Any information system providing access to Personally Identifiable Information (PII) and/or classified information from the Internet must assess the need for additional strong authentication, to prevent a significant data breach if a password is compromised. Strong authentication is defined as additional mandatory authentication over and beyond the password, for each account which has direct access to PII and/or classified information, or which has administrative privileges. The following factors should be included in the assessment:

- Applicable policies and regulations.
- Sensitivity of the PII or classified information.
- Number of data records.
- Number of user accounts with access to data.
- Level of control over end users.
- Level and frequency of log monitoring.
- Automated alerts and controls for unusual data access patterns.
- End user training on security practices.
- Other mitigating security controls.

The Project/Program providing access to PII and/or classified information from the Internet must either implement an approved strong authentication method, or document why strong authentication will not be utilized. This documentation must be provided to the CDPH ISO for review and approval.

The following methods are approved for strong authentication:

- **Physical Token:** A physical device in the possession of the account holder, which must be physically connected to the computer. Examples include a USB token or Smartcard.
- **One Time Password (OTP):** A temporary one time pass code is provided to the account holder, either by a physical device in their possession, or by way of a pre-defined communication channel such as cell phone or e-mail address. Examples include OTP token, or OTP sent via SMS text message, e-mail, or by automated voice call.
- **X.509 Certificate:** A digital certificate which has been installed on the access point computer or device, utilizing a Public Key Infrastructure (PKI).
- **Firewall Rules:** Firewall TCP/IP rules which ensure the account is only usable from an authorized access point, based upon specific IP address or IP subnet.

The following strong authentication method is approved for personal data access, where accounts have access to only the account holder's personal data, or a single data record they are custodian over such as a family member or information about their company. For example, an application where a client can submit or edit an enrollment form for themselves or someone else, but cannot access any other data records.

- **Personal Challenge Questions:** During registration, the account holder pre-answers one or more questions known only to them. When logging into a different computer, typically tracked with a cookie, they cannot login without correctly answering the pre-configured questions. The user should be prompted for whether the new computer is trusted vs. a one-time login, and this information used to determine whether to save a new cookie.

The proposed strong authentication mechanism must be included in the detailed design documentation as described in Section E.5, Application Security Approvals.

D. Documentation of Solution

1. System Configuration

Project/Program must document and maintain documentation for the system/application. This should include the following:

- Detailed design.
- Description of hardware, software, and network components.
- Special system configurations.
- External interfaces.
- All layers of security controls.

2. Information Classification

Project/Program will document and maintain an information classification matrix of all information elements accessed and/or processed by solution.

The matrix should identify at a minimum:

- Information element.
- Information classification/sensitivity.
- Relevant function/process, or where is it used.
- System and database, or where is it stored.

3. System Roles and Relationships

Project must document the following roles and ensure everyone understands their role, and complies with all applicable policies and regulations.

- The designated owner of the system.
- The designated custodian(s) of the system.
- The users of the system.
- The security administrator for the system.
- Outside entities sending or receiving data to system.

Project must document the organizational structure and relationships between these roles.

4. Audit Method Documentation

Project/Program will document the solution's auditing features and provide samples of audit reporting.

5. Retention of Documentation

The system/application administrators will retain documentation, including audit and activity logs, for a minimum of three (3) years (up to seven (7) years maximum) from the date of its creation or the date it was last in effect, whichever is later. Shorter retention periods must be allowed contingent upon applicable regulations, policies, and standards, and upon approval by the CDPH ISO. In certain circumstances the retention period must be lengthened to comply with regulatory requirements.

E. ISO Notifications and Approvals

1. Security Compliance Notification

As part of each project, assigned staff will document how the proposed solution meets or addresses the requirements specified in this document. This documentation must be submitted to the CDPH ISO prior to taking custody of CDPH information.

2. Notification of Changes to Solution

Once a project is approved as final by the CDPH ISO, no changes will be made to the project scope, documentation, systems or components without a change approval by the CDPH ISO.

3. Notification of Breach

The system/application administrators must immediately, and in writing, report to the CDPH ISO any and all breaches or compromises of system and/or information security. They must also 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 information security, the CDPH ISO may require a system/application security audit. The CDPH ISO must review the recommendations from the security audit, and make final decisions on the steps necessary to restore security and repair damage.

The system/application administrators must properly implement any and all recommendations of the security audit, as approved by the CDPH ISO.

4. Project Security Approvals

Projects must ensure checkpoints throughout the System Development Life Cycle (SDLC) which verify security requirements are being met. This must be incorporated in the project plan along with identification of necessary resources, timelines, and costs to address these requirements. The CDPH ISO should be involved throughout the SDLC to ensure this occurs.

For reportable Feasibility Study Reports (FSRs), the California Office of Information Security (OIS) requires submission of the *Questionnaire for Information Security and Privacy Components in Feasibility Study Reports and Project-Related Documents*.
See
http://www.cio.ca.gov/OIS/Government/documents/docs/Info_Sec_and_Priv_Components_FSR-Questionnaire.doc.

The response to this document must be approved by the CDPH ISO prior to submission.

Projects must ensure all applicable security requirements and deliverables are included in the project plan, and that ISO approvals are obtained, where required. This includes those listed in the following section, and any covered by other sections of this document. The CDPH ISO must be given reasonable time to review and comment on these deliverables.

5. Application Security Approvals

At a minimum, for any application which accesses classified information, the following documented CDPH ISO approvals must be obtained at the appropriate project phases, and before the application is moved to production.

- CDPH ISO approval of a dated, detailed design document. This design must include network layout including specific firewall port requirements, server hosting locations, operating systems, databases, data exchange interfaces, and points of authentication/authorization. The project must not move beyond the design phase until there is a CDPH ISO approved design.
- CDPH ISO approval of any non-standard development tools (such as programming languages or toolkits).
- CDPH ISO approval of a plan for an independent security code review which addresses at minimum the current Open Web Application Security Project (OWASP) top ten application vulnerabilities, and CWE/SANS Top 25 Most Dangerous Programmer Errors, where applicable. CDPH ISO must approve any findings of that code review not being corrected. CDPH ISO recommends the security code review be carried out during the development process rather than only at the end.
- CDPH ISO approval of a plan for security code reviews of future maintenance code changes, which addresses at minimum the current OWASP top ten application vulnerabilities, CWE/SANS Top 25 Most Dangerous Programmer Errors, where applicable.
- CDPH ISO approval of a plan for an independent automated security vulnerability assessment of the application, and approval of the findings of that assessment. The assessment must assess at minimum the OWASP top ten risks and CWE/SANS Top 25 Most Dangerous Programmer Errors, where applicable.

Independent as indicated above is defined as organizationally separate from those developing or configuration the application. The independence and skill level of the entities being utilized must be approved by the CDPH ISO.

Application code and infrastructure is subject to a CDPH ISO audit, and must match the approved detailed design.

F. Appendix A – SR1 Exemption Form

REF	Security Requirement	Exemption (Yes, No, or N/A)	Business Justification
A	**Administrative / Management Safeguards**		
1	Workforce Confidentiality Statement		
2	Access Authorization & Maintenance		
3	Information System Activity Review		
4	Periodic System Security & Log Review		
5	Disaster Recovery Plan		
6	Change Control		
7	Supervision of Information		
8	Escorting Visitors		
B	**Technical and Operational Safeguards**		
1	System Security Compliance		
2	Malware Protection		
3	Patch Management		
4	Encrypted Electronic Transmissions		
5	Encrypted Data Storage		
6	Workstation / Laptop Encryption		
7	Removable Media Encryption		
8	Secure Connectivity		
9	Intrusion Detection and Prevention		
10	Minimum Information Download		
11	Information Sanitization		
12	Removal of Information		
13	Faxing or Mailing of Information		
C	**Solution Architecture**		
1	System Security Compliance		
2	Warning Banner		
3	Layered Application Design		
4	Input Validation		
5	Data Queries		
6	Username/Password Based Authentication		
7	Administrative / Privileged Accounts Management		
8	Service Accounts Management		
9	Authentication and Authorization		
10	Authentication Logging		
11	Automatic System Session Expiration		
12	Automatic System Lock-out and Reporting		

REF	Security Requirement	Exemption (Yes, No, or N/A)	Business Justification
13	Audit (Access)		
14	Audit (Minimum Information)		
15	Application Security Controls		
16	Application Code Security		
17	Strong Authentication		
D	**Documentation of Solution**		
1	System Configuration		
2	Information Classification		
3	System Roles and Relationships		
4	Audit Method Documentation		
5	Retention of Documentation		
E	**ISO Notifications**		
1	Security Compliance Notification		
2	Notification of Changes to Solution		
3	Notification of Breach		
4	Project Security Approvals		
5	Application Security Approvals		