**Section 1: Data Classification and Data Collection**

Data collection methodologies and processes will vary dependent on the category of data being collected. Per the Washington States [Office of the Chief Information Officer Policy 141.10](https://ocio.wa.gov/sites/default/files/public/policies/141.10_SecuringITAssets_201711_Approved.pdf?f5mmyeu) all state agencies must use the following classification for data:

|  |
| --- |
| **DATA CLASSIFICATION LEVEL MATRIX**   |
| **LEVEL:**  | **PUBLIC (Category 1)** | **INTERNAL (Category 2)** | **CONFIDENTIAL (Category 3)** | **RESTRICTED (Category 4)** |
| **LOSS OF CIA COULD CAUSE**Confidentiality, Integrity, Availability (CIA) | **LOW** impact to agency but needs integrity and availability controls. | **LIMITED** impact to agency, affiliates and employees. | **SERIOUS ADVERSE** impact to agency, affiliates and employees legally or financially; or damage public integrity. | **SEVERE or CATASTRAPHIC** adverse impact to agency, affiliates, employees or the affected individuals; or damage agency reputation. |
| **DESCRIPTION**  | **Public** information which does not need protection from unauthorized disclosure.  | **Sensitive** information for official use only and requires authorization from data owner.*\* May not be protected by public records disclosure laws.* | **Confidential** information that is **protected** **by public records disclosure laws**.*\* RCW 42.56.590 notification if there is a breach in the security of certain unencrypted information.* | **Confidential** information with a need for added protection or **strict handling required by law, contract, or agreement.** |
| **EXAMPLES**Personally Identifiable Information (PII), Personal Health Information (PHI), Electronic Protected Health Information (EPHI) | **Public domain** – Widely distributed material, agency public website, brochures, pamphlets, financial reports required by regulatory authorities. | **PII** – Personal phone numbers, addresses, full/maiden names, place of birth, email address, information not protected by law.**Organization** - Agency processes, procedures, activities.\* *PII context of use affects the degree of data level classification.* | **Personal Information** – Information that is specifically protected from either release or disclosure by law (may include PII). Personal information as defined in RCW 42.56.590 and RCW 19.255.10. Public employee or health professional contact information. Information as defined in RCW 42.56.250, RCW 42.56.070.**Contractual** – RFP, RFQ, RFI responses, contract negotiation, proprietary data, non-disclosure agreements with clients/vendors.**Investigations** – Ongoing investigative/complaint files, criminal history, industrial insurance claims, tort claims**Emergency Response/Recovery** – Plans, processes, procedures, shared secrets, codes.**IT infrastructure** – Telecommunication systems, network architecture, system diagrams, IP address, UserID/password combinations, information as defined in RCW 42.56.420. | **PII** – SSN, DEA#, individual taxpayer identification #, passport #, fingerprints.**PHI** – medical records, X-rays, biomedical or behavioral research records, test results, medical case numbers, coroner reports.**EPHI** – physical storage or transmission media, internet/extranet/systems transmitting PHI.**Individually Identifiable Health Information** – Health plan numbers, HIV/STD lab test results, accident reports, Geo-coded patient addresses stored as GIS points.**Financial** – credit/debit account numbers and tracking data, bank account numbers, PINS, expiration dates, passwords.**Security** – Computer/network passwords. |
| **ACCESS** | No restriction | Limited to DOH staff and business partners with a need-to-know.Authorization may be explicit or implicit. | Limited to explicitly authorized DOH staff and business partners with a need-to-know. Data sharing agreements, individual release forms and/or statutory regulations are required. | Same as previous |

***Information shall be classified when:***

* + - 1. a new application or system is planned
			2. a new data collection/database is planned
			3. existing data collections/databases are linked or otherwise combined
			4. changes to existing data collections/databases impact the classification level
			5. changes to regulatory requirements impact the classification level
			6. changes to an existing applications or systems impact risk
			7. changes to how data flows through existing systems or infrastructure are planned

***Data classification levels shall be assessed:***

* + - 1. During technical reviews
			2. During risk and security assessments
			3. When a potential or actual security breach is reported.

Below is an outline of the major surveillance platforms in which varying aspects of notifiable conditions reporting data across the state would be collected under the ELC project grant:

* Washington Disease Reporting System (WDRS): Clinical, Laboratory, Immunization, public health case and contact management data. Category 4 level data.
* Washington Electronic Laboratory Reporting System (WELRS): Non-standardized HL7 Electronic Reporting Data (includes reportable and non-reportable disease conditions). Category Level 4
* DRIVE: Standardized Electronic Laboratory Reporting Data for only reportable conditions. Category Level 4 data.
* Electronic Case Reporting Data (eCR): Direct connection to electronic medical records for review of clinical data for potential public health notifiable conditions investigation and case management support. Category 4 level data.
* Rapid Health Information NetwOrk (RHINO): Direct connection to de-identified public health syndromic surveillance data linked to electronic health records within all state emergency departments, urgent cares, and clinical settings.
* Birth Defects Registry: registry of birth defects within WA state documented in birth certificates or from clinical report. Data specific for Zika prevention and management project. Category 4.
* Vital Statistics System (WHALES): Birth and death certificate data. Category 3 level data.
* Electronic Test Ordering System: Public Health Lab specimen retrieval, testing, and result sharing platform for any test being conducted at the state Public Health Lab. Category 4 level data.
* Laboratory Information Management System: Public Health Lab Specimen processing and result reporting system for local health and DOH disease investigators. Category 4 level data.
* Bioinformatics Analysis System: Public Health Laboratory instrument operational tracking system to monitor instrument performance and outputs. Category level 1 data.
* Central Accessioning Specimen Tracking System: Paper and electronic based data tracking process system for pass through of specimen from clinical labs to PHL to CDC or other regional lab testing partners. Category 3 level data.
* Promoting Interoperability data provider system: Tracking list of data providers, list of status with reporting compliance, and monitoring of data issues for quality improvement efforts. Category 2 level data.
* Others (Data@Health)

**Section 2: Data Sharing and Security**

The IT Security Officer (ITSO) is authorized by the Secretary, Department of Health (policy 10.002) to establish IT security policies, standards and guidelines to protect the integrity, availability and confidentiality of agency IT resources.

These standards apply to all DOH employees, programs, offices and divisions. They impact the entire agency and its public/private partners. They apply to all IT activities; whether they are operated by or for the agency.

If compliance with these standards is not technically or operationally feasible, [exceptions](http://dohweb/dirm/Standards/exceptions.htm) may be permitted. All exception requests must be submitted to the ITSO and approved by the Chief Information Officer (CIO).

To achieve our mission and maintain the public’s trust we must act as responsible stewards of the information we hold. We must provide appropriate access to confidential information in limited situations authorized by law. We must protect the privacy of individuals and make sure confidential information is protected from inadvertent or intentional misuse and disclosure.

***Data Sharing Requirements:***

* + 1. [DOH Policy 17.006 Release of Confidential Data/Information](http://dohweb/About/Pol_Pro_DOC/17-006.doc) outlines the responsibilities that govern the release of confidential information and the use of data sharing agreements and contracts. The following requirements are addressed in the policy:
			1. Confidential information must be shared only when permitted by law.
			2. Only the minimum amount of information (both records and elements) necessary to accomplish an authorized purpose may be released.
			3. Data sharing agreements or contracts must be in place prior to releasing confidential information.
			4. The standard DOH data sharing agreement template must be used. Changes to the established templates must be done in consultation with the Contracts Office, IT Security Officer and Privacy Officer
		2. Data sharing agreements and contracts must include security requirements for the protection of confidential information
			1. Data sharing agreements and contracts must include security requirements that are consistent with DOH, state and federal requirements.
			2. Special attention must be paid to requirements for access, storage, transmission and disposal of electronic information. See the sections on [data classification](#Classification), [backup requirements](#DataBackup), and [encryption](#DataEncryption) for more information.
		3. The agreements and contracts shall include notification requirements for reporting unauthorized access, use or disclosure to the DOH IT Security and Privacy Officers

| **DATA CLASSIFICATION SECURITY CONTROLS MATRIX** |
| --- |
| **HANDLING STANDARDS** | **PUBLIC** | **INTERNAL** | **CONFIDENTIAL** | **RESTRICTED** |
| **PASSWORDS**  | **All passwords are classified RESTRICTED and must not be stored or transmitted in clear text.**  |
| **AUTHORIZATION OF uSER pRIVILEGES** |   |   |   |  |
| a. Access authorization to network share drives and applications | Available to any internal or external user. | Access is based on a business need-to-know.  | Access is based on a business need-to-know. Requires explicit written authorization for named users or roles, or named services by the data owner/steward.  | Access is based on a business need-to-know. Requires explicit non-transferable written authorization for named users or named services by the data owner/steward.  |
| b. Access authorization records.  | No collection required | The collection and retention of records documenting when access is authorized and who authorized it is required when integrity is a priority. | The collection and retention of records documenting when access is authorized and who authorized it is required. | Same as previous |
| **AUTHENTICATION REquirements** |  |  |  |  |
| 1. Internal Authentication – from behind the DOH internal firewall to internal network systems and services: including Intranet applications
 | Requires enterprise active directory authentication  | Same as previous  | Same as previous  | Same as previous  |
| b. Remote Access Authentication – from external networks to internal network systems and services. (behind DOH firewalls) | Access must be controlled through DIRM and/or CTS managed secure gateways. Requires two-factor authentication using hard or soft tokens/certificates | Same as previous | Same as previous | Same as previous |
| **NOTE:** See the [Access Security Standards](http://dohweb/dirm/Security/SecStnds/AccessSecurityStandards.doc) for specific requirements |
| **AUTHENTICATION REquirements (Cont’d)** |  |  |  |  |
| c. Internet Application Authentication - Access to a Web application that enables the public or business partners to access information.  | No verification of identity required (anonymous access). | Requires user-ID / password authentication through Secure Access Washington (SAW)  | Requires multi-factor authentication through SAW. Use of tokens or digital certificates is recommended.Note – a single record belonging to the individual may be accessed using user-ID / password authentication through SAW. | Same as previous except digital certificates or hard tokens are required.Note – a single record belonging to the individual may be accessed using alternate multi-factor authentication methods offered through SAW |
| **NOTE:** See the [Access Security Standards](http://dohweb/dirm/Security/SecStnds/AccessSecurityStandards.doc) for specific requirements |  |
| **EVENT LOGGING** |  |  |  |  |
| a. Audit trail requirements. | The collection, retention and periodic review of system logs that meets the minimum requires as defined in the [Security Monitoring and Log Management Standards](http://dohweb/dirm/Security/SecStnds/Security_Mon_Log_Management.doc) is required. | Same as previous. except when integrity is a priority, actions taken by all accounts must be documented   | Same a previous except the actions taken by all accounts must be documented  | Same as previous |
| **RELEASE TO THIRD PARTIES** |  |  |  |  |
| See  [policy 17.006 Release of Confidential Data/Information](http://dohweb/About/Pol_Pro_DOC/17-006.doc)  | Available for distribution outside of the organization.  | Intended for use within the DOH.  | For use on a need-to-know basis only. May only be released according to specified policies and procedures and as permitted by statue. Data sharing agreements or contracts are required | Same as previous**NOTE**: Information is very sensitive and should be closely controlled from creation to destruction.  |
| **TRANSMISSION VIA NETWORK/INTERNET** |  |  |  |  |
| 1. Transmissions within the internal network.
 | Encryption not required for internal transmissions  | Same as previous | Same as previous | Same as previous |
| b. Transmissions to the internal network originating from external sources (VPN, Citrix, etc). | Connections must be obtained through encrypted sessions (128 bit minimum). Authentication methods as described in [Remote Access authentication](#remote_access) above are required. | Same as previous | Same as previous | Same as previous  |
| c. Transmissions to external sourcesIncludes FAX and phone Internet transmissions  | No restrictions | No RestrictionsConsider use of encrypted session (128 bit minimum) or file encryption if data integrity is a priority. | Encrypted sessions or file encryption methods required. Consider use of public key encryption methods.Must have a contract or data sharing agreement or contact in place. | Same as previous.  |
| d. File Transfer Protocol | No restrictions. | No RestrictionsConsider file encryption or secure file transfer if data integrity is a priority. | Secure file transfer is requiredSee [Appendix A](#sft) for specific secure file transfer requirements | Same as previousConsider use of public key file encryption methods for an additional layer of protection. |
| e. Transmissions to and from Internet applications or Web services | No restrictions. | Encrypted session outside the SGN required.  | Encrypted sessions and multi-factor authentication methods as described in [authentication requirements](#Internet_Authentication) above are required. | Same as previous  |
| **NOTE:** See [encryption requirements](#EncryptMethods) for more information |
| **Email transmissions** |  |  |  |  |
|  a. Sent to addresses within DOH  | No restrictions | No restrictions | No Restrictions. Use of email without encryption is discouraged.Consider use of secured network shares, or secure file transfer. | Same as previousPublic key file encryption or Secure email is strongly encouraged. |
|  b. Sent to addresses outside DOH  | No restrictions | No restrictions Consider file encryption or secure file transfer if data integrity is a priority. | File encryption, or secure e-mail is required.  | Public key file encryption or Secure email required. |
|  c. Use of distribution lists  | No restrictions | No restrictions  | Broadcast to distribution lists is discouraged. Verify recipients before sending. | Broadcast to distribution lists is prohibited |
|  d. Transmission safeguards  | No restrictions | Verify recipients before sending.  | Same as previous  | Same as previous  |
| **FAX transmissions** | Reasonable care in dialing. | Reasonable care in dialing. | **Sending** –Permitted only to [Public Health Partners](#Partners); or when the specific individual has provided written pre-authorization; or when authorized by statute.**Receiving** - Location of receiving fax machine must be in a limited access area or in presence of specific recipient.  | **Sending** - Same as previous**Receiving:** * Same as previous
* Consider use of password controlled printing options.
 |
| **Development** | No Restrictions | Use for development purposes is discouraged. Requires prior approval from the Data Owner/Steward. Security controls must meet or exceed the controls described in this matrix | Use for development purposes is prohibited | Same as previous |
| **Electronic StoragE** |  |  | Media must be “sanitized” as described under [disposal](#Disposal) before it is sent out for repair |
| 1. DOH production network servers
 | No restrictions.Access to consoles must be restricted to authorized IT administrators. | Same as previous EXCEPT access to the data must be restricted to authorized users | Same as previous, EXCEPT: Access must be limited to specifically authorized users AND access to consoles must be limited to named IT administrators.File, column or platter level encryption is required if data is not stored on a physical server dedicated to confidential data. External application access to the physical host must be restricted to the confidential DMZ. | Same as previous, EXCEPT: File or database column level encryption is required for passwords and credit cardholder data. File or database column level encryption is strongly recommended for all other restricted data. |
| 1. non-mobile computer workstation (desktop) hard drives
 | Storage of data is discouraged. | Same as previous. | Same as previous EXCEPT prior written authorization from the Data Owner/Steward AND encryption is required  | Same as previous.  |
| 1. Portable or Mobile devices: such as laptops, PDAs, Blackberry, cell phones etc.
 | Care must be taken to protect the device from loss, theft or unauthorized use. | Same as previous  | Same as previous EXCEPT Prior written authorization from the Data Owner/Steward AND encryption is required.  | Same as previous  |
| 1. Backup Media
 | Mission critical data must be stored in a DOH data center or other ITSO approved facility.  | Same as previous  | Same as previous. Must be encrypted if stored off site. If unencrypted, must be stored in a DOH Data Center with access restricted to named IT administrators. Encryption is strongly recommended.  | Same as previous EXCEPTEncryption is required. |
| 1. Removable magnetic or optical storage media (CDs/DVDs, tapes, USB devices, etc.)
 | No special precautions required.  | Same as previous  | Same as previous EXCEPT prior written authorization from the Data Owner/Steward AND encryption is required.  | Same as previous  |
| **NOTE:** See [Section 4 Data Encryption](#DataEncryption) above and the [Physical Security Standards](file://DOHFLTUM01/Division/DIRM/Administration/ITSO/IT%20Security%20Standards/For%20CIO%20Approval/PhysicalSecurity.doc) for specific requirements |
| **Workstation Computers** |  |  |  |  |
| a. Workstation location | No restrictions | No restrictions | Positioned or shielded to prevent viewing by unauthorized parties is recommended.  | Same as previous  |
| b. Securing workstation computers | Computers must be turned off, logged off, or password-locked when unattended.  | Same as previous. | Same as previous | Same as previous |
| **PRINTING AND SCANNING** |  |  |  |  |
| c. Printing  | No special precautions. | Use of a local or DOH network printer is recommended.  | Data Steward authorization is required. Unattended printing is permitted when * The printer is accessible by authorized persons only, or
* the printer is configured to request a password before printing
 | Same as previous |
| d. Scanning hardcopy documents | No special precautions. | Same as previous | Data Steward authorization is required. See [electronic storage](#Electronic_Storage) above for storage and encryption requirements.Unattended scanning is permitted only when the scanner is not accessible to unauthorized persons.  | Same as previous  |
| **TELECOMMUNICATONS** |  |  |  |  |
| a. Wireless Headsets. | No restrictions | No restrictions | Use of encryption between headset and phone is recommended. | Use of encryption between headset and phone is required. |
| a. Cell Phones. | No restrictions | No restrictions | Use of cell phones must be infrequent and short in duration. | Same as previous.  |
| **TELECOMMUNICATONS (continued)** |  |  |  |  |
| 1. Voice messages.
 | No restrictions | No restrictions | Deletion after retrieval is required. If the message must be retained see [electronic storage](#Electronic_Storage) above for specific storage and encryption requirements | Same as previous  |
| **disposal** |  |  |  |  |
| 1. Fixed Media - magnetic or optical storage media.
 | **disposal:** Media must be destroyed or deposited in locked DOH destruction bins designated for magnetic media. **Reuse:** Media must be "sanitized" using a DOH standard data cleaning utility before reuse. See the [Physical Security Standards](http://dohweb/dirm/Security/SecStnds/PhysicalSecurity.doc) for specific requirements | Same as previous | Same as previous EXCEPT media must be sanitized using a DOH standard data cleaning utility before sent out for repairs, or surplusSee the [Physical Security Standards](http://dohweb/dirm/Security/SecStnds/PhysicalSecurity.doc) for specific requirements | Same as previous |
| 1. Removable magnetic or optical storage media (CDs, DVDs, Diskettes, tapes, USB Disk devices, etc.)
 | No special precautions required. | Same as previous | Same as for a. [Fixed Media](#Media_Disposal) above | Same as previous |

**Section 3: Data Security Roles and Responsibility**

The table below defines the required roles for all DOH data applications or systems.

|  |  |  |
| --- | --- | --- |
| **ROLE** | **DEFINITION** | **RESPONSIBILITIES include…** |
| **Data Owner** | Data Owners are the department’s Secretary, Chief of Staff and Assistant Secretaries.  | Holds staff accountable for the stewardship of information. Delegate the authority to create, maintain and protect information to Data Stewards and Data Custodians.Promote responsible and effective data resource management. |
| **Data Steward** | DOH employees who have been delegated the authority by Data Owners to create, maintain and protect electronic information within their program.  | Determine the classification of the information for which they have delegated authority. Assure the information is protected in accordance with its current classification and regulatory or contractual requirements. Make decisions about the permissible uses of the information and authorizing user access to it. |
| **Data Custodian** | Information Technology staff with technical control of the information.  | Protect the information in their possession from unauthorized access, use, alteration, or destruction. Change or enable access to the information only after receiving authorization from the appropriate Data Steward. Report possible or actual security vulnerabilities or violations to the CISO and the Data Steward.  |
| **Users** | People who are authorized to access and use information.  | Use the information only for the purposes specifically approved by the Data Steward. Adhere to all DOH IT security policies, procedures, standards, and guidelines. Sign the Employee Confidentiality Statement upon initial employment and annually thereafter.Maintain the confidentiality of information they access.Report possible or actual security vulnerabilities or violations to the CISO and Data Steward. |

**Section 4: Data Archival**

The Department must comply with the specific data retention policies outlined by the Office of the Chief Information Officer (<https://www.sos.wa.gov/archives/recordsmanagement/state-agencies-records-retention-schedules.aspx>). For example (complete requirements can be found in the link provided):

| * 1. INVESTIGATIONS

The activity of investigating illness and disease. |
| --- |
| **DISPOSITION AUTHORITY NUMBER (DAN)** | **DESCRIPTION OF RECORDS** | **RETENTION AND****DISPOSITION ACTION** | **DESIGNATION** |
| 03-10-60572Rev. 2 | ***Communicable Disease Outbreak Investigations***Investigations and reports of unusual communicable disease outbreaks that involve large numbers of people, deaths, and new or unknown causes. Used for research and for comparative studies in the event of similar future outbreaks. | **Retain** for 10 years after case closed *then***Transfer** to Washington State Archives for appraisal and selective retention. | **ARCHIVAL****(Appraisal Required)**NON-ESSENTIALOPR |
| 95-06-55118Rev. 2 | ***Foodborne Illness Investigations***Records relating to foodborne illness investigations. May include copies of lab results, copies of epidemiology, hazard analysis critical control points, reports, correspondence, and questionnaires. | **Retain** for 6 years after case closed *then***Transfer** to Washington State Archives for permanent retention. | **ARCHIVAL****(Permanent Retention)**NON-ESSENTIALOPR |
| 94-08-54053Rev. 3 | ***Pesticide Exposure Investigations – All Other Investigations***Records related to pesticide related illness investigations. May include medical records, referrals from various agencies, correspondence, incident reports, records of conversations, Labor and Industry claim forms, and pesticide incident summary reports. | **Retain** for 6 years after case closed *then***Destroy**. | NON-ARCHIVALNON-ESSENTIALOPR |
| 12-12-68401Rev. 1 | ***Pesticide Exposure Investigations – Historically Significant Investigations***Records related to pesticide related illness investigations that *are unusual, result in death, involve the use of new or illegal products, are of public interest, or that involve a relatively large number of affected people*. May include medical records, referrals from various agencies, correspondence, incident reports, records of conversations, Labor and Industry claim forms, and pesticide incident summary reports. | **Retain** for 6 years after case closed *then***Transfer** to Washington State Archives for permanent retention. | **ARCHIVAL****(Permanent Retention)**NON-ESSENTIALOPR |
| 13-12-68478Rev. 0 | ***Shellfish Illness Investigation Summary Records***Summary records of shellfish related illnesses such as Vibrio Parahaemolyticus (Vp)and Norovirus.Includes, but is not limited to:* Shellfish Illness Log.
 | **Retain** until no longer needed for agency business *then***Transfer** to Washington State Archives for permanent retention. | **ARCHIVAL****(Permanent Retention)**NON-ESSENTIALOPR |
| 09-03-61966Rev. 2 | ***Shellfish Illness Investigations, Studies, Research Projects***Investigations of shellfish related illnesses such as Vibrio Parahaemolyticus (Vp)and Norovirus. May include documents such as minutes and agendas, surveys, samples, investigation files, progress reports, correspondence, research and background files, presentation materials, cost estimates, implementation plans and final reports. Used to improve public health and safety and identify shellfish illness trends.*Note: Vibrio Parahaemolyticus Outbreak Investigations are required by WAC 246-282-006.* | **Retain** for 30 years after end of project or investigation *then***Destroy**. | NON-ARCHIVALNON-ESSENTIALOPR |
| 12-12-68423Rev. 1 | ***Waterborne Disease Outbreak Investigations***Records relating to waterborne disease outbreak investigations. May include lab results, photographs, interviews, correspondence, and reports. Used for developing training events, research, and for comparative studies in the event of similar future outbreaks. | **Retain** for 6 years after case closed *then***Transfer** to Washington State Archives for permanent retention. | **ARCHIVAL****(Permanent Retention)**NON-ESSENTIALOPR |
| 06-05-61159Rev. 2 | ***Zoonotic Disease Case Investigations***Records related to zoonotic or vector-borne disease investigations. May include correspondence, copies of reports collected by local health department officials, records of conversations, photographs, maps, lab and testing results, and case summaries. | **Retain** for 6 years after case closed *then***Transfer** to Washington State Archives for permanent retention. | **ARCHIVAL****(Permanent Retention)**NON-ESSENTIALOPR |

**Section 5: Data Storage and Backup**

Data, System and Source Code Backup

Recovery Point Objectives (RPO) will be defined during the system risk assessment processes. Recovery Point Objectives identify the amount of data that can be lost after a major disruption to the system without severely impacting the recovery of operations.

Processes that meet or exceed the minimum standards for data and system backup, as defined in the DOH Backup Standards must be established and followed.

* + - 1. The processes must address media rotation, onsite storage, and offsite storage.
			2. Each division/program must establish procedures for the creation, maintenance, verification, and emergency use of back-up data.

Backups of current source code for critical systems must be backed up and available to restore applications after system failure.

* + - 1. Tests to restore services for various levels of system failure should be conducted at least annually for mission critical systems

**Information classified as confidential or restricted must be encrypted:**

When required by law.

* + - 1. All state and federal regulations shall be considered when determining when to encrypt. Some regulations are very specific as to when data must be encrypted.

During transmissions into or out of DOH networks.

* + - 1. Transmission across the SGN may be exempt in certain cases.
				1. All exemptions must be reviewed by the ITSO and documented in the IT Security Program

When the information resides or is at rest outside the DOH SGN internal production network. Examples include:

* + - 1. All DOH DMZ environments
				1. Information residing on a DOH SGN production DMZ **isolated from external** networks (e.g., the SGN) and external facing Web servers **is exempt from this requirement**.
			2. At a private entity location
			3. At the Consolidated Technical Services (CTS) or other external government entity.
				1. In certain cases, specific data sharing agreements and security controls may exempt this requirement. All exemptions must be reviewed by the ITSO and documented in the IT Security Program

When the information is stored in an area that is readily accessible by individuals who are not authorized to access the information. Examples include:

* + - 1. A desktop (workstation) computer hard drive
			2. A database or file server that does not meet DOH Physical Security Standards
			3. A shared database server that does not restrict access to authorized users based upon a need-to-know.
			4. A shared network location that does not limit access to authorized users with a need-to-know.

When the information is transmitted across an un-trusted network such as the Internet.

When the information is stored on mobile devices or removable media, such as laptops, Blackberries/smart phones, USB storage devices, CDs/DVDs.

* + - 1. Explicit written permission is required from the Data Owner or Data Steward prior to storing confidential or restricted information on a mobile device or removable media.

Additional encryption requirements may apply to information that is classified as restricted or is protected by certain state or federal regulations.

* + - 1. Use data classification criteria for guidance on what information should be classified as restricted.
			2. State and federal regulations governing medical or personal information often mandate stringent safeguards that drive encryption requirements.
			3. Data Stewards are responsible for understanding specific laws or regulations that apply to the information for which they have been assigned authority.

**Minimum encryption requirements:**

**Data transmissions**

* + - 1. Information classified as confidential or restricted require use of industry standard cryptographic protocols, such as SSL, SSH, HTTPS, or VPN for secure communications across un-trusted networks. 128 bit encryption or better is required.
				1. All VPN connections must be coordinated through the ITSO. For specific requirements regarding VPN technology see the [Access Security Standards](http://dohweb/dirm/Security/SecStnds/AccessSecurityStandards.doc) and the [Network Infrastructure Security Standards](file://DOHFLTUM01/Division/DIRM/Administration/ITSO/IT%20Security%20Standards/For%20CIO%20Approval/NetworkInfrastructureSecurityStandards.doc).
			2. In some instances confirmation of receipt or use of PKI authentication may be required for data transmissions.

**Data storage**

* + - 1. Cryptographic modules validated by NIST, which offer the following features are required:
				1. 256 bit encryption
				2. Securely generated keys
				3. Key features, such as Additional Encryption Key (ADK), Key reconstruction and key splitting, to ensure policy-defined access to data.
				4. Use of public key exchange algorithms

The specific encryption requirements for new or existing data collections will be identified and documented through [Visibility reporting](http://dohweb/dirm/prc/index.htm), [data classification](#Classification) and [IT Risk Management](http://dohweb/dirm/Security/SecStnds/ManagingITRisk.doc) processes.