# Initial Gap Analysis: Comparing Current DHS Privacy and Security Policies/Standards to the Privacy and Security Requirements Identified in 45 C.F.R. § 155.260

| | CFR | Policy # | DHS Policy | Technology Controls (documented standards) |
|---|---|---|---|---|
| **(a)** | ***Creation, collection, use and disclosure.*** | | | |
| (1) | Where the Exchange creates or collects personally identifiable information for the purposes of determining eligibility for enrollment in a qualified health plan; determining eligibility for other insurance affordability programs, as defined in 155.20; or determining eligibility for exemptions from the individual responsibility provisions in section 5000A of the Code, the Exchange may only use or disclose such personally identifiable information to the extent such information is necessary to carry out the functions described in §155.200 of this subpart. | 2.16 | 2.16 Requesting, Accessing, Using, or Disclosing Minimum Necessary Information<br><br>DHS employees must request, access, use, or disclose only the minimum amount of protected information necessary to provide services and benefits to clients, and to comply with applicable laws and DHS policies permitting disclosures.<br><br>DHS retains discretion to make its own minimum necessary determination when disclosing protected information. | • Role-based access controls<br>• 2-factor authentication<br>• Assignment of roles (given roles restricted to specific screens)<br>• Screen-lock/screen access controls<br>• Log-in/Password controls<br>• Datebase firewalls. |
| (2) | The Exchange may not create, collect, use, or disclose personally identifiable information while the Exchange is fulfilling its responsibilities in accordance with §155.200 of this subpart unless the creation, collection, use, or disclosure is consistent with this section. | 2.1 | **2.1 Rights of Individuals From Whom DHS Obtains Information**<br><br>Individuals from whom DHS collects confidential data, private data, and protected health information (referred to collectively as "protected information") have the right to have that information safeguarded, to comment on what it contains, to have reasonable access to it, and to know the circumstances under which it is being shared.<br><br>DHS will maintain policies and procedures concerning the rights of individuals from whom DHS collects protected information. DHS will provide ongoing training to its staff regarding the safeguarding of protected information and the rights of individuals regarding their protected | • Email encryption<br>• Encrypted file transfer<br>• Database firewalls<br>• TLS for transport<br>• Role-based access control<br>• Screen-lock/screen access controls |

| | | | | |
|---|---|---|---|---|
| | | | information.<br><br>**5.9 Encryption for Data Transport**<br><br>Private data, confidential data, or Protected Health Information (PHI) transported via a network or electronic communication resource that is not considered secure must be encrypted. | |
| (3) | The Exchange must establish and implement privacy and security standards that are consistent with the following principles: | | | |
| (i) | ***Individual access***. Individuals should be provided with a simple and timely means to access and obtain their personally identifiable health information in a readable form and format; | | **2.5 Right to Request Access to Their Information**<br><br>Generally, individuals about whom DHS collects private or confidential data, or protected health information (referred to collectively as "protected information") have a right to access their information. Under some circumstances, however, access may be denied.<br><br>**2.6 Right to Request Amendment of Client Information**<br><br>Individuals about whom DHS collects private and confidential data, and protected health information (collectively referred to as "protected information") have the right to request that their information be amended if they believe it is inaccurate or incomplete. | • Role-based access controls<br>• ADA compliance |
| (ii) | ***Correction***. Individuals should be provided with a timely means to dispute the accuracy or integrity of their personally identifiable health information and to have erroneous information corrected or to have a dispute documented if their requests are denied; | | **2.6 Right to Request Amendment of Client Information**<br><br>Individuals about whom DHS collects private and confidential data, and protected health information (collectively referred to as "protected information") have the right to request that their information be amended if they believe it is inaccurate or incomplete. | • Business and Technical requirements |

| | | | | |
|---|---|---|---|---|
| (iii) | ***Openness and transparency.*** There should be openness and transparency about policies, procedures, and technologies that directly affect individuals and/or their personally identifiable health information; | | **2.0 Guiding Principles**<br><br>In order to protect the privacy of individuals with whom DHS interacts, including clients, applicants, patients, licensees, and health care professionals, DHS will develop, adopt, adhere to, and periodically revise policies, standards, and procedures designed to reasonably safeguard the privacy of their information.<br><br>As appropriate, DHS will incorporate and adhere to standards and definitions outlined in the following state and federal laws, specifically, and, as applicable, in other state and federal laws affecting the privacy rights of individuals: Minnesota Government Data Practices Act, Minnesota Statutes Chapter 13; the Minnesota Medical Records Act, Minnesota Statues, Section 144.335; the federal Alcohol and Substance Abuse Treatment Records statutes, 42 USCS section 290dd-2 and 42 CFR section 2.1 to 2.67; and the privacy and security regulations of the Health Insurance Portability Accountability Act, 45 CFR Parts 160 and 164.<br><br>**2.2 Right to Receive Notice and Acknowledgement of Privacy Practices**<br><br>DHS will provide a "Notice of Privacy Practices" to individuals from whom DHS collects private or confidential data and protected health information (referred to collectively as "protected information"). This notice will explain how DHS uses protected information, and the individual's rights regarding DHS' use of the protected information. | • DHS policies are already posted on the public web site |
| (iv) | ***Individual choice****.* Individuals should be provided a reasonable opportunity and capability to make informed decisions about the collection, use, and disclosure of their personally identifiable health information; | | **2.3 Right to Request Restrictions of Uses and Disclosures of Protected Health Information**<br><br>Individuals about whom DHS collects *protected health information* may request that DHS restrict the use or sharing of their protected health | • Business requirements |

| | | | | |
|---|---|---|---|---|
| | | | information with others outside of DHS.<br><br>DHS will apply criteria as required by involved statutes and rules in determining when to grant a request to restrict disclosures. DHS reserves the right to deny requests if they are found to be contrary to the law, impractical to implement, or otherwise unreasonable.<br><br>Notes: This policy applies only to protected health information of adults and certain types of private data about minors. This policy does NOT generally apply to other types of private or confidential information. | |
| (v) | ***Collection, use, and disclosure limitations.*** Personally identifiable health information should be created, collected, used, and/or disclosed only to the extent necessary to accomplish a specified purpose(s) and never to discriminate inappropriately; | | **2.3 Right to Request Restrictions of Uses and Disclosures of Protected Health Information**<br><br>Individuals about whom DHS collects *protected health information* may request that DHS restrict the use or sharing of their protected health information with others outside of DHS.<br><br>DHS will apply criteria as required by involved statutes and rules in determining when to grant a request to restrict disclosures. DHS reserves the right to deny requests if they are found to be contrary to the law, impractical to implement, or otherwise unreasonable.<br><br>Notes: This policy applies only to protected health information of adults and certain types of private data about minors. This policy does NOT generally apply to other types of private or confidential information. | • DHS currently prohibits browsing data and has some controls to protect family/friends/interesting case browsing.<br>• Business rules must be articulated |
| (vi) | ***Data quality and integrity.*** Persons and entities should take reasonable steps to ensure that personally identifiable health information is complete, accurate, and up-to-date to the extent necessary for the person's or **entity**'s intended purposes and has not been altered or destroyed in an unauthorized manner; | | **2.5 Right to Request Access to Their Information**<br><br>Generally, individuals about whom DHS collects private or confidential data, or protected health information (referred to collectively as "protected information") have a right to access their information. Under some circumstances, | This needs clarification |

| | | | | |
|---|---|---|---|---|
| | | | however, access may be denied. | |
| (vii) | ***Safeguards.*** Personally identifiable health information should be protected with reasonable operational, administrative, technical, and physical safeguards to ensure its confidentiality, integrity, and availability and to prevent unauthorized or inappropriate access, use, or disclosure; and, | | **Information Policy** details operational, administrative and technical safeguards throughout policy, **Chapters**<br>**3. Securing Data**<br>**4. System Security**<br>**5. Securing Communications** | • Addressed with the entire technical and security architecture:<br>  • SLM<br>  • Vulnerability management<br>  • Segmentation of data<br>  • Encryption<br>  • Logging<br>• Security overview from ZOCA may be helpful |
| (viii) | ***Accountability.*** These principles should be implemented, and adherence assured, through appropriate monitoring and other means and methods should be in place to report and mitigate non-adherence and breaches. | | **1. Roles and Responsibilities**<br>1.1 Management Roles and Responsibilities<br>The responsibility for the creation and enforcement of information policies belongs to the management of DHS at all its levels. Various positions have specific responsibilities to protect the agency's information assets through diligent decisions and actions that must be taken.<br><br>1.2 Privileged Accounts Roles and Responsibilities<br>Privileged accounts, also known as elevated account privileges, must be restricted to those users directly responsible for multi-user system, network or application management or security, where such privileges are required for assigned job duties.<br><br>The supervisor of a user needing a privileged account must document the request for the privileged account and specify the purpose for the privileged account.<br><br>Each user requiring elevated privileges must be assigned a unique privileged user account.<br><br>The user of a privileged account must not grant any privileges to any other user without first obtaining the appropriate authorization for that user and those privileges. The user of a privileged account must document and report to their technical manager the granting of any additional privileges or privileged accounts to themselves. | ▪ Logging and monitoring<br>▪ Incident Management<br>▪ Authentication |

| | | | | |
|---|---|---|---|---|
| | | | A privileged account must only be used when a business need exists for the use of the privileged account to accomplish the activity or operation.<br><br>Service accounts and shared accounts are not included in this policy.<br><br>1.3 User Responsibilities<br>Users must:<br>• Use resources only for the purposes specified by DHS.<br>• Comply with controls established by DHS or state and federal law.<br>• Prevent unauthorized disclosure of protected information.<br>• Prevent unauthorized disclosure and/or destruction of audit trails.<br>• Maintain current knowledge on Information policies and standards<br>• Set a security question for password resets.<br>Direct questions about the appropriate handling of a specific type of information to one's supervisor, DHS Office of Information Security, or to the DHS Privacy Official.<br><br>By virtue of accepting access to DHS information assets, users agree to comply with DHS Information Policies and Standards. The use of technology or government data not explicitly permitted by Information Policies and Standards is prohibited.<br><br>Users must protect DHS information resources from unauthorized activities including disclosure, modification, copying, deletion and usage. Users must not change, remove or bypass security or other controls in information resources.<br><br>**4.7 Security Event Logging**<br>Logs must be created and maintained to fulfill auditing requirements and to manage threats against DHS computer and electronic communication resources. Any information recorded in a log or derived from a log must be handled as security information. | |

| | | | | |
|---|---|---|---|---|
| | | | **6.5 Reporting of Suspected or Known Security or Privacy Incidents**<br>All users must report suspected or known security and privacy incidents or breaches.<br><br>Incidents and breaches must be reported to the Incident Determination Team (IDT).<br><br>Users are protected against retaliation or interference when making a report in good faith.<br><br>Privacy incident/breach reports and accompanying documentation are classified as non-public/private data. Security incident/breach reports and accompanying documentation are classified as security information.<br><br>**6.6 Responding To and Handling Suspected or Known Security and Privacy Incidents and Breaches**<br>Designated staff must respond to all identified or reported security and privacy incidents and breaches. Responses must occur within the standard time frame based on the severity level of the incident or breach.<br><br>Incident and breach responses must mitigate, to the extent practical, harmful effects of known security and privacy incidents with an emphasis on containment, notification, eradication and recovery. Mitigation may occur within the business area or agency-wide based on severity of the incident or breach as determined by the Incident Determination Team in consultation with the business area management.<br><br>**8.1 Information Policy Compliance and Consequences**<br>All Department of Human Services (DHS) users, including employees, volunteers and contractors, who have rights to access or modify DHS information in any media, or who use DHS computers, business applications or electronic | |

| | | | | |
|---|---|---|---|---|
| | | | communication resources, must comply with DHS Information Policy, the federal Health Insurance Portability and Accountability Act (HIPAA), the Minnesota Government Data Practices Act , the Minnesota Medical Records Act and all other laws or rules governing the protection of data. Failure to comply is grounds for sanction and/or disciplinary action up to and including termination of employment, cancellation of contract and/or loss of resource privileges. Failure to comply may also result in notification to law enforcement officials and regulatory, accreditation and licensure organizations. | |
| (4) | For the purposes of implementing the principle described in paragraph (a)(3)(vii) of this section, the Exchange must establish and implement operational, technical, administrative and physical safeguards that are consistent with any applicable laws (including this section) to ensure— | | | |
| (i) | The confidentiality, integrity, and availability of personally identifiable information created, collected, used, and/or disclosed by the Exchange; | | **Information Policy** details operational, administrative and technical safeguards throughout policy, **Chapters**<br>**3. Securing Data**<br>**4. System Security**<br>**5. Securing Communications**<br>**6. Security Management** | • Addressed with the entire technical and security architecture:<br>▪ SLM<br>▪ Vulnerability management<br>▪ Segmentation of data<br>▪ Encryption<br>▪ Logging<br>• Security overview from ZOCA may be helpful |
| (ii) | Personally identifiable information is only used by or disclosed to those authorized to receive or view it; | | **2.16 Requesting, Accessing, Using, or Disclosing Minimum Necessary Information**<br><br>DHS employees must request, access, use, or disclose only the minimum amount of protected information necessary to provide services and benefits to clients, and to comply with applicable laws and DHS policies permitting disclosures.<br><br>DHS retains discretion to make its own minimum necessary determination when disclosing protected information. | • Role-based access controls<br>• 2-factor authentication<br>• Assignment of roles (given roles restricted to specific screens)<br>• Screen-lock/screen access controls<br>• Log-in/Password controls<br>• Datebase firewalls. |
| (iii) | Return information, as such term is defined by section 6103(b)(2) of the Code, is kept confidential under section | | | |

| | | | | |
|---|---|---|---|---|
| | 6103 of the Code; | | | |
| (iv) | Personally identifiable information is protected against any reasonably anticipated threats or hazards to the confidentiality, integrity, and availability of such information; | | Risk assessments and risk management<br><br>**6.9 Security Risk Assessment**<br>Periodic risk assessments must be performed on all critical business resources. All DHS computer or electronic communication resources are subject to a risk assessment at any time. All information gathered in a risk assessment must be handled as security information.<br><br>Any staff discovering a substantial threat during a risk assessment must report the threat to the Information Security team. | • Vulnerability management<br>• Incident management<br>• COOPs<br>• BCP |
| (v) | Personally identifiable information is protected against any reasonably anticipated uses or disclosures of such information that are not permitted or required by law; and | | **2.15 Verifying the Identity and Legal Authority of the Person Requesting or Receiving Protected Information**<br><br>All DHS personnel must verify the identity and/or legal authority of an individual who requests or is allowed access to protected information before providing access to that information.<br><br>**2.16 Requesting, Accessing, Using, or Disclosing Minimum Necessary Information**<br><br>DHS employees must request, access, use, or disclose only the minimum amount of protected information necessary to provide services and benefits to clients, and to comply with applicable laws and DHS policies permitting disclosures.<br><br>DHS retains discretion to make its own minimum necessary determination when disclosing protected information.<br><br>**2.17 Obtaining authorization for use and disclosure of protected information**<br><br>When required by law, DHS must obtain authorization before it can disclose an individual's protected information.<br><br>**2.18 Accounting for Disclosures of Protected Health Information** | • Email encryption<br>• Encrypted file transfer<br>• Database firewalls<br>• TLS for transport<br>• Role-based access control<br>• Screen-lock/screen access controls |

| | | | | |
|---|---|---|---|---|
| | | | DHS staff must maintain a record and be able to account for certain types disclosures of an individual's protected health information. This policy applies only to protected health information and health records; it does NOT apply to other types of information that may be private or confidential.<br><br>Note: Special procedures apply for health records maintained by State Operated Services<br><br>**5.9 Encryption for Data Transport**<br>Private data, confidential data, or Protected Health Information (PHI) transported via a network or electronic communication resource that is not considered secure must be encrypted. | |
| (vi) | Personally identifiable information is securely destroyed or disposed of in an appropriate and reasonable manner and in accordance with retention schedules; | | **2.22 Recycling, Disposal, & Destruction of Protected Information**<br>When protected information is no longer needed it must be securely recycled or destroyed using procedures approved by the Director of Management Services and the Chief Information Security Officer.<br><br>All unneeded printed copies of protected information that are generated in the course of copying, printing, or otherwise handling such information must be disposed of or destroyed.<br><br>Portable computer storage media, which has been used to record protected information, must not leave DHS possession until it has been electronically or physically destroyed according to the standards set forth by the Director of Management Services and the Chief Information Security Officer.<br><br>**3.10 Records Managed by Schedule**<br>All government records created and/or maintained by DHS employees, staff and contractors must be managed according to the DHS general records retention schedule or other approved records retention schedule.<br><br>Divisions and business units that wish to create | 2.22.1 DHS-owned Computer and Electronic Media Sanitization<br>The sale, transfer, or disposal of DHS-owned computers, computer peripherals, servers, network infrastructure and other IT devices can create information security risks for DHS. These risks are related to potential violation of software license agreements or unauthorized release of protected information from DHS-owned equipment and electronic media.<br><br>Before a DHS-owned computer system or IT device is sold, transferred, or otherwise disposed of, all protected information (includes security information) programs or data files on any storage media must be completely wiped or otherwise made unreadable.<br><br>Memory components should also be sanitized before disposal or release. Memory components reside on boards, modules, and sub-assemblies. A board can be a module, or may consist of several modules and sub-assemblies.<br><br>**2.22.2 Physical Disposal of Protected Information**<br>Proper disposal of protected information in the following formats must be done on a daily basis and according to record retention policies.<br><br>Also see table below. |

| | | | | |
|---|---|---|---|---|
| | | | records retention schedules that directly address specific types of records created and maintained within their area must have those retention schedules approved by the state's records disposition panel. | • Paper and other types of hard copies must be put in secured bins designated for paper recycling, or shredded using an approved paper shredder.<br>• Photographic and imaging technology or transparencies must be shredded using an approved shredder or put in secured bins designated for destruction. These materials are not recyclable.<br>• Audio or video recordings must be put in secured bins designated for destruction.<br>• Portable computer storage media must be put in secured bins designated for destruction.<br>• Other types of magnetic storage (e.g. hard drives) that do not fall under portable computer storage media or not meant to be destroyed must be submitted to DHS Desktop Services. All contents of the magnetic storage device will be destroyed, while preserving the device for reuse.<br>Each business area will determine the appropriate methods for disposing of protected information used or handled in their area.<br><br>If a secured bin for destruction is not available in a DHS location, box the items and send them using an authorized person or service to 444 Lafayette, attn: Dock Supervisor, St. Paul, MN 55101.<br><br>**2.22.3 Disposal of Protected Information While Away from DHS Facilities**<br>While working away from DHS facilities, protected information must be securely discarded when no longer needed.<br><br>Paper copies, photographic material or transparencies must be either shredded to .25 inches shred size or smaller, or returned to DHS for proper disposition.<br><br>Types of magnetic storage or devices (e.g. hard drives) that are not meant to be destroyed must be returned to a DHS facility and submitted to DHS Desktop Services. All contents of the magnetic storage device will be destroyed.<br><br>All materials may be returned to a DHS facility and placed in secured bins designated for destruction or recycling if appropriate. |

| | | | | |
|---|---|---|---|---|
| | | | | If a secured bin for destruction is not available in a DHS location, box and seal the items and send them using an authorized person or service to 444 Lafayette, attn: Dock Supervisor. |
| (5) | The Exchange must monitor, periodically assess, and update the security controls and related system risks to ensure the continued effectiveness of those controls. | | **6.9 Security Risk Assessment**<br>Periodic risk assessments must be performed on all critical business resources. All DHS computer or electronic communication resources are subject to a risk assessment at any time. All information gathered in a risk assessment must be handled as security information.<br><br>Any staff discovering a substantial threat during a risk assessment must report the threat to the Information Security team.<br>6.11 Security Monitoring Tools<br>All servers, devices and network infrastructure are subject to approved and appropriate security control and monitoring tools. All servers, devices and network infrastructure must be scanned and monitored for security purposes.<br><br>**4.14 Maintaining Business Technology Resources**<br>DHS network, desktop, and telecomm hardware and software must be evaluated and updated according to schedules set forth in the standards. Updates to computers and communication resources must support efficiency and continuity of delivering DHS services, and ensure security of DHS assets.<br><br>**5.15 Patch Management**<br>DHS computer and electronic communication resources* in production must be maintained to appropriate patch levels determined by technical managers / system managers, and line managers / business area managers. Patches must be evaluated, documented and deployed as appropriate according to the schedule and process set forth in the standards. The CISO may require the implementation of appropriate critical security patches. | • Vulnerability management<br>• Patching Management<br>  ○ 5.15.1 Patch Management Process<br>• Monitoring<br>• Antivirus controls |
| (6) | The Exchange must develop and utilize | | **5.9 Encryption for Data Transport** | **5.9.1 Data Encryption Standard** |

| | | | | |
|---|---|---|---|---|
| | secure electronic interfaces when sharing personally identifiable information electronically. | | Private data, confidential data, or Protected Health Information (PHI) transported via a network or electronic communication resource that is not considered secure must be encrypted.<br>5.12 Protecting Electronic Transaction Data<br>Business processes that generate or exchange Electronic Transactions must have adequate protective measures.<br><br>Electronic Transactions and their protective measures must be evaluated periodically.<br><br>**5.13 Administration of Electronic Transactions**<br>Appropriate Electronic Transaction format and content standards (e.g. HIPAA Electronic Data Transaction Standards and Code Sets) must be implemented and maintained.<br><br>Incoming and outgoing (i.e. to and from DHS) Electronic Transactions must be auditable.<br><br>Electronic Transactions exchanged with trading partners must be certified. | E-Mail<br><br>E-mail will be encrypted based on the e-mail address of the recipient. This means that in order to encrypt e-mail, the recipient must have an existing encryption registration.<br><br>All E-mail that requires encryption, exiting the DHS Mail System, will be sent through the TFS Encryption Server. Only e-mail clients that support PGP or S/MIME will be supported. The business partner will be responsible for acquiring and supporting their hardware, software, and certificates. For business partners that receive/send a lot of encrypted e-mail from DHS, it will be recommended that the business partner acquire a TFS Encryption Server also. This will allow for server-to-server encryption.<br><br>File Transfer<br><br>Trading Partners that wish to transfer files will need to be registered in advance.<br><br>All files that need to be encrypted, to and from the IBM mainframe, will use the BlueZone product or the IBM ZOS Ftp.<br><br>Encrypted files that go to and from the DHS network will use the Secure File Transfer application.<br><br>Only secure ftp clients that use https or follow the RFC 2228, secure ftp protocols are allowed. The supported clients are Valicert's secure file transport client.<br><br>Depending on the application requirements (frequency of transport, number of files sent to/received from the business partner) the Secure FTP manager will determine whether there will be server side only certificates or both server and client side certificates. |
| **(b)** | ***Application to non-Exchange entities.*** Except for tax return information, which is governed by section 6103 of the Code, when collection, use or disclosure is not otherwise required by law, an Exchange must require the same or more stringent | | | |

| | | | | |
|---|---|---|---|---|
| | privacy and security standards (as §155.260(a)) as a condition of contract or agreement with individuals or entities, such as Navigators, agents, and brokers, that: | | | |
| (1) | Gain access to personally identifiable information submitted to an Exchange; or | | TBD – defining roles<br>2.0 applies | |
| (2) | Collect, use or disclose personally identifiable information gathered directly from applicants, qualified individuals, or enrollees while that individual or **entity** is performing the functions outlined in the agreement with the Exchange. | | TBD – defining roles<br>2.0 applies | |
| (c) | ***Workforce compliance.*** The Exchange must ensure its workforce complies with the policies and procedures developed and implemented by the Exchange to comply with this section. | | **6.1 Privacy and Security Training**<br>All staff must be annually trained on information privacy and security. A centralized record of staff participation in these training areas must be maintained.<br><br>**8.1 Information Policy Compliance and Consequences**<br>All Department of Human Services (DHS) users, including employees, volunteers and contractors, who have rights to access or modify DHS information in any media, or who use DHS computers, business applications or electronic communication resources, must comply with DHS Information Policy, the federal Health Insurance Portability and Accountability Act (HIPAA), the Minnesota Government Data Practices Act , the Minnesota Medical Records Act and all other laws or rules governing the protection of data. Failure to comply is grounds for sanction and/or disciplinary action up to and including termination of employment, cancellation of contract and/or loss of resource privileges. Failure to comply may also result in notification to law enforcement officials and regulatory, accreditation and licensure organizations. | **6.1.1 Privacy Training standard**<br>The privacy computer based training is available as "Protecting Information Privacy." Alternative or adaptive training must be maintained to meet ADA requirements and appropriateness for certain job responsibilities.<br><br>The computer-based training provides a central record of those completing the training. The central record is maintained using Pathlore. Those supervisors with staff who are taking alternative or adaptive training must manually report participation/ results to the central record.<br><br>New staff must complete privacy training within 10 business days of their first day of employment.<br><br>**6.1.2 Security Training standard**<br>The security computer based training is available as "Putting Security into Action." Alternative or adaptive training must be maintained to meet ADA requirements and appropriateness for certain job responsibilities.<br><br>The computer-based training provides a central record of those completing the training. The central record is maintained using Pathlore. Those supervisors with staff who are taking alternative or adaptive training must manually report participation/results to the central record.<br><br>New staff must complete security training within 10 business days of their first day of employment |

| | | | | |
|---|---|---|---|---|
| | | | | **6.1.3 DHS Privacy and Security Training for non-DHS Staff**<br>Non-employees who do not login to DHS systems, and yet have physical access to secured DHS facilities, must receive either annual training on DHS Privacy and Security, and/or sign a confidentiality agreement with DHS. Non-employees include, but are not limited to, other state agency employees, vendors, repair people, service workers, and county workers. Refer to the table below for criteria and requirements.<br><br>• Development of user/citizen-friendly FAQs<br>• Recertifications<br>• System-based oath/acknowledgment |
| (d) | ***Written policies and procedures.*** Policies and procedures regarding the collection, use, and disclosure of personally identifiable information must, at minimum: | | | |
| (1) | Be in writing, and available to the Secretary of HHS upon request; and | | | |
| (2) | Identify applicable law governing collection, use, and disclosure of personally identifiable information. | | Consumer Health Technologies HIX System and Data Security prevailing laws, rules, guidelines and regulations-3 | Articulated in Preamble to Information Policy |
| (e) | ***Data sharing.*** Data matching and sharing arrangements that facilitate the sharing of personally identifiable information between the Exchange and agencies administering Medicaid, CHIP or the BHP for the exchange of eligibility information must: | | | |
| (1) | Meet any applicable requirements described in this section; | | yes | |
| (2) | Meet any applicable requirements described in section 1413(c)(1) and (c)(2) of the Affordable Care Act; | | yes | |
| (3) | Be equal to or more stringent than the requirements for Medicaid programs under section 1942 of the Act; and | | Yes, since we already have Medicaid | |
| (4) | For those matching agreements that meet the definition of “matching program” under 5 U.S.C. 552a(a)(8), comply with 5 U.S.C. 552a(o). | | | |

| | | | | |
|---|---|---|---|---|
| (f) | *Compliance with the Code.* Return information, as defined in section 6103(b)(2) of the Code, must be kept confidential and disclosed, used, and maintained only in accordance with section 6103 of the Code. | | application/attestation | |
| (g) | ***Improper use and disclosure of information****.* Any person who knowingly and willfully uses or discloses information in violation of section 1411(g) of the Affordable Care Act will be subject to a civil penalty of not more than $25,000 per person or **entity**, per use or disclosure, in addition to other penalties that may be prescribed by law. | | Disclosure training development | |