Oregon HISPIC Project
Effective Security Practices
February 20, 2007 – Version 4

The Oregon HISPIC Team and stakeholders participating in the Oregon HISPIC Project have identified the following effective and appropriate security practices as defined by the HIPAA Security Rule and what is considered by security professionals to be appropriate security practices. Some of the practices listed may be more stringent than what HIPAA requires. As with most states, Oregon continues its efforts to reasonably ensure such practices are uniformly followed by caretakers of individually identifiable health information.

The noted practices address the security requirements identified in the nine domains. Rather than developing a redundant list, the appropriate domain is listed following each practice where appropriate. Some of the effective security practices listed were not identified in the nine domains but are effective and appropriate given HIPAA requirements, state legal requirements and what is considered appropriate security practice.

Administrative Practices/Standards

Security Management::

- Risk Analysis – A risk analysis should be conducted periodically and when any major system or business changes occur. Such a risk assessment should be conducted within an organization and across organizations wherever a health information exchange network has been established.
- Risk Management – A sound risk management program needs to be established that manages the risks identified during the risk analysis. Risk management should be addressed within an organization, either by a collaborative team or neutral third party and by the governing body of a health information exchange. The exchange of information is not necessary to conduct an appropriate risk management program but needs to be considered when a larger entity or collaborative is responsible for the management of shared information.
- Sanction Policy – Sanctions policies that are administered uniformly need to be established and followed. Sanctions need to be no less stringent for management or executives than it is for other members of the workforce. Sanctions also need to be established and enforced when multiple organizations enter into a common data sharing agreement. This should include termination of access up to and including criminal/civil prosecution.
- Information System Activity Review – Technical systems need to generate audit trails that can be reviewed later to reasonably ensure security practices are followed and reasonably protect against new vulnerabilities/threats. This includes internal systems monitoring and reporting and should include clearly defined, understood and regularly

review reports addressing interaction between multiple organizations where such exchange networks have been established.

- Security Officer – An individual needs to be appointed to act as the security officer. This person should have the appropriate authority that matches responsibility and should not report to the CIO or IT. Also, a neutral third party or collaborative cross-organizational team needs to be established to perform the same functions a security officer would perform across a health interchange involving multiple organizations. If a third party is selected, that third party should not be employed by or significantly controlled by any single organization that is a member of such a collaborative.

Workforce Security:

- Authorization and/or Supervision – Process/policies need to be implemented that provide for appropriate workforce supervision and authorization management when managing access to confidential data. This includes the implementation of appropriate system/application access controls and includes implementation of an authorization/supervision control structure across multiple organizations involved in a health interchange. Such authorization/supervision responsibilities should be controlled by a collaborative team or neutral third party with sufficient knowledge of security, legal and contractual (negotiated contracts between participating organizations) related to the established health interchange.
- Termination Procedures – Policies/procedures need to be implemented that ensure workforce access to confidential information is terminated when the workforce member is terminated. Access termination needs to be immediate when a workforce member is involuntarily terminated (physical, technical and remote). Such termination policies/procedures need to be implemented and closely followed by member organizations who are participating in a health exchange network. Close monitoring is necessary if multiple organizations are involved to reasonably ensure access to confidential information is terminated timely.
- Access Establishment and Modification – Policies/procedures need to be implemented that outline how access to confidential information is granted and modified to meet minimum necessary requirements (within an organization and between organizations). .
- Log-in Monitoring – An audit trail needs to be created that records when a workforce member logs on to the network or a software application and that audit trail needs to be periodically reviewed (may be a random audit). This includes monitoring within an organization and by a collaborative team or neutral third party where a health information exchange has been established between multiple organizations.

- Authentication Management – Policies/procedures need to be implemented that assist in managing proper password management (i.e., creation, periodic changes, etc.) for those organizations using single factor authentication. This means the operating system and software applications need to accommodate the use of a password that is unique to each user/workforce member. It should be noted that the financial industry is moving towards two factor authentication and it is advisable that healthcare or related organizations also plan to move to two factor authentication given passwords do not represent the most secure solution to authentication management.

  Also, if multi-factor authentication is used (such as smart cards and/or biometrics in addition to passwords), policies, procedures and practices need to be implemented to manage issuance, deactivation upon termination, etc. of authentication mechanisms over and above the use of a password. In the case of a health interchange, common authentication methodologies need to be established, agreed to by all participating organizations and enforced by each participating organization and across organizations. Interface applications need to be implemented to enforce proper authentication management (e.g., require change of passwords every 60 to 90 days, enforcement of strong passwords, appropriate credential management such as with smart cards or security tokens, etc.).

Security Awareness and Training:

- The full workforce of individual organizations and, where established workforce members of organizations participating in a health information exchange need to be provided security awareness training and training on security policies/ procedures and training needs to be on-going rather than a one-time event. In the case of a health information exchange, such security training related to the use of the health information exchange needs to be collaboratively developed, include the same content and administered in the same manner across all participating organizations.

Security Incident Procedures:

- Response and Reporting – Policies/procedures need to be implemented that define actions to be taken in the event of a security incident. This means audit trails need to be present to assist in investigating security incidents. This also means a security response team needs to be formed and trained before any security incidents occur. If a health information exchange has been established, a collaborative team or neutral third party needs to be appointed with appropriate authority to act as the exchange's security incident response team

Contingency Plan:

- Data Backup Plan – Confidential and business critical data needs to be backed up on a regular basis and stored off-site (not at an employee's home). Also, data recovery from backup medium needs to be tested periodically. Backed up date needs to be readily available in the event of a disaster, data corruption, etc. If a health information exchange includes the development of a large repository to centrally locate data (versus a distributed network), appropriate data backup and recovery plans need to be developed and managed to reasonably ensure centrally stored data can be recovered in the event of a disaster, data corruption, etc. Also, standard back up and recovery processes should be established and adhered to by member organizations if data is stored in a distributed network. This would be in addition to individual organizational requirements to implement and manage appropriate data back up and recovery policies, procedures and practices.
- Disaster Recovery Plan – Disaster recovery plans (DRP) need to be developed that clearly outlines how critical data is to be recovered in the event of a disaster. Plans need to be thorough and periodically tested and need to involve accommodating business, physical and technical requirements. Also, plans need to be updated on a periodic basis or whenever any significant system, business or staffing changes occur. Priority will be given to recovering mission critical data first. This includes the development, regular updates and testing of a DRP for individual organizations and for health information exchange networks (especially for networks where data is stored centrally).
- Emergency Mode Operation – Plans need to be implemented that allow access to mission critical data in the event of a disaster and while operating in an emergency mode. This also means allowances need to be made to accommodate access to mission critical data in the event of an emergency or when the authorized user is not available and access to the data is critical to continued operation. Emergency mode operation plans need to be implemented and managed for any health information exchange network. This is true for a distributed or a centralized network.

<u>Evaluation</u>:

- Periodic technical and non-technical evaluations need to be conducted to reasonably ensure the organization or organizations participating in a health information exchange network are maintaining a sound security program (inter and intra-organization). In the case of a multi-organizational network, such evaluations should be conducted by a collaborative team or a neutral third party.
- An appropriate audit program with criteria based on risks identified during the risk analysis, existing policies and procedures, etc. needs to be developed and implemented. Full organizational audits need to be conducted periodically or whenever any major system or business

changes occur. Also, more frequent targeted audits should be conducted on systems where sensitive data is stored, accessed, created, modified and destroyed. The same is true for multiple organizations participating in a health information exchange network. The audit criteria will likely differ somewhat from the criteria established for individual organizations but should address any cross-organizational risks identified, appropriate access control management, data integrity checks, adherence to appropriate data transmission standards, etc.

Business Associate Contracts and Other Arrangement:

- Written Contract or Other Arrangement – Organizations need to enter into written contracts with entities outside the organization with access to the organization's confidential information and perform business activities for the organization. Also, organizations need to enter into common contracts between participants in a health information exchange network and should outline responsibilities (management, authorization controls, sanctions for contract non-compliance, etc.) and agreed upon standards for security and privacy. (Domains 7 and 9.)

Physical Practices/Standards

Facility Access Controls:

- Facility Security Plan – A facility security plan needs to be developed, implemented and maintained. This includes installation of alarms where needed, fire suppression equipment maintenance and proper location, etc. An additional facility security plan needs to be developed to address any physical location where health information data is stored. This would include the storage of data associated with a health information exchange.
- Control and Validation Procedures – Policies/procedures need to be implemented that govern access management to the facility (i.e., key management, key card management, etc.). This includes managing access to the whole facility as well as areas designated as restricted within the facility. Additionally, control and validation procedures need to be developed, implemented and properly managed to address access to any physical location where data from a centralized health information exchange is stored.
- Maintenance Records – Organizations need to implement policies/procedures that accommodate maintenance of records when hardware, doors, locks, etc. are maintained. Additionally, maintenance records need to be maintained and properly monitored to address access to any physical location where data from a centralized health information exchange is stored.

Workstation Use & Security::

- Policies/practices need to be implemented that govern workstation or class of workstation use, physical location, etc. This means hardware and software accessible on workstations need to accommodate appropriate data protection and minimum necessary access. This also includes implementing controls so, if it is the organization's policy, confidential data cannot be downloaded onto jump drives, flash drives, CD-ROMs, etc. Scalable workstation use, location, etc. policies/procedures need to be established and adhered to by organizations participating in a health information exchange network primarily for devices with access to the established network.
- Policies/practices need to be implemented that accommodate the physical security of workstations used to access confidential or mission critical data. This means adequately protecting workstations (especially portable workstations) from theft, inappropriate access, inappropriate viewing of data displayed on screens, etc. Scalable policies, procedures and practices to reasonably ensure the physical security of workstations use by member organizations of a health information exchange network for devices with access to the established network. This would especially include agreed upon appropriate controls of portable workstations and like devices such as laptops, hand-held computers, smart phones, etc.

Device and Media Controls:

- Disposal – Proper practices need to be implemented that accommodates secure disposal of electronic media and hardware when no longer needed or usable. This includes complete destruction of any confidential information stored on the electronic media or hardware. This may include shredding CD & DVD ROMs, degaussing hard drives (use of a magnetic), dual formatting of flash or jump drives, etc. Common agreed upon disposal practices need to be implemented and followed by organizations participating in a health information exchange network, especially for media used to store data that is exchanged on the network and is not individually "owned" by individual participating organizations.
- Media Re-use – Proper practices need to be implemented that provides for the proper destruction/erasure of confidential information stored on electronic media or hardware when the media or hardware will no longer be used to store confidential information and will be used in other areas of the organization. Common agreed upon media re-use practices need to be implemented and followed by organizations participating in a health information exchange network, especially for media used to store confidential data that is exchanged on the network and is not individually "owned" by individual participating organizations.
- Accountability – Policies/procedures need to be implemented that record movement of electronic media and/or hardware and individuals authorized

to make such moves. Also, all media should be owned by the organization and workforce members prohibited from using their own personal media. Accountability standards and associated audit practices need to be developed, implemented and followed by organizations participating in a health information exchange network, especially for devices and media used to store confidential data and "owned" by the network. All media that is commonly used should be "owned" by the general collaborative or where appropriate, individual participating organizations. It should never be owned by an individual (versus an entity or organization).

Organizations need to move towards the use of technology and existing functionality in applications/software already in use (e.g., Microsoft Office, Adobe, etc.) that controls the use of the data (e.g., allows read only, does not allow printing, does not allow forwarding or downloading to another device, etc.). While EHR functionality has not necessarily advanced to that point, such controls can be established using other document or data management programs currently in use.

- Data Backup and Storage – An exact copy of confidential data stored on hardware to be moved should be made before the hardware is moved (inter and intra-organization).

Technical Safeguards

Access Control:

- Unique User Identification – Users need to be assigned unique logon identification and that unique login information needs to be stored in audit logs when that user creates, modifies, destroys or, in some cases, accesses confidential information. This includes within an organization and for users accessing data stored or used by a health information exchange network. The unique user identification assigned to users of the network need to be standardized and issued by a collaborative team or neutral third party when a new user is granted access to the network.
- Emergency Access Procedure – Organizations need to reasonably ensure access to confidential or mission critical information in the event of an emergency. This is true within and between organizations. When a health information exchange network is established, policies, procedures and practices need to be established to accommodate prompt access to data in the event of an emergency; such emergency access is monitored and periodically audited. The authority of the individual or individuals authorized to allow emergency access needs to be defined. Also, a set time period should be established during which emergency access is allowed. Emergency access should not be open ended.

- Automatic Logoff – Technical processes (such as those available using the Windows operating system) need to be activated so a user's access is automatically terminate after a period of inactivity. Exceptions may be made under certain circumstances such as in the emergency department but any exceptions need to be clearly documented and risk mitigation processes identified. Commonly agreed upon automatic logoff practices need to be implemented and followed by all organizations who are members of a health information exchange network.
- Encryption and Decryption – Proper technical processes need to be implemented to encrypt and decrypt confidential information transmitted over an open network (the Internet). This includes e-mail, web sites, FTP, VPN, etc. The minimum level of encryption needs to be at least 128 bit. Common encryption/decryption practices need to be established, implemented and followed for confidential information flowing across a health information exchange network.
- Send and Receive Interface Protections – Appropriate safeguards need to be implemented (such as firewalls, additional methods of authentication, etc.) to protect that data as it leaves a sender and as it arrives at the recipient site. Also, when confidential data passes through a third party or passes through a centrally managed database (centralized health information exchange networks), additional appropriate safeguards need to be implemented and managed to protect data as it travels through multiple data exchange points in transit between sender and receiver or between sender and any centralized repository.
- Remote Access – Appropriate safeguards need to be implemented to reasonably ensure any workforce member with remote access has implemented appropriate security controls at the site of remote access and adheres to the security policies, procedures and practices of the organization. Because remote access can create a significant security risk, organizations who are members of health information exchange network need to determine if remote access will be allowed and, if so, implement appropriate commonly agreed upon safeguards to protect data exchanged or accessed remotely.
- Wireless Access – As with other network configurations, wireless networks need to be adequately protected with appropriate security safeguards implemented to prevent inappropriate access or interception of data sent over the wireless network. Because wireless transmission can create a significant security risk, organizations who are members of a health information exchange network need to determine if wireless transmission of data will be allowed and, if so, implement appropriate commonly agreed upon wireless security standards which need to be managed by a collaborative team or neutral third party.

Audit Controls:

- Organizations need to implement technical processes that accurately records activity related to creation, modification and deletion of confidential information. This potentially means creating manual audit controls for confidential data stored in paper form and/or on legacy systems that do not have appropriate audit functionality. Technical audit controls need to be implemented that monitor and create appropriate logs to address access, transmission, creation, destruction and modification of data stored centrally for a centralized health information exchange network and, where access, transmission, creation, destruction and modification of data are allowed to another organization's data participating in a decentralized health information exchange network.

Integrity:

- Organizations need to implement processes to reasonably ensure confidential or mission critical data is not improperly altered or destroyed. This includes data that is centrally stored supporting a centralized health information exchange network.
- Protection from Malicious Software – Anti-virus and anti-spyware software needs to be acquired, properly updated and utilized to reasonably ensure viruses, worms, trojans, spyware, etc. do not infect the network or software applications. All member organizations participating in a health information exchange network need to adhere to scalable standards collaboratively established to reasonably ensure protection against malicious software. Also, such protection needs to separately managed for data stored outside individual organizations (such as in a centralized database).
- Protection from Outside Threats – Workforce members should be prohibited from loading any software brought from home and not approved by the security officer. Also, workforce members should be prohibited from downloading applications from the Internet unless specifically authorized by the security officer. Member organizations should be prohibited from transmitting executable and other related files across a health information exchange network unless specifically approved by member organizations. Any software/application to be commonly used by member organizations needs to be jointly evaluated to reasonably ensure the software/application includes appropriate security functionality such as access control mechanisms, appropriate role based access control functionality, audit logs, etc.

Person or Entity Authentication:

- Organizations need to implement controls that accommodate proper authentication of the user before allowing the user access to confidential

or mission critical data. This is true for internal and cross-organizational data access control.

Transmission Security:

- Integrity Controls – Organizations need to implement integrity controls that check for improper modification or destruction of data in transit across an open network (the Internet). The preferred method is to appropriately encrypt data that will be transmitted across an open network. A review of data integrity should also be included as part of a regular audit process. Such integrity controls need to be implemented across organizations participating in a health information exchange network.