Encryption Procedures

<table>
<thead>
<tr>
<th>Version</th>
<th>Approval Date</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3</td>
<td>September 26, 2022</td>
<td>Chief Information Security Officer</td>
</tr>
</tbody>
</table>

1. **Purpose of Procedure**

To establish the methods for protecting the confidentiality, authenticicty and integrity of enterprise data at rest, in transit, and in storage by cryptographic methods.

2. **Procedure Scope**

All employees, interns, contractors, members, participants, vendors and third parties who have access or exposure to HealthShare Exchange (HSX) confidential data are required to comply with this policy.

3. **Procedures**

A. **Approval and Regulation**

1. All encryption mechanisms and procedures for ensuring encryption must first be approved by the Chief Information Security Officer (CISO) before implementation.
2. As a part of the approval process, all encryption mechanisms implemented below must support a minimum of 256-bit AES (Advanced Encryption Standard) encryption.
3. Compliance with the relevant regulations is reviewed by the CISO on an annual basis, with the CISO making the necessary modifications.
4. Trusted authority shall be used (e.g. for the purposes of issuing and maintaining digital signatures and/or digital certificates) security is integrated and embedded throughout the entire end-to-end certificate/signature management process.
5. HSX maintains all digital certificates which are stored in the DigiCert vault, google authenticator is used to accessing to vault, and access is given to limited trustworthy employees.
6. HSX shall use ZIX to scan all outbound mails for any organizational information and applies encryption to the mails.

B. **Ensure FIPS-validated cryptographic mechanisms are used during transmission to prevent unauthorized disclosure of information and detect changes to information unless otherwise protected by an organization-defined alternative physical measures. HSX Supported mechanisms are TLS 1.3, TLS1.2 and Bouncy Castle and are implemented.** The protocols used for
communications will be enhanced to address any new vulnerability. The updated versions will be adopted as soon as possible.

C. Enterprise data on mobile computing devices, removable media and across communication paths must be implemented per the Encrypting and Securing Devices Procedure

https://hsxsepa-my.sharepoint.com/personal/onedrive_hsxsepa_org/_layouts/15/guestaccess.aspx?guestaccesskey=CcEdC5ckz6LOQEkMcNy0loZwe144l2VrhQptvXMRPPQ%3d&docid=2_14a3bea8ebbdd445db4e933a315da365c&rev=1

D. When un-encrypted information is discovered the following steps should be taken:

1. If un-encrypted enterprise data is discovered on removable media, they will be transferred either to a HSX-managed computing device or to an approved, encrypted removable media format.
2. If un-encrypted media had been used for enterprise data storage, the unencrypted media will be first transferred to an approved, encrypted media and formal then turned in to the CISO for disposal.

E. Encryption Key Management

1. Encryption keys and/or passwords are neither be printed or accompany removable media and are kept both physical and electronically separate.
2. Encryption key management shall be implemented based on specific roles and responsibilities (see approval and regulation section above) and in consideration of national and international regulations, restrictions and issues by the usage of an approved external vendor.
3. Encryption keys and the equipment to generate, store and archive keys shall be logically and physically protected against modification, loss, destruction and disclosure by the use of an approved external vendor. The AWS identify access management system manages our encryption keys and prevents any key use from being downloaded or modified. The most HSX Administrators can do is create, enable or delete keys.
4. Approved encryption tools and protocols in use: PGP, TLS1.2 or higher and AES 256, WPA2 on access points.
5. A formal key management system shall be defined and implemented consistent with federal and industry-recognized guidelines to securely manage secret/private keys and public keys issued by trusted Certificate Authorities.
6. Access to encryption keys shall be limited to designated HSX employees and not revealed to consultants, contractors, vendors, or other third parties.

7. Employees responsible for encryption key management shall sign a Confidentiality Agreement and shall be subject to background checks and screening at the time of employment and regularly thereafter.

8. Encryption keys shall be generated and maintained in such a way that no single person has full knowledge of any single encryption key.

9. Encryption keys shall be encrypted in storage by a separate key used only for this purpose.

10. Encryption keys shall be limited to a period of time not to exceed one year through purchasing certificates which are valid for one year at a maximum.

11. Specific mechanisms shall be put in place to recover information in case the encryption keys are lost by utilizing an external vendor for key maintenance and storage.

12. Keys shall not be stored in the cloud (i.e. at the cloud provider in question), but maintained by the cloud consumer or trusted key management provider (external vendor). Key management and key usage shall be separated duties.

13. HSX ensures the storage of the transaction details are located outside of any publicly accessible environments and not retained and exposed on a storage medium directly accessible from the Internet.

4. Definitions

For a complete list of definitions, refer to the Glossary.

5. References

Attachment – Certificate Management Step By Step Process (Below)
<table>
<thead>
<tr>
<th>Date Procedure to go into Effect:</th>
<th>September 26, 2022</th>
</tr>
</thead>
<tbody>
<tr>
<td>Related Documents:</td>
<td>Encryption Policy</td>
</tr>
<tr>
<td></td>
<td>Glossary</td>
</tr>
</tbody>
</table>

Attachment – Certificate Management Step By Step Process

1. A certificate is expiring soon.
2. Change request ticket is opened to get approval, this is reviewed once a week by the team.

3. Chief Information security officer- Brian Wells or Director of Technology- Alice Vuong approves the change request during the weekly meeting.
4. CSR file is generated and used to place the new/renewal order on DigiCert
5. Order placed by one of the users that has access to HSX DigiCert account (see attached DigiCert user list)
6. Certificate is renewed/ordered following DigiCert’s guideline, see screenshot of a sample order.

7. Once the order is placed on DigiCert, Brian who is a verified contact will receive an email, the email contains a link directly to the DigiCert order. He needs to approve for DigiCert to...
proceed with finalizing the request.

8. DigiCert issues the cert after it has been approved by Brian
9. new certificate files are used to replace the expiring certs
10. private key, public key and CSR files are stored on the HSX LastPass account, with only a few has access to the shared folder (see attached), Users on LastPass are required to use MFA
to login. These certificates files are then deleted from the HSX representative’s local machine.
MULTIFACTOR AUTHENTICATION

Enter a one-time passcode from your authenticator app.

Passcode
- Must be at least 6 digits

Trust this computer for 30 days

I've lost my Google Authenticator device